

HU ISSN 1588-6735 (print)

HU ISSN 3004-2518 (online)

EUROPEAN INTEGRATION STUDIES

VOLUME 20, NUMBER 2 (2024)



FACULTY OF LAW

UNIVERSITY OF MISKOLC

The Editorial Board of the Journal of European Integration Studies

A publication of the Faculty of Law, University of Miskolc (UOM)

Editor –in-Chief:

Prof. Csilla Csák, lawyer (UOM)

Editor:

Andrea Jánosi, PhD, lawyer (UOM)

Secretary of

the Editorial Board:

Csenge Halász, PhD, lawyer (UOM)

Gergely Cseh-Zelina, lawyer (UOM)

Members of

the Editorial Board:

Anna Petrasovszky, PhD, lawyer (UOM)

Prof. Nóra Jakab, lawyer (UOM)

Prof. Emőd Veress, lawyer (Sapientia Hungarian University of Transylvania, Cluj-Napoca)

Prof. Sibilla Buleca, D.Jur.Sc., lawyer (Uzhhorod National University, Ukraine)

Prof. György Kocziszky, economist (UOM)

Attila Dudás PhD, lawyer (University of Novi Sad, Serbia)

Anikó Raisz, PhD, lawyer (UOM)

Zsófia Asztalos, PhD, lawyer

István Bajánházy, PhD, lawyer (UOM)

Edina Vinnai, PhD, lawyer (UOM)

Jenő Szmodis, PhD, lawyer (University of Public Service)

Pavel Salák, PhD, lawyer (Masaryk University, Brno, Czech Republic)

Prof. János Ede Szilágyi, lawyer (UOM)

Prof. Anita Paulovics, lawyer (UOM)

Zsolt Czékman, PhD, lawyer (UOM)

Prof. Erika Jámborné Róth, lawyer (UOM)

Adrienn Nagy, PhD, lawyer (UOM)

Zoltán Varga, PhD, lawyer (UOM)

Ágnes Juhász, PhD, lawyer (UOM)

Bence Udvarhelyi, PhD, lawyer (UOM)

Zsófia Hornyák, PhD, lawyer (UOM)

Miklós Nyíró, PhD, philosopher (UOM)

Kinga Szabó-Tóth, PhD, sociologist (UOM)

Diana Cirmaciu, PhD, lawyer (University of Oradea, Romania)

Prof. Mariann Veresné Somosi, economist (UOM)

Prof. Alina Badulescu, economist (University of Oradea, Romania)

Prof. Dan-Cristian Dabija, economist (Babeş-Bolyai University Cluj-Napoca, Romania)

Prof. Ákos Farkas, lawyer (UOM)

Zoltán Angyal, PhD, lawyer (UOM)

Prof. Zsuzsa Wopera, lawyer (UOM)

* * * * *

**UNIVERSITY OF MISKOLC, FACULTY OF LAW
3515 MISKOLC-EGYETEMVÁROS, HUNGARY**

Tel.: +(36) (46) 565-111/13-53

E-mail: editor.eis@uni-miskolc.hu

CONTENTS

Tamás Csiki Varga:

Kickstarting the Hungarian defence industry in the 2020s – Synergies, opportunities, and obstacles for smaller member states within EDTIB 7

Karl-Heinz Gimmmler:

Constitutional and European legal rules for armaments' quality and presentation of alternative procurement: Contribution to the possibilities of contractual optimisation in armament procurement (the contract as a force multiplier)..... 33

Stjepan Groš:

Social engineering warfare as a tactic of information warfare- 67

Attila Horváth:

New Types of Higher Airspace Flight Operations and Their Legal Challenges 87

Marko Jurić:

Legal regulation on the use of artificial intelligence for national security purposes in Europe 107

Barbara Kaczmarczyk:

Cybersecurity from a systemic perspective 137

Bálint Kovács:

Screening for Security: The Defence Sector as a Gateway to Broader Economic Control 161

Kaja Kowalczevska:

Human oversight and risk-based approach to artificial intelligence: What does the Artificial Intelligence Act have in common with discussions about lethal autonomous weapon systems?..... 189

Katarzyna Malinowska:

Space defence legal regime in the service of sustainable development 213

Krzysztof Masło:

Accession of the European Union to the European Convention on Human Rights from the perspective of the Common Foreign and Security Policy ... 241

Jan Mazal:

Defence capability development optimization 263

Anna Molnár:

The growing role of the European Commission in defence capability development 291

Grzegorz Ocieczek:

The Internal Security Agency and Poland's Critical Infrastructure Protection: Challenges and Solutions 319

Andrzej Pawlikowski:

The EU's defence ambitions in the field of defence technological and industrial development 345

Iztok Prezelj:

Challenges in the Use of Artificial Intelligence-enabled Systems in Modern Armed Forces 383

Miha Šepec - Maša Kočivnik:

Combatting Cyberwarfare Crimes in the European Union 409

János Székely:

Export Restrictions in the Field of Artificial Intelligence and Quantum Computing: Justification and Risks – The United States–China Rivalry from a European Union Perspective 433

Zvonko Trzun:

Artificial Intelligence and Human-out-of-the-Loop: Is It Time for Autonomous Military Systems? 479

TAMÁS CSIKI VARGA*

Kickstarting the Hungarian defence industry in the 2020s – Synergies, opportunities, and obstacles for smaller member states within EDTIB**

ABSTRACT: Since 2016, Hungary has embarked upon developing its national defence industrial capacities as part of a comprehensive homeland defence and armed forces modernisation programme. Once underfinanced and degraded, with minimal capacity remaining, the national defence technology and industrial base have been reorganised and developed over the past decade as an integral part of the defence modernisation programme. Meaningful production, research, and development capacities have been developed in close cooperation with Tier-1 European (particularly German) defence industry firms, with a focus on regionalisation; cooperation with Turkish, Austrian, and Czech firms; and various joint ventures. Relying on the opportunities offered by European cooperation initiatives (both within the EU and NATO), these projects aim to tie Hungarian and joint ventures to the European Defence Technological and Industrial Base, as well as to make use of joint technology development and available resources for multinational cooperation. Based on the thorough assessment of primary sources (strategic documents, expenditure data) and secondary literature (expert analyses and media reports) this paper provides an overview of these processes. The goal of the paper is to assess the synergies, opportunities, and obstacles for developing the Hungarian defence industry in the 2020s, presenting the lessons learned to its European allies. The conclusions of the research show that kick-starting a rapid, large-scale industrialisation and modernisation programme with an innovation edge by the early 2030s is a “high risk – high reward” strategy. This ambitious goal is supported by sizeable midterm procurement programmes driven forward by a record-breaking defence budget; redesigned institutional, legal, and innovation frameworks; and an integrated long-term national industry development programme. Still, sustaining high-level investment, providing skilled and

* Tamas Csiki Varga, PhD, is senior research fellow at John Lukacs Institute for Strategy and Politics, affiliated with Ludovika – University of Public Service, Hungary. <https://orcid.org/0000-0003-3971-8231>, csiki.tamas@uni-nke.hu.

** The research and preparation of this study was supported by the Central European Academy.

qualified workforce, and developing innovative capacities remain the most crucial pillars of developing the Hungarian defence industry.

KEYWORDS: Hungary, industry, strategy, defence spending, technology, EDTIB.

1. Introduction

When examining national defence industrial capacities and capabilities in Europe, Hungary should be considered a special case compared to other countries, as much of its national defence technological and industrial base was reconstructed, redeveloped, or newly established after 2016. There are several reasons for this as follows. First, because of an overarching trend, the Hungarian defence sector has been chronically underfinanced since the 1990s, thus leading to abandoning complete services and weapons systems (e.g. artillery of almost every kind and much of the heavy equipment), losing hardware, and leaving the Hungarian Defence Forces (HDF) exposed and vulnerable by the 2010s. Therefore, the national defence industry was not involved in supporting modernisation and was only occasionally employed in the operation and maintenance (O&M) of equipment. Second, partly in parallel to these processes, the Hungarian defence industry has continually been decreasing production capability, technological know-how, management expertise, the number of skilled workers such as technicians and engineers, and the capabilities necessary to run a complex, modern defence industrial ecosystem. This downward spiral was driven by the limited modernisation of HDF until the late 2010s, off-the-shelf procurement from foreign companies whenever modernisation was taking place, and a lack of incentives to develop national firms' production and innovation capacities. As such, the workshare and added value of Hungarian firms were marginal. Third, since the innovation infrastructure and management in Hungary has remained underdeveloped in a general sense, particularly regarding defence innovation, defence industrial supply chains have become degraded, with small and middle enterprises (SMEs) only occasionally involved in supporting defence production and innovation. Most importantly, even the most capable national defence firms remained weakly integrated in European defence industrial cooperation.

This downward trajectory had been changed by initiating the comprehensive Homeland Defence and Armed Forces Modernization

Programme – originally dubbed ‘Zrínyi 2026’ – in 2016. Since then, the modernisation has become not only the largest for the HDF since the 1980s, but also a comprehensive action to strengthen military capabilities, as well as the system of homeland (territorial) defence, and to reinforce the defence industry. The latter goal envisages the rebuilding and advancement of the defence industry based both on national pillars and through international cooperation with leading innovators able to push key players in the Hungarian defence industry to excel in industrial competition.

After decades, this was the first defence modernisation programme to include a determining industrial defence element. At the same time, this took place based on the remnants of Hungarian defence industrial capacities from the 2000s, now aimed at kick-starting a rapid, large-scale industrialisation and modernisation programme with an innovation edge by the early 2030s. This ambitious goal is supported by sizeable midterm procurement programmes driven forward by a record-breaking defence budget; redesigned institutional, legal, and innovation frameworks; and an integrated long-term national industry development programme.

The current international environment is favourable for accommodating and supporting such industrial defence plans. European countries have witnessed subsequent crises in the 2010s and a large-scale, high-intensity conventional war in Ukraine following Russia’s 2022 military aggression. Regional instability and threat perceptions focusing on Russia drive European countries’ strategic considerations towards strengthening their armed forces’ defence capabilities. As most European countries have undergone similar capability losses, while the research and development of modern technologies lags behind the U.S. and its potential rivals, there is a lack of capabilities and production capacities that motivate European countries to develop their national defence industries. Many European countries not only strive to make up for lost capabilities and strengthen national and allied capacities but also to support Ukraine with weapons and war material in its war of self-defence. Joint European defence collaboration has been gaining momentum in recent years, with the European Defence Industrial Strategy adopted in 2024 as the latest example, along with many other financial, technological, and institutional initiatives. The current era of rapid technological advancement in dual-use and military technologies, as well as the combination of emerging and disruptive technologies, serves as a strong driving force behind the research, technology, and innovation in the defence sector.

2. Goals and methodology

Following these drivers, this study aims to provide an overview and assessment of the synergies, opportunities, and obstacles to developing the Hungarian defence industry in the 2020s, thus presenting the lessons learned to other member states within the European Defence Technological and Industrial Base (EDTIB). As the modernisation and upgrading of the Hungarian defence industry is primarily driven by the ongoing Homeland Defence and Armed Forces Modernization Programme, the underlying drivers and goals, as well as the strategic framework, will be introduced to determine which areas of the defence industry are to be developed. This is followed by the introduction of Hungary's national defence technological and industrial base (NDTIB), highlighting primary development projects and outlining the new institutional setup that underpins them. An assessment of the defence investment background will show the material sustainability of the sectoral transformation, while an outlook on the coming years and the identification of inherent risks to success will conclude the paper.

The thorough investigation of these issues was realised through the analysis of national strategic documents, available government reports, and commentaries, as well as the comprehensive context and goals of the armed forces' modernisation programme. The Hungarian case study is mapped on the major initiatives and projects related to the development of the defence industry, such as the purchase of military equipment, cooperation with European manufacturers, and reorganisation of the national defence technology and industrial base. These steps make it possible to identify the major innovation trends in the defence industry intertwined with international technological cooperation, thus identifying opportunities for growth and synergies. At the same time, structural weaknesses and risks to the successful development of the defence industrial ecosystem, as well as its efficient functioning and stable production capacities, can be identified. This may also hinder the integration of the Hungarian defence industry with its European partners. However, throughout this evaluative process, a possible shortcoming is the limited transparency of ongoing processes, visible only through government communication (of success) because independent critical analyses remain scarce.

3. Underlying drivers and goals

The comprehensive armed forces modernisation programme, which serves as the direct background for the development of the defence industry, is both an opportunity and a constraint. We can identify several drivers that have led to political decisions mandating these development programmes over the past decade.

The security environment of Hungary – and of Europe – has been deteriorating during the past decade, as non-military challenges and military threats appeared in the security perception of Hungarian society and the political elite. The Russo–Georgian war (2008), the global economic crisis (2008–2009), the ‘Arab Spring’ (2010) and the ongoing resulting crises and civil wars (Syria, Libya 2011–), the rise of the Islamic State (IS) in the Middle East (2014) and IS-motivated terrorist attacks in Europe (2015), uncontrolled mass migration (2015), the coronavirus pandemic (2019–2021), the Armenia–Azerbaijan war (2020), the escalation of the Russia–Ukraine war (2022–) with subsequent energy and economic crises (2022–2023), and the latest Hamas–Israel war in Gaza (2024) all acted as stress factors for European security and stability. It was not a coincidence that Hungarian defence modernisation, coupled with defence industrial upgrades, began in the mid-2010s.

Meanwhile, European integration stalled and despite external threats and challenges, joint European action to manage crises has not become more effective due to the different approaches of its member states; for instance, the increasing popularity of the ‘Europe of strong nation-states’ model weakens integrated, joint action. In the military field, Russia’s repeated aggression in 2014 and 2022 triggered NATO’s united political action and strengthened its collective defence and deterrence on the eastern flank, bringing about a general modernisation drive of national armed forces. This was coupled with a significant transition in legacy military equipment from Central European countries to Ukraine as military aid, leaving a caveat that must be filled with new modern equipment as soon as possible.

Since the 1990s, despite joining NATO (1999) and the European Union (2004), the Hungarian Defence Forces have been moving on an almost unbroken trajectory of reducing personnel, military equipment, and military capabilities. The last systemic procurement took place in the early

1980s, but since then, there have only been episodes of gaining relatively modern equipment (T72 tanks, Mig 29 fighter aircraft, and Mistral air defence systems). Since the regime change (1989), it was only possible to keep up with the development of military technology on a case-by-case basis for individual weapon systems (e.g. the multi-purpose Gripen aircraft); in general, the lifecycle extension of the equipment (helicopters, transport aircraft) or the abandonment of capabilities (artillery, tanks) was typical. This made the comprehensive modernisation of HDF inevitable in the 2010s.

Thus, Hungarian military modernisation fits into regional trends: although with time differences, all Eastern and Central European militaries have been modernising, and in many cases even expanding their forces, through strengthening territorial defence capabilities as a general trend. This means the procurement of heavy military equipment (armoured vehicles and artillery) and strengthening of (territorial defence) reserve forces, which is also a priority for Hungary.

As assessed in detail later in this paper, the necessary economic background – the dynamic and predictable growth of the national defence budget – became available for defence modernisation in 2015 and has been sustained since then. Based on this transformation of the threat landscape and allied responses, the planning of a comprehensive homeland defence and armed forces modernisation programme (2016) enjoyed the government's conviction and commitment. This commitment has been maintained throughout the execution phase, despite the economic downturns caused by COVID (2019–2021) and the economic fallout of Russian aggression against Ukraine (2022–).

Moreover, large-scale military modernisation was directly embedded in the development of the Hungarian defence industry, either through new investment in international (German, Turkish, and French), cooperation and from the perspective of innovation, or through the foundation of new capacities in the national defence industry from R&D and innovation through production to the future export of arms. This means that, beyond the off-the-shelf procurement of advanced systems that had no meaningful technological footprint in Hungary (helicopters, aircraft, air defence systems, and tanks), large-scale co-production and co-development projects have also been initiated (infantry fighting vehicles and mine-resistant ambush-protected vehicles). Some basic building blocks of arm production,

such as gunpowder, explosives, small arms, and small-calibre artillery, must be established from scratch.

4. Strategic framework

The strategic objectives and main pillars of the programmes that constitute the framework of the comprehensive homeland defence and armed forces development programme can be mapped indirectly based on the 2020 National Security Strategy (NSS)¹, 2021 National Military Strategy (NMS),² policy statements, and scientific articles. Specific Defence Industrial Strategies were also adopted in 2021 and 2023, but these – similar to the planning documents of the Armed Forces Development Program – are not publicly disclosed and can only be assessed based on secondary sources.

The strategic goal for 2030 is to create a comprehensive national defence system that can defend against military threats, hybrid challenges, and civilian crisis-management tasks (NSS, Article 126). To this end:

The Hungarian Armed Forces must have well-equipped and well-trained forces, as well as flexible, effectively applicable, deployable, and sustainable, interoperable capabilities, striving to improve quality indicators in addition to quantity. In addition to its traditional national defence and international crisis management tasks, it must be equally capable of contributing to the management of crisis situations caused by mass immigration or terrorist threats, to play a role in preventing hybrid attacks, and to contribute to the elimination of the consequences of natural or industrial disasters. The armed forces must be developed in such a way that they are able to produce effects in the operational spaces relevant to our country: on land, in the air and in cyberspace.³

Therefore, the armed forces development plans did not aim at creating specialised ('niche') capabilities, but rather a – relatively – broad spectrum HDF capabilities. The means of realising these goals were the homeland defence and armed forces development programme (NSS, Art. 27-28), the

¹ Government Decree 1163/2020.

² Government Decree 1393/2021.

³ NSS, Art. 135.

strengthening of military cyber defence capabilities (NSS, Art. 159), and the development of the national defence industry (NSS, Art. 2, 5, 6, 28-29, 105, 128, 136).⁴

In accordance with the NSS, the National Military Strategy not only squared the government's strategic considerations behind the armed forces development programme and the views of military commanders on modern warfare but also summarised the drivers of the developments between 2016 and 2021 and set tasks for the 2020s. The strategy organised the tasks of the Hungarian Defence Forces into two comprehensive groups: the national dimension contained nine comprehensive tasks and six international comprehensive tasks with numerous sub-tasks. Increased ambition and underlying goals in procurement, personnel, and structure were also observed, with a modernisation horizon of 2032. Current force structure development plans are built on a four-brigade structure by increasing the number of troops from 26,700 active soldiers plus 11,000 reserves to 37,650 active-duty soldiers plus 20,000 reserve soldiers.

Regarding the specific capability requirements for military equipment, that is, modernisation priorities, we can formulate guidelines based on the work of Ferenc Márkus and Balázs Szloszjár. Accordingly, systems-based development covers the entire range of equipment and weapons of infantry riflemen and squads, infantry fighting vehicles, tanks for heavy brigades, command and control, surveillance and reconnaissance systems, IT, and cyber defence systems at the battalion level that form the backbone of the brigades, army air defence, self-propelled artillery, direct fire support, CBRN protection, and maintenance and logistics assets.⁵ In 2017, Szloszjár also added that

it is advisable to procure certain military equipment of high importance – the individual military equipment of the soldiers, infantry fighting vehicles, mechanized vehicles – preferably from domestically developed or domestically produced sources (through purchase of licenses, production based on cooperation).⁶

⁴ Csiki Varga and Tálas, 2020, pp. 89–112.

⁵ Márkus, 2013, pp. 30–33.

⁶ Szloszjár, 2017, p. 27.

These guidelines were incorporated both in the acquisition of equipment and in the development of the defence industry for the subsequent years.

Based on publicly disclosed information and practical experience from procurement, force development can be characterised retrospectively according to the following general principles:

- The HDF must become a highly mobile joint force equipped with modern arms and capable of rapid reaction and effective intervention simultaneously in several theatres by possessing information and decision-making superiority and relying on its all-volunteer professional and reserve forces within both national and allied frameworks.⁷
- As a result, by 2030, the Hungarian Defence Forces

will be able to guarantee the security and sovereignty of Hungary both through credible deterrence based on its national capabilities, and within the framework of collective defence together with allies (benefitting from security guarantees and contributing to strengthening these), as well as through international peace operations that contribute to the stability of the international system by building partnerships, security sector reform, and training.⁸

- A systemic approach was applied throughout the planning of modernisation, from the individual fighters to the brigade level, and in terms of the ability to integrate forces, weapons, and specialised teams in both human and technological dimensions.
- Capability-based force planning was applied.
- Lifecycle planning considers procurement costs, infrastructure, logistics, operations, and maintenance.
- Where possible, the procurement of ‘product families’ was realised for weapons systems as this increases efficiency in logistics, operations, and maintenance.
- R&D, innovation, production, procurement, and maintenance have been viewed as joint processes with integrated implementation

⁷ Sticz and Seprődi-Kiss, 2020, p. 6.

⁸ Ibid.

supported by the expansion and development of the national defence technology and industrial base.

- The national production and supply bases of some highly important military industry segments (e.g. small arms, gunpowder, explosives, armoured vehicles, and artillery) have been established.
- New ‘incoming’ technologies (even those still under development) were acquired and combined into new products (Lynx and Gidrán) to further develop the fourth-generation military technology and offer the perspective of international sales of new products.
- The national defence technological and industrial base was developed with a regional focus and networked approach, developing connections with the German, Czech, Austrian, and Turkish defence industries.

In sum, technological modernization has been a central element of the ongoing armed forces development programme, which encompasses across-the-board procurements in almost every armed service: small and light weapons, ammunition, anti-tank weapons, infantry fighting vehicles, tanks, artillery ranging from mortars to long-range artillery; light and medium utility and multi-purpose helicopters, military transport, training and combat aircraft, air defence and missile defence; command, control and communication, as well as logistics, repair and maintenance capabilities are under modernization. The current and future development of national defence technology and industrial bases support this endeavour.

5. National defence technological and industrial base (NDTIB) in Hungary by 2024

The entire Hungarian defence ecosystem is undergoing a fundamental transformation through the comprehensive homeland defence and armed forces modernisation programme, constituting not only a generational upgrade in technology but also the adoption of suitable modern doctrines and operating procedures, as well as adapting the workforce and service (wo)men’s training to the use of new hardware and software.⁹ This transformation of NDTIB had two main goals. One is to create and/or strengthen certain pillars of the defence industry that have been weak or non-existent in Hungary since the Cold War. These include the assembly,

⁹ Budavári, 2021, pp. 137–151.

production (and future development) of small arms and light weapons, artillery, armoured vehicles (IFVs), radars, and sensors. Some niche products (e.g. helicopter parts) have also been targeted. The second goal is to develop strong tie-ins to major European arm manufacturers' networks (Rheinmetall, Krauss-Maffei Wegmann, Airbus) or through the acquisition (Hirtenberger, Aero Vodochody) or establishment (ZalaZone, Lynx, Gidran) of new defence industrial plants, which can support the successful transformation of the NDTIB. This (prospective) tie-in to top European value chains is accompanied by 'networked' regional defence industrial cooperation, involving German, Austrian, Czech, and Turkish firms, as mentioned above.

Currently, 568 entities are registered in Hungary for defence-related activities, of which 187 have self-declared production capacities (the others provide security and defence-related services and/or have such an export portfolio).¹⁰ These include dual-use technologies and services. The Hungarian Defence Industry Association, which is currently undergoing transformation, had (only) 40 registered members as of 2023, and the current number is not disclosed publicly. The forty members includes 'old' MoD-governed major enterprises (e.g. Currus, Arzenál, Armcom, or EI), but the newly established/acquisitioned national and joint international ventures (e.g. Rheinmetall Hungary, Hirtenberger Defence Systems, Aero Vodochody) had not yet joined. Of these 40 companies, 23 listed production and R&D capacities in their portfolios (different subsets), 19 listed maintenance, and only seven indicated existing test laboratories. Among the services provided, 13 indicated manufacturing, engineering, and test equipment; 13 indicated engineering services, training, and R&D; nine companies produced military and special-purpose vehicles; and seven military vehicle parts and spares. Eight companies provide services related to IT, computing, and software; seven companies provide C4I; and seven offer communication systems and equipment, sometimes in cross-cutting subsets.¹¹ Most of these companies are SMEs, and the more significant enterprises have limited resources, know-how, manpower, and expertise. The degree of development after 2023 in this subset cannot be estimated because the change is not transparent.

¹⁰ In spring 2023, the number of registered entities was 525, of which 169 had production capacities, which indicates a ca. 10%, dynamic increase in a year. Source of data: Government Office of the Capital City of Budapest, 2024.

¹¹ Defence Industry Association of Hungary, 2023, pp. 184–185.

Altogether, the total number of employees currently directly involved in the defence industry was estimated to be around 2,000 people, the Ministry of Innovation and Technology plans to increase this number to 5,000–8,000 employees by 2030, driven by ongoing investment projects involving large-scale manufacturing and the associated production chain.¹²

Furthermore, the Hungarian defence sector is expected by the Ministry of Defence to generate a HUF 500 billion¹³ output by 2030, becoming ‘one of the determining defence industrial hubs of the region’. This would be a gigantic leap from the EUR 40 million annual average from defence exports in the 2010s and a significant increase compared to the approximately EUR 900 million dual-use export value.¹⁴ The latest data available (for 2019) show that arms exports primarily involve ammunition, land vehicles and parts, radio and communication systems, CBRN equipment, and personal protection gear. The overall trade amounted to EUR 231.45 million, out of which exports represented EUR 53.39 million; thus, the balance was negative.¹⁵ Hungary’s main defence export partners were Germany, Switzerland, the U.S., and Canada, with minor/occasional shares from Malaysia, Austria, France, Italy, and Slovakia.

To achieve this ambition, the Defence Industrial Strategy (adopted in 2021, publicly unavailable) identified six clusters around which investments, partnerships, and development will be centred in the next decade. The clusters and their flagship projects are as follows:

- *IVF, APC production, and military vehicles manufacturing in the Zala, Somogy, and Győr counties (SW and NW Hungary).* As the most important element, joint venture Rheinmetall Hungary will provide Lynx infantry-fighting vehicles (218 pieces, out of which 172 will be manufactured in Zalaegerszeg) supplied with a StrikeShield active protection system, including Israeli LR-2 Spyke anti-tank rockets. Future innovation projects may include integrating the Israeli-made Trophy active protection system and Rheinmetall’s Oerlikon Skyranger anti-aircraft system into Lynx. Cooperation with Rheinmetall also includes the procurement/manufacturing of 300 armoured personnel carriers, 40 of which bought from Turkish Norul Makina in its original design (Ejder Yalcin), while the remaining 260

¹² Hecker, 2022.

¹³ EUR 1.28 billion at a HUF/EUR 390 exchange rate.

¹⁴ Guttray, 2018, p. 64.

¹⁵ Budapest Főváros Kormányhivatala, 2019, pp. 24–25.

will become a Hungarian configuration, called Gidran, equipped with a wide range of sensors and flexible in functional fitting (produced in Győr, in cooperation with Hungarian vehicle manufacturer Rába). Moreover, 4 x 4 vehicles and military trucks will be manufactured in Kaposvár. This cluster also includes a test range (ZalaZone) and validation labourers to support innovation, particularly for autonomous vehicles based on Rheinmetall's Mission Master XT. The design and development of a new 8×8 hybrid next-generation fighting vehicle in cooperation with Rheinmetall and Krauss-Maffei Wegmann is also an option that might even serve as a long-term replacement for the BTR-80 IFV in the HDF (currently unresolved). Furthermore, news of participating in the research and development phase of Rheinmetall's next-generation main battle tank, the KF51 Panther, equipped with a 130 mm gun, active defence systems, AI-assisted fire control system, associated drones, and a range of sensors, has been aired in 2023.¹⁶

- *Aviation industry in Békés county (SE Hungary)*. A rather small but high-value footprint from Airbus Helicopters will provide for the production of helicopter engine parts in Gyula, accompanied by the surface treatment of helicopter parts by Satys PSP Hungary Ltd. The Brazilian Embraer, from whom the HDF procures two KC-390 military transport planes, also announced the establishment of an R&D centre in Hungary.
- *Small arms production in Bács-Kiskun county (S Hungary)*. Based on the licence of Česká Zbrojovka, the MoD Arzenál assembles small arms in Kiskunfélegyháza together with Unique Alpine machine guns and develops the Hungarian-designed Gestamen small arms family. Colt CZ Group and N7 Holding Ltd. established a joint venture for small arms production. Dynamit Noble Defence and MoD Arzenál will produce reactive armour (possibly a DND ERA to be integrated into the Lynx IFV) and anti-tank weapons for light infantry.
- *Ammunition and explosives production in Veszprém and Fejér counties (Central Hungary)*. Rheinmetall Waffe Ammunition has developed two facilities in the vicinity of Várpalota: one to manufacture 30-, 120-, and 155-mm artillery shells (for the Leopard-2 tanks, Lynx IFVs, and PzH-2000 artillery) and the other to produce

¹⁶ Huszák, 2023.

hexogen/RDX explosives. The relocation of Hirtenberger Defence Systems' mortar production capacities in this area will occur in 2024.

- *Radio and satellite communication systems manufacturing in Budapest and Fejér county (Central Hungary).* In the field of defence information technology, communication, and the space industry, 4iG, a joint venture of Rheinmetall AG (51%), 4iG Ltd. (39%), and MoD EI Ltd. (10%) is the leading actor and serves as a system integrator for network-based C4 functions. The 4iG Group has been expanding its portfolio beyond telecommunication services and IT system integration to include space, unmanned aerial vehicles (UAVs), counter-UAVs, and defence digitalisation. Furthermore, in 2022, 4iG will acquire an initial 20% stake in the Israeli company Spacecom, with the option of an additional 31% over the next three years. Since 2024, the orbital slot, currently providing space-based telecommunication opportunities for Spacecom leased from Hungary, has been occupied by CarpathiaSat, a 4iG joint venture. The slot will be used to launch Hungary's first commercial satellite in approximately five years. Most recently, the 4iG subsidiary Remred Space Technologies began developing a facility (Remtech) in Martonvásár capable of producing, testing, and validating space systems, including satellites weighing up to 400 kg, entering the market of low Earth orbit space assets in the coming years.
- *Radar and locator production in Szabolcs-Szatmár-Bereg county (NE Hungary).* When providing for the procurement of ELM-2084 multi-mission radars (11 pieces) for the HDF, Rheinmetall, Canada, places the production and maintenance of these assets in Nyírtelek.

In sum, one could characterise the next decade of the Hungarian defence industry as an attempt to grow from a backward garage-operated SME into a well-established national and, in some areas, an internationally recognised company with an innovative edge and sizeable arms export potential. This evolutionary jump situates the Hungarian defence industry in a particular position and creates unique requirements for the years ahead.

6. Developing the defence industrial ecosystem

Owing to the underdeveloped Hungarian defence industry by the 2010s, a two-track approach was applied in developing the sector. For highly advanced products for which Hungarian firms have no chance to compete in

the short term, renowned Tier-1 international firms with strong market positions became involved in joint projects, creating an industrial footprint involving both manufacturing and R&D in Hungary. Therefore, high market-entry costs were reduced to some extent. These flagship projects, most importantly, IVF, APC production, ammunition/artillery production, and space technologies, involve new multinational partnerships from Europe, particularly German, Turkish, and Israeli enterprises. The first tier of defence modernisation in the armed forces modernisation programme, the procurement of modern equipment, was designed and realised in a manner that focused on European manufacturers getting involved in a long-term production and innovation cooperation model, establishing new facilities in Hungary. In a general sense, a strongly ‘networked’ feature of these developments is observable: Hungary has been buying-in to German, Czech, Austrian, Turkish, and Israeli cooperations, with a prospect of acquiring technologies and know-how that can be combined and further innovated into new, high-tech marketable products. There is a certain risk involved in this approach because of the lack of battle-proof experience for these assets (Lynx and Gidran) and some of the experimental technologies combined with them. Moreover, for less advanced products and services, in which Hungarian firms have better chances of involvement, national enterprises receive tailored support from the government to improve their position and develop their capacity to join advanced production chains. Since 2021, SMEs have been competing for the resources of a defence industry supply chain venture fund worth HUF 50 billion (EUR 130 million).

The realisation of strategic goals related to the defence industry was first overseen by the Ministry of Innovation and Technology (until 2022), then by the Ministry of Technology and Industry (2023), and eventually delegated to the Ministry of Defence, where it belongs. The reason for the initial institutional setup was that, after not conducting meaningful defence industrial development activities and losing much of the R&D knowledge, the MoD seemed to lack the necessary management expertise, which had been developed as of 2024.

As a large number of procurement and development projects have been established as part of the armed forces modernisation programme, sometimes with the participation of newly established Hungarian companies and companies entering the Hungarian defence sector as newcomers from abroad establishing joint ventures, coordination and management have become crucial issues. To effectively coordinate their work, the institutional

and ownership concentrations of national government-owned entities became necessary. Just as the defence sphere is wider than companies with an exclusive military profile, the reorganisation of control over the most important companies took place with the cooperation of the Ministry of the Interior and the Ministry of Innovation and Technology by 2022.

As then minister of innovation László Palkovics summarised, defence industrial activity relies on two national pillars.¹⁷ The first was the National Defence Industrial Innovation CLC., where, in 2021, the ownership rights of elements with a defence industry profile from the national asset management organisations were merged; this is thus responsible for the management of, at least, partially state-owned companies, including the former MoD companies (Currus, Armcom, Arzenal), Rába, the ZalaZone test track, HungaroControl, Aeroplex, the state share in the Airbus plant in Gyula, the surface treatment plant in Gyula, Hirttenberger, Aero Vodochody, and the Hungarian business part of Rheinmetall Hungary CLC, as well as the state-owned part of the Várpalota munitions and explosives manufacturing joint venture, and finally, BM Heros.¹⁸ The other pillar is the Defence Innovation Research Institute (VIKI), which is the centre of the domestic defence innovation ecosystem. I would like to emphasize that this is a defence organization in a broad sense – that is, it is meant to support the general security of our country – and not a military industrial organization only. It is involved in developing dual-use products and technologies as well. It conducts research independently, but also oversees Hungarian and international R&D projects. Is also tasked with creating the conditions for technology transfer. VIKI is practically the domestic implementation of the American DARPA and NATO's DIANA program, summarised Palkovics.¹⁹ As Figure 1 shows, the defence industrial ecosystem now functionally involves R&D, with connections to the international defence industry and allied R&D programmes.

¹⁷ Hecker, 2022.

¹⁸ Ternovác, 2021.

¹⁹ Hecker, 2022.

Figure 1 Research, development and innovation in the Hungarian defence industrial ecosystem



Source: Végvári, 2023, p. 77.

Thus, involvement in the European and NATO defence innovation cooperation has become ever more important for enhancing Hungarian capacities. Innovation in the field of emerging and disruptive technologies in Hungary focuses on four aspects (out of eight identified by NATO): big data, AI, autonomous systems, and quantum computing. NATO's innovation accelerator programme, DIANA, first accepted two test centres from Hungary, linked to autonomous systems (ZalaZONE Automotive Proving Ground and ZalaZONE Research and Technology Center), with six test centres under the network brand VIKI-NOKIA accredited by NATO in 2024 (University of Pécs, University of Óbuda, BHE Bonn Hungary Electronics Ltd., Alverad Technology Focus Ltd., ITSec Area Ltd. and Nokia Bell Labs).

The 2021 European Defence Fund call sponsored six defence innovation projects with Hungarian participation: 5G COMPAD (Saab – BHE Bonn Hungary Electronics Ltd.), focusing on 5G communications for peacekeeping and defence; EuroHAPS (Thales – C3S Elektronikai Fejlesztő Ltd.), focusing on high altitude platform systems demonstration; FaRADAI (Ethniko Kentro Erevnas Kai Technologikis Anaptyxis – Certh Számítástechnikai és Automatizálási Kutatóintézet) diving into frugal and

robust AI for defence advanced intelligence; iFURTHER (Hellenic Aerospace Industry SA – BHE Bonn Hungary Electronics Ltd.), developing a high frequency over the horizon sensors’ cognitive network; NOMAD (Equipos Móviles de Campana Arpa, S.A.S. – F4STER–FUTURE 4 Co.), focusing on novel energy storage technologies at military deployments in forward operating bases; and ALTISS (Magellium S.A.S. – SAGAX Communications Ltd.), developing highly automated swarm of affordable ISR long endurance UAVs for force protection.²⁰ It is important to note that the SMEs that became involved in EDF projects in 2023 were among the Hungarian test centres accredited by NATO DIANA in 2024, showing the aim of creating synergies. However, among the 53 EDF-sponsored R&D projects awarded in the 2023 call, only one has Hungarian participation: CALIPSO, researching innovative propulsion solutions for land and naval defence applications with the participation of the Defence Innovation Research Institute.²¹ This may indicate that Hungarian innovation capacities are still limited in terms of the actors (companies) involved and research areas addressed. Hungary also leads one PESCO project (EUROSIM) and participates in eight other projects.²²

Directly driven by Ursula von der Leyen’s ‘geopolitical Commission’ and particularly triggered by the Russia–Ukraine war, the dynamic development of EU defence industrial policy reached new milestones throughout 2022–2024, eventually culminating in the adoption of the European Defence Industrial Strategy. Previous initiatives, such as EDIRPA and EDIP, created a role model for supporting early R&D in defence and a framework for co-sponsoring production. These new multinational solutions were also brought forward by EDIS. A programme that has already directly impacted Hungarian projects is ASAP, providing EUR 4.5 million in 2024 for extending Hungarian explosives and EUR 22.5 million for ammunition (shells) production capacities.²³

As the Hungarian NDTIB is still in the early development phase, its limited capacities and participation are not surprising; however, meaningful trends and results will likely be visible by the end of the 2020s. Cooperation is strongly focused on EDTIB, and dependence on European enterprises is seen as an opportunity (access to technology and international markets that

²⁰ European Commission, 2022.

²¹ European Commission, 2024a.

²² Nádudvari, Etl, and Berecky, 2020.

²³ European Commission, 2024b.

would otherwise not be open to Hungarian defence products) rather than a risk.

7. Defence investment trends

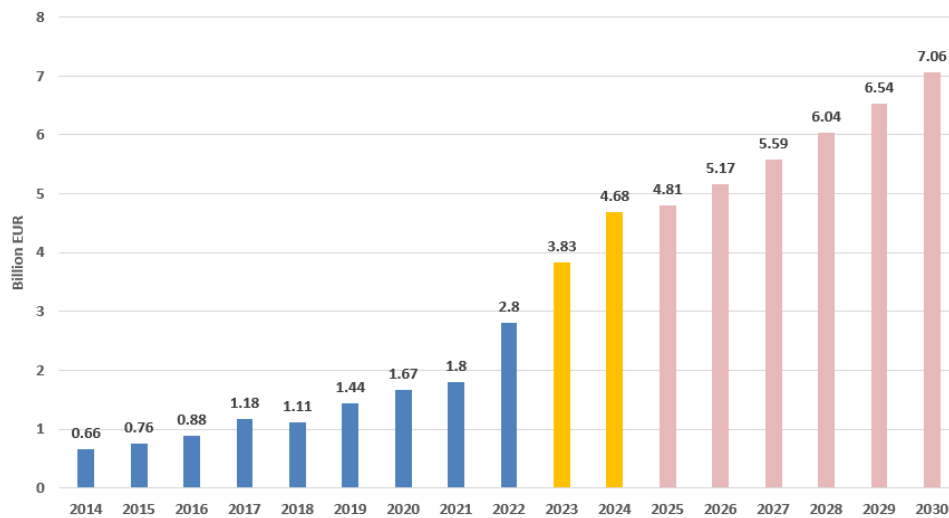
To sustain the current momentum of defence industry's development, there is one prerequisite that cannot be neglected: financial incentives and direct investment in the sector. After more than a decade of underinvestment and a practically flat defence expenditure trend between 2004–2014, leaving no room for modernisation, the Hungarian government began to substantially increase defence investment from 2015, paving the way for the modernisation programme of its armed forces.²⁴ As Figure 2 shows, following the 'lost decade'²⁵, the defence expenditure increased sevenfold between 2014–2024, EUR reaching 4.68 billion, thus fulfilling both NATO member states' Wales defence pledge for spending 2% of the GDP for defence and the commitment to spend a minimum of 20% of defence expenditures on procurements and modernization (actually exceeding 35% since 2019).²⁶

The current forecast of the Ministry of Defence for 2030 not only sustains the 2% GDP ratio but also expands it, with a gradual increase of 0.1% annually to reach 2.6% by 2030, which would amount to approximately EUR 7 billion. This investment background can stabilise the development of the armed forces and offer substantial development prospects for the NDTIB.

²⁴ Csiki Varga, 2023, pp. 1–2.

²⁵ Csiki Varga and Lázár, 2022.

²⁶ NATO, 2024.

Figure 2 Hungarian defence spending trend, 2014–2030

Source: Respective national laws on closing accounts (blue columns), on the annual state budget (yellow columns), and forecast of the Hungarian Ministry of Defence (MoD). The conversion to euros has been calculated using a 390 HUF/EUR exchange rate. Source of the MoD forecast: the public presentation of Lt. Gen. Ferenc Kajári, Deputy Chief of Defence of the Hungarian Defence Forces, at the Hungarian Defence Industry Summit, on May 10, 2024, in Budapest.

However, both the FY 2023 and FY 2024 defence budgets have included some degree of uncertainty, as 56% and 71% of the annual defence budgets were to be covered from the newly created ‘Homeland Defence Fund’, respectively. This Fund is the designated source of procurement and modernisation spending, and funds are collected from newly introduced taxes from the banking, finance, and insurance sectors, if achievable. This and any possible economic downturn must be observed in the coming years to make realistic planning and forecasting achievable.

8. Analysis of potential risks

While the goals identified above outline an ambitious plan to dynamically re-establish and build the Hungarian defence industrial capacities with an innovative edge, there are internal and external risks associated with this process. Some are internal, namely developing a practically new branch of industry out of scratch poses challenges, while others are structural, originating from the international embeddedness of the Hungarian defence industry (or lack thereof).

Internal risks stem from a lack of a consolidated defence industrial background on which new initiatives or projects are built: underdeveloped industries, non-existing national supply chains founded on a fragmented SME network, limited capacity in defence industrial start-ups, newly developed research institutions, and educational programmes; thus, new talent management needs to provide a skilled workforce in larger quantities and higher quality to meet the requirements of 21st century work requirements. Expertise in the management of individual defence industrial projects and their parallel coordination – not only in terms of defence planning by the MoD and the HDF but also on the wider coordination in the defence sphere – is scarce after neglecting such projects since the Gripen procurement, the last major procurement programme before the current comprehensive modernisation of the HDF. In addition, as mentioned above, long-term funding for structural development must be provided at a time when the Hungarian economy is still suffering the effects of COVID and the Russia–Ukraine war.

Certain risks can be associated with external and structural factors related to international frameworks and EDTIB, which the Hungarian national defence industry is part of and is becoming increasingly integrated into. Because of the transitional nature of the Hungarian defence industry, many background-enabling processes, such as the stable supply of raw materials and specialised parts in international supply chains, are currently unclear. This aspect is present in the strategic deliberations and contributes to choosing mostly European products for procurement and partners for enhanced manufacturing and R&D cooperation (not U.S. or Asian ones). However, Hungary has limited diplomatic, political, and economic capacity to influence such international processes on its own. Therefore, relying on the influence of European (particularly German) partners can be an asset.

Similarly, participating in international arms trade is expected to be particularly valuable, together with German companies or joint ventures, because more restrictive German arms export policies might offer windows of opportunity for exports through Hungary (even to crisis areas). Simultaneously, international competition puts pressure on newly established firms and projects, which can be balanced by good strategic foresight, identifying marketable products and new niche areas of technological development, and connecting with emerging markets. Whether these risks will be effectively tackled will only be seen in a couple of years as developments unfold and R&D and production expand.

9. Instead of conclusion: Outlook to 2030

When the comprehensive homeland defence and armed forces modernisation programme was launched in 2017,²⁷ its defence industrial pillar was to be built around the 2016 long-term national re-industrialisation strategy (Irinnyi Plan²⁸), which identified the defence industry (‘personal defence equipment, small arms, light armoured vehicles’) as a possible break-out area for Hungary among seven areas to be developed. Currently, the Research, Development, and Innovation Strategy for 2021–2030²⁹ serves as the backbone for initiating new defence industry projects through investment and partnership. The confidential Defence Industrial Strategy (2021), referred to earlier, was based on four pillars, each of which needs to excel to achieve the ambitious goals of the government on 1) actors, structures, processes; 2) innovation; 3) human resources; and 4) management.

The exact development areas and projects, as well as their respective partners, are outlined here with an outlook for 2030. Based on the agreements concluded during the first major phase of the Armed Forces Development programme (2016–2023), one can envision the main projects until the 2030s; in other words, actors, structures, and processes have been calibrated.

However, a general feature can be identified as a crucial area in which progress (and long-term success) clearly depends on Hungary’s weak

²⁷ Government Decree No. 298/2017 (02.06.2017).

²⁸ Drafted by the Ministry of Economy, endorsed by the government on 05.02.2016.

²⁹ Government Decree No. 1456/2021, replacing the R&D&I Strategy for 2013–2020 (Gov. Decree No. 1414/2013, adopted on 04.07.2013).

performance as an innovator. The 2023 European Innovation Scoreboard listed Hungary among ‘moderate innovators’, 21st among 27 EU member states in 2023 and at 70.4% innovation output compared to the EU average. However, this is already an improvement, as in 2021, Hungary was only assessed as an ‘emerging innovator’ (22nd in the EU), with 67.9% innovation output. Based on data from 2018, only 9.5% of (all) industrial companies in Hungary engaged in continuous innovation activities (compared to the 29.6% EU average), and only 28.4% conducted innovation occasionally (compared to the 53.1% EU average).³⁰ Unfortunately, no updated data are available on these aspects. However, this is inadequate if the ambitious goals outlined for 2030 are satisfied. Bringing high-tech defence enterprises with an innovation edge to Hungary (e.g. Rheinmetall) was successful, and the government introduced funding programmes tailored to the needs of SMEs to develop the national actors in the supply chain.

To provide a skilled and qualified workforce, tighter and deeper cooperation programmes with institutions of higher education, innovation hubs, and research centres have also been initiated. Of course, these will bear the first results in the next few years, and the competitiveness of the defence sector as an employer will remain in question.

Considering other internal and external–structural–risks associated with Hungarian defence industry development, the outlook to 2030 can be characterised as “high risk–high reward”.

³⁰ European Commission, 2023.

Bibliography

- [1] Budavári, K. (2021) '*A magyar védelmi ipar helyzete és fejlődési lehetőségei*' [The current situation and development prospects of the Hungarian defense industry], Budapest: Magyar Hadtudományi Társaság.
- [2] Csiki Varga T. (2023) 'A honvédelmi ágazat 2023-as rekord költségvetése és a NATO-kötelezettségek teljesítése' [The 2023 record expenditure of the defense sphere and the fulfilment of NATO commitments] *Stratégiai Védelmi Kutató Központ (Elemzések)*, 2023/1, pp. 1-9.
- [3] Csiki Varga, T., Lázár, Zs. (2021) 'Filling the two percent gap – An update on Hungarian defense spending trends' *Stratégiai Védelmi Kutató Központ (Elemzések)*, 2021/15, pp. 1-7.
- [4] Csiki Varga, T., Tálas, P. (2020) 'Magyarország új Nemzeti Biztonsági Stratégiája' [The new National Security Strategy of Hungary], *Nemzet és Biztonság – Biztonságpolitikai Szemle*, 13(3), pp. 89–112; <https://doi.org/10.32576/nb.2020.3.7>.
- [5] Guttray, L., (2018) '*Biztonságpiac Évkönyv*'. [Yearbook of the security market], Budapest: Biztonságpiac.hu Kft.
- [6] Hecker, F. (2022) '*Magyarországot választhatja a NATO*' [NATO may choose Hungary], [Online]. Available at: <https://www.vg.hu/vilaggazdasag-magyar-gazdasag/2022/01/magyarorszagot-valaszthatja-a-nato> (Accessed: 20 April 2024).

-
- [7] Huszák, D. (2023) 'Hamarosan Magyarországon gyárthatják Európa legmodernebb tankját' [Soon Europe's most modern main battle tank may start production in Hungary], [Online]. Available at: <https://www.portfolio.hu/global/20230830/hamarosan-magyarorszagon-gyarthatjak-europa-legmodernebb-tankjat-megvalaszoltuk-a-3-legegetobb-kerdest-636099> (Accessed: 20 April 2024).
- [8] Márkus, F. (2013) 'A kötelékben lévő lövészzászlóalj szervezeti és technikai korszerűsítésének lehetőségei a XXI. század elején' [The possibilities of institutional and technological modernization of an infantry battalion in the beginning of the 21st century], *Seregszemle*, 11(4), pp. 30–33.
- [9] Nádudvari, A., Etl, A., Bereczky, N. (2020) 'Quo vadis, Pesco? An analysis of cooperative networks and capability development priorities' *Stratégiai Védelmi Kutató Központ (Elemzések)*, 2020/15, pp. 1-27.
- [10] Szloszjár, B. (2017) 'Az integrált modell. A dandárképesség jövője – Mennyiség vagy minőség?' [The integrated model. The future capabilities of the brigade – Quantity of quality?], *Honvédségi Szemle*, 145(5), pp. 26–45.
- [11] Sticz, L., Seprődi-Kiss, Á. (2020) 'A Magyar Honvédség képességfejlesztése, egy korszerű haderő megteremtése' [Developing the capabilities of the Hungarian Defense Forces, creating a modern armed force], *Hadtudomány*, 30(4), pp. 3–19; <https://doi.org/10.17047/Hadtud.2020.30.4.3>.
- [12] Ternovác, Á. (2021) 'Egységes holdingba tömörül a magyar hadiipar' [Hungarian defense industry becomes united under one holding], [Online]. Available at: <https://magyarnemzet.hu/belfold/2021/12/egyseges-holdingba-tomorul-a-magyar-hadiipar> (Accessed: 15 April 2024).

- [13] Végvári, Zs. (2023) ‘Defense innovation in focus’, *Military Technology*, Special Issue 2023, pp. 74–77.
- [14] Budapest Főváros Kormányhivatala (2019) ‘*Tájékoztató a Haditechnikai és Exportellenőrzési Osztályok tevékenységéről*’ [Report on the activities of the Departments of Defense Industry and Exports Control], [Online]. Available at: https://www.sipri.org/sites/default/files/2021-11/hun_2019.pdf (Accessed: 20 April 2024).
- [15] Defense Industry Association of Hungary (2023) *Hungarian Defense Industry 2023*, pp. 184–185.
- [16] European Commission (2022) ‘*European Defense Fund 2021 Calls for Proposals – Results*’, [Online]. Available at: https://defence-industry-space.ec.europa.eu/funding-and-grants/calls-proposals/european-defence-fund-2021-calls-proposals-results_en (Accessed: 20 May 2024).
- [17] European Commission (2023) ‘*European Innovation Scoreboard*’, [Online]. Available at: <https://op.europa.eu/o/opportal-service/download-handler?identifier=04797497-25de-11ee-a2d3-01aa75ed71a1> (Accessed: 20 May 2024).
- [18] European Commission (2024a), ‘*Results of the EDF 2023 Call for Proposals*’, [Online]. Available at: https://defence-industry-space.ec.europa.eu/funding-opportunities-0/calls-proposals/results-edf-2023-calls-proposals_en (Accessed: 20 May 2024).
- [19] European Commission (2024b), ‘*ASAP results: Boosting ammunitions production*’, [Online]. Available at: https://defence-industry-space.ec.europa.eu/document/download/b694b109-fa2c-493e-bf1e-87768ae6469e_en? (Accessed: 20 May 2024).
- [20] NATO (2024) ‘*Defense expenditure of NATO countries (2014-2023)*’, [Online]. Available at: https://www.nato.int/cps/en/natohq/news_223304.htm (Accessed: 15 April 2024).

KARL-HEINZ GIMMLER*

Constitutional and European legal rules for armaments' quality and presentation of alternative procurement: Contribution to the possibilities of contractual optimisation in armament procurement (the contract as a force multiplier)**

ABSTRACT:

1. War is a legally relevant hazardous situation with potentially incalculable human casualties in terms of life and limb, especially of the soldiers in action. This dangerous situation is comparable to a nuclear power plant meltdown.
2. Many European states have a constitutional obligation (not examined in detail). For example, the Federal Republic of Germany and Austria must qualitatively optimise armament for the purpose of protecting the fundamental rights of soldiers who may be fighting.
3. This obligation exists throughout the EU based on the CFR and the jurisdiction of ECHR, in the rank of ordinary statutory law.
4. Armament procurement is also a legal subject for multidimensional optimisation under numerous legal aspects, in particular the choice of contract type, price optimisation, and tax optimisation. Therefore, it should (finally) be considered multidimensionally for the benefit of the defence of freedom in EU-Europe and NATO as a whole.
5. The procurement of defence equipment must contractually enable the core objectives of the state, namely secure availability, sustainable defence equipment, and cost-effective procurement. To this end, hundreds of individual contractual clauses and regulations must be used.
6. Rental and leasing contract procurement is generally more cost-effective and otherwise offers no disadvantages compared to traditional purchase procurement. All conceivable disadvantages can be contractually prevented and avoided. Specific unavoidable

* PhD, lawyer, Koblenz, Germany. <https://orcid.org/0009-0009-4276-3667>, k.gimmler@gimmler-gruppe.com.

** The research and preparation of this study was supported by the Central European Academy.

disadvantages are practically not recognisable. It is a suitable “force multiplier and defence enabler.”

7. Optimised contractual arrangements, particularly other contract types and VAT optimisation, can save at least tens of billions of euros per year in the whole EU-Europe.
8. Due to the lower impact on the annual budget, more and/or better quality of armaments can be procured.

KEYWORDS: Armament – Constitutional obligation for optimized armament, Fundamental rights of soldiers, Optimized modes of procurement, VAT optimization modes.

1. Introduction: Military operations and legal requirements for armament decisions

This study deals with the eternal question of the relationship between military armament in the broader sense and the legal system. This relationship has only entered the realm of legal consideration since the increasing validity of fundamental rights. Earlier approaches went in other directions; for example, the book *Gericht über Habsburgs Wehrmacht*¹ does not actually deal with a legal assessment but a more overall political evaluation.

Methodically, the factual basis of the relevant branches of science, especially history of war and its relation to technological progress, must be carved out, and conclusions must be shown to create binding legal rules for armament policies and procurement decisions in democratic constitutional states.

In other words, the aim is to examine the extent to which legal obligations exist for armament decisions and thus to what extent these are removed from free political evaluation, by applying the broad constitutional review density applicable in the European Union (EU) and non-European North Atlantic Treaty Organization (NATO) states. To this end, the military factual basis to be taken as a foundation will first be established by going back through history; then, the legal standard of review will be determined and practical application criteria developed. Finally, the armaments sector is examined as a comprehensive area open to contractual optimisation using

¹ Regele, 1968.

the example of alternative arms procurement channels. In addition, value-added tax (VAT) optimisation is considered as a “mosaic stone example.”

2. The factual basis: In search of superiority. *Tour d'horizon* to war—history and contemporary history or how to win a war and survive

2.1 Journey through the history of war and current operational events to establish the factual basis

We describe and analyse selected historical situations that focus on modern history, which is considered as the whole history of war; this is because thousands of years and ages could be analysed and situations could serve as examples. Therefore, we do not focus on the historical events but rather analyse the conflicts, battles, victories, and defeats from a single point of view: To what extent does better equipment in terms of position lead to victory in the broadest sense, and what effect does this have on the loss ratios? In short, how do you win a battle and survive? Is there an established relationship between victory and survival, and is there perhaps even a mathematical correlation?

This analysis takes us to selected locations in the history of war right up to the present day, and it naturally makes special reference to combat troops of the army and air force, and some examples from the field of naval armaments are also covered. Our aim is identifying factors of military superiority in specific operational situations and the consequences for the fighting soldiers. In doing so, we are primarily looking at duel situations—that is, battle tank against battle tank and aircraft against aircraft—but also the substitutional possibilities. This signifies that a certain weapon, a certain means of combat, can be eliminated by another suitable means of combat. Prime examples of this are the mass deployment of anti-tank armour using shaped-charge projectiles and today, of course, drones.

Let us begin our journey in the German western campaign of 1940: the German “Panzer II, III, and IV” or the (Czech) 38 t were neither qualitatively nor numerically superior to the Allied tanks. However, they were led with a better operational doctrine, particularly the concept of concentration and rapid deep penetration. Guderian’s principle of “*nicht kleckern, sondern klotzen* = no frittering, but concentration” is just as important as “small” technical advantages, such as equipping each vehicle with radio. However, these advantages only unfolded their full effect through the inadequate actions of the French and British, who viewed the

tank as an infantry support weapon. Here, the better operational doctrine of the German side, in terms of both strategy and tactics, proved to be a decisive edge.

Let us now turn to Normandy after D-Day in 1944, when the British and Americans used the Sherman tank as the standard tank during the invasion. The experiences from the African and Italian campaigns from the end of 1942 are confirmed once again: 5–10 Sherman tanks were reckoned to be a match for one German “Panther” or “Tiger” in the deadly hedgerow landscape of Normandy. What is the reason for this technical superiority? In addition to the war experience and good training of the crew, particularly because of the mix of effective and protective technology, the long 7.5-cm L/70 cannon with a V0 of 1020 m/s had extreme penetrating power, as did the 8.8-cm cannon of the “Tiger” heavy battle tank. At the same time, both main battle tanks had good protection concepts thanks to strong armour.

The 1973 Yom Kippur War between Israel and some Arab states and the countless losses of tanks, some of which were still Second World War tanks, had a direct influence on Western tank armament: It led to a complete revision of the protection concept of the German “Leopard 2,” for example, thus indirectly influencing the entire new generation of tanks in the west.

This tank generation made its grand debut in the Iraqi desert during the 1991 Gulf War: Iraq’s numerically strong armoured forces, more than 4,200 battle tanks, consisted mainly of superficially modernised T 55s, T 64s, and T 72s from Soviet production. Until recently, this was the standard equipment of the former Eastern Bloc states, including Hungary. Several hundred T 72 tanks are still in service there today and are gradually being replaced by the Leopard 2.²

In Iraq, the outdated Soviet tanks were fitted with additional armour (for a relatively high price) and equipped with infrared night-vision devices with a range of up to approx. 1,000 m. Overall, this was as expensive as it was ineffective. A Latin principle applies here: *Non faciunt meliorem equum aurei freni*, meaning golden reins do not make a horse better. Tanks prove to be real coffins for their crews in all operational scenarios, not just classic tank battles. Whether the kill ratio in tank-to-tank combat is around 1:500 or 1:1000 (depending on the source) is ultimately an almost academic question. What is certain is that the Iraqi tanks had virtually no chance against the

² Wikipedia (2025) Ungarisches Heer, [Online]. Available at: https://de.wikipedia.org/w/index.php?title=Ungarisches_Heer&oldid=250281587 (Accessed: 06 March 2025).

well-managed, well-trained, provided with good logistics, technically state-of-the-art battle tanks of the main coalition states, namely the M1, Challenger II, and Leclerc. The Iraqi tanks were simply inefficient and the concept ineffective. Lesson: class instead of mass! From a commercial point of view, the Iraqi armoured fleet was simply pointless, as 500 or 1,000 battle tanks, even of an older generation, were far more expensive overall than a few modern battle tanks.

Let's leave the world of classic symmetrical battles and move on to asymmetrical warfare, with Iraq and Afghanistan after 2003 up to 2021 as examples.

A comparison of the susceptibility to loss and thus the frequency of casualties when using certain armoured vehicles, for example of the Canadian armed forces, is particularly suitable here. The Americans, followed by the Canadians, partially implemented the new doctrine of replacing the main battle tank with by a lightly armoured weapons platform for variable weapon systems. This concept is a "grandchild" of the German assault gun concept from the Second World War with its variants, such as the "Bison" self-propelled gun with a 15-cm infantry gun. This vehicle could be confused with a mechanised infantry combat vehicle or armoured infantry fighting vehicle, but actually it is materially a different concept. This, the so-called "Stryker," carries variable armament up to a 105-mm cannon. German General Willmann's catchy and apt phrase, "*leicht rein, tot raus* = easy in, dead out," is misunderstood here. However, in asymmetrical combat operations, numerous vehicles are lost, and the crews are killed and seriously wounded. The Canadians soon made a spectacular decision: The Strykers, which were extremely vulnerable to anti-tank fire — such as RPG 7 rocket-propelled grenades in Afghanistan — were replaced by German Leopard 2A6Ms with additional mine protection.³

After four years, the Canadians were convinced of the effectiveness of the Leopard 2A6M as a "combat multiplier." In particular, both the better protection technology and the effect of the long 120-mm cannon with new, situation-appropriate ammunition (e.g. shrapnel up to 4 km) are emphasised. However, it must be mentioned that heavy armour technology is no guarantee of success: Turkey did indeed suffer several losses of Leopard 2A4s in the operation against the Islamic State, although these were probably also deployed in a tactically suboptimal manner, such as for terrain

³ Cadieu and Adams, 2010, p. 32.

surveillance. A main battle tank is an ideal target in terrain suitable for ambushes.

The current game changer is, of course, drones of all kinds, and they already come in a variety of types and scenarios that are historically unparalleled in terms of speed: From unmanned aerial vehicles to unmanned ground systems, earth-bound drones, and unmanned marine systems, the family of military drones is growing at a more than rabbit-like rate.

2.2 Evaluation of our journey: Causes of superiority, victory, and survival

Let us be clear: Superiority can result from a wide variety of factors, from a correct assessment of the situation to optimised operational principles, tactics, and strategies as well as good training. However, *technical superiority* is always important. Some situations in war history are the best examples for this hypothesis.

In the 1991 Gulf War, the western coalition lost 31 tanks, most of them by “friendly fire,” and the Iraqis lost 3,300 tanks. Thus, the ratio was 1:100.⁴ The casualty ratio of human losses, that is, killed or wounded soldiers, was nearly 1:100 too. This ratio is valid under the assumption that the crew of a battle tank comprises four soldiers. So the calculation is that nearly 12,000 Iraqi soldiers were killed or heavily wounded.⁵

The Canadian Armed Forces’ replacement of the Stryker in Afghanistan by the Leopard 2A6 brought an immediate result: There were no human losses any longer.⁶ Thus, superiority means survival.

As will be shown later, this is also the reason why, considering the basic rights of the soldiers concerned, a quantitative view is ruled out as the cause of victories. This means that you win despite an inferior weapon because you are outnumbered 10 to 1, but this means that you accept

⁴ Wikipedia (2025) Gulf-War, [Online]. Available at: https://en.wikipedia.org/wiki/Gulf_War and U.S (Accessed: 13 January 2025); U.S. Army Center of Military History (2021) Operation DESERT STORM in history army mil [Online]. Available at: <https://www.history.army.mil/html/bookshelves/resmat/desert-storm/index.html> (Accessed: 20 November 2024); Roos, D. (2023) How Tanks Played a Critical Role in the Persian Gulf War in history.com, [Online]. Available at: <http://www.history.com/news/tanks-abrams-persian-gulf-war> (Accessed: 03 January 2025); ‘1991: Sturm auf Kuwait’ (2019) in Schweizer Soldat [Online]. Available at: <https://www.schweizer-soldat.ch/2019/04/1991-sturm-auf-kuwait.html> (Accessed: 16 April 2019).

⁵ Thorne, 2015, p. 523.

⁶ Cadieu and Adams, 2010, p. 32.

numerous losses, such as five or six weapons, and then win. In other words, victory is gained through high losses of men and material. Incidentally, this is the astonishing and inhumane concept of the Russian army in Ukraine. They are trying to take Ukrainian defensive positions by storm with ruthless, frequent quantitatively superior attacks, which sometimes succeed with extreme losses. Section 4.2.2 ends with a deeper discussion on why it is unacceptable to compensate for inferior armour with human sacrifices. The following principle applies: *non multa, sed multum*, or quality instead of quantity.

Protection technology and effective technology suitable for the situation are equally important here. It is always difficult to win in specific deployment scenarios with inferior, outdated equipment, unless it is replaced by other superiority factors.

2.3 Detailed findings on superiority, particularly technical superiority

Briefly summarised here are some historically proven superiority factors in terms of the “eternal” military experience, facts⁷ of victory, and survival on the battlefield:

- Tactical and strategic surprise leads to victory.
- Superiority in key dimensions, especially better armament, leads to victory.
- Inferiority in key dimensions leads to defeat and death.
- Optimised active and protective armour is dynamic in time — it becomes obsolete.

Disrespecting these facts is *wrong*, not *justifiable*, and not the discretion of politicians. Such an approach is *falsified* based on the prevailing scientific theory of critical rationalism and the related method of statistical significance tests as equivalent methods of hypothesis testing.⁸ This scientific theory is of course only prevalent in democratic free states.

As this is the most tangible aspect, the following section essentially focusses on technical superiority and technical assessment. These aspects are hard facts. In comparison, tactics, strategy, and training are soft factors that are less easily accessible for assessment.

⁷ ‘1991: Sturm auf Kuwait’ (2019) in Schweizer Soldat [Online]. Available at: <https://www.schweizer-soldat.ch/2019/04/1991-sturm-auf-kuwait.html> (Accessed: 16 April 2019); Thorne, 2015, p. 523.

⁸ Bortz et al., 2002, p. 22, 26.

2.4 Differences in the causes of technical superiority: Linear and disruptive developments

For technical developments, especially in the case of development of armament, there are two basic lines of development.

The first is “organic,” evolutionary development: A basic weapons system is constantly being improved. Many small improvements simply make older models obsolete and less effective. For example, the Leopard 2 main battle tank of the German Bundeswehr and many other nations has been improved continuously since 1979, and the first examples would have died out “evolutionarily” today.⁹

Especially in the case of evolutionary developments, the sometimes-astonishing longevity of armour material must also be considered. In this respect, the so-called platform concept applies. A good armour platform — for example, the original model of the Leopard 2 main battle tank — must be constantly developed further with regard to obsolescence, that is, ongoing obsolescence. This results in a service life of around 50 years for evolutionary platforms; for example, see the “Marder” infantry fighting vehicle or fighter aircraft such as the American “F-16” or even the “B52” heavy strategic bomber of the US Air Force. The latter has now reached a proud 72 years, of course with hundreds of updates and further developments.

On the other hand, there is disruptive development: Some examples are the global positioning system used in the 1991 Second Gulf War and the development and implementation of the Dreadnought battleships in the years after 1904¹⁰ in the royal navy, which obsolesced all formerly build battleships. The Shaped Charge Bazooka had an impact wherein all steel-armoured tanks became very vulnerable. The latest example is the nearly total overuse of military drones (unmanned aerial vehicles, unmanned ground systems, and unmanned marine systems) in the Russia-Ukraine war.

These developments *end* another line of development and no longer allow the organic evolutionary development of the predecessor systems. Of course, there are also revolutionary developments within continued evolutionary lines of development that make certain features irreversibly obsolete. These developments have the character of technology-driven “revolution in military affairs” with fundamental effects on tactics and even

⁹ Von Crevel, 1991, p. 311.

¹⁰ Potter and Nimitz, 1974, p. 295.

strategy. A prime example of this is the pure “steel tank,” which has no longer been the basis for tank technology since the compound armour became established. In other words, those who deny this disruptive, revolutionary development and do not immediately convert their armour will lose.¹¹ The principle of *numquam retrorsum*, or never go back, applies.

3. Superiority, threat, and public law, especially constitutional law

3.1 Threat prevention and public law

We have found that the use of a technically superior weapon system, whether in duel situations or other missions appropriate to the situation, generally increases the probability of success. This is true if training, tactics, mission doctrine, etc., are also adequately good. Victory in a duel situation (tank against tank) or in other operational scenarios is therefore considerably more likely. In other words, inferior equipment exponentially reduces the chance of leaving a battle alive (and ideally as a winner).

In terms of specific consequences for armament and equipment decisions for troops in the field, modern equipment, particularly the “best” protection and effective technology based on state of the art in science and technology, is clearly the main measure that minimises risk based on scientific findings and concrete operational experience.

This statement is an established empirical finding in a wide range of relevant empirical disciplines. These include the history of war; operations research; and stochastics with, for example, so-called Monte Carlo simulations. Complex military simulation and training programmes are based on stochastic and operations research methods and models. One thing is always certain: The better a weapons system and the better the soldiers operating it and the environment, the better their chances in battle and the higher the chances of winning in combat. However, this also simply means surviving.¹²

Let see some examples for explanation. It remains to be seen to what extent the deterioration in chances can be expressed in powers of ten (1:10, 1:100) based on the experience of recent decades with regard to the effect of

¹¹ Wikipedia (2025) Jom-Kippur-Krieg, [Online]. Available at: <https://de.wikipedia.org/w/index.php?title=Jom-Kippur-Krieg&oldid=251395776> (Accessed: 16 January 2025).

¹² Dupuy, 1980; Macksey, 1986. For scientific utilisation, see also Jarausch, Arminger, and Thaller, 1985.

an (evolutionary) generational leap or a disruptive development in combat-critical large-scale equipment (e.g. the leap from the “T 62/T64/Leopard 1” generation to the “M1/Leopard 2”). What is certain, however, is, that there is at least a high probability of this happening and that there will be a significant change in the probability of success and survival. However, one thing is beyond doubt: the superiority of a tactic or even a weapon system, especially with regard to the protective and effective components, must always be assessed in relation to time. While the “Panther” main battle tank was a superior weapon system in the Second World War, it was hopelessly outdated just a few years later. In this context, effective and protective technology should be mentioned as complementary technologies that can only be substituted by other factors to a limited extent: the Stryker certainly had good effective technology, but the protection was too weak.

Of course, it should not be denied here that a duel situation is not the standard case in the battle of combined forces and cannot be used without restriction.

Complete weapon systems can be completely or partially replaced by other weapon systems, for example, anti-tank defence can also be provided by precision artillery and other weapon systems instead of tanks, at least in part. The only decisive factor is that the effective and protective technologies are optimized for the situation. In other words: if I have to fight without an adequate weapon system, an adequate substitution decision must be made.

What does all this mean for the crews of the combat vehicles, for the soldiers? The example of the Iraqi tanks or infantry fighting vehicles that were destroyed makes this drastically clear: the firing ratio of 500:1, for example, also means that an Iraqi tank or armoured infantry soldier had a 1:500 chance of survival compared to an American tank soldier in an M1 Abrams tank, i.e. a fight *usque ad finem* - to the bitter end.

What does the special nature of asymmetric warfare mean for the question of superiority? Is everything different there? The answer is a clear no. It is true that there are numerous special features, such as guerrilla warfare, suicide attacks, etc. In particular, this also includes the lack of compliance with the rules of international law of war, a prime example being the Geneva Convention and supplementary agreements. However, the decisive factor for the question of superiority is also here: if a suicide becomes “pointless”, i.e. does not lead to the intended effects, it is better not to commit it. The effect is of course also the psychological effect on a “zero-

loss” society like ours. In view of the effect, even a single victim can be seen as the success of a suicide attack. As always, the question of establishing the appropriate superiority for the situation arises here, only with slightly different answers.

Just to summarize an essential conclusion: being superior in combat, especially with regard to the weapon system, results in an exponentially higher probability of survival. In negative terms: an exponentially lower probability of death or serious injury. In other words, the risk of being killed or wounded in action is greater, usually exponentially so, if the most appropriate equipment is not used (this does not always have to be the latest, see the partial misdevelopment of the “new” Stryker!) in terms of protection and weapon effectiveness combined with the best training for soldiers, operational logistics and tactics. To deny this would be, due to the basis of scientific findings just as wrong as to deny that cancer, for example, is a life-threatening disease. It would be just as wrong to deny the threats of the peaceful use of nuclear energy.

3.2 Legal relevance of the “superiority and threat” relationship

Superiority, especially technical superiority, means minimising the threat for humans. The relevant legal aspects of these identified threats and reduced opportunities now arise from the fundamental rights of people: Threats to material are practically legally irrelevant in this respect. The subjects of fundamental rights are people—in this case, soldiers. This leads to the legal instrument of threat prevention, based on both police law and other security-related legal areas.

Military operations above a certain intensity are dangerous and are subject to risk assessment. What definition of threat do we use for this? The definition used here under police law is as follows: A threat in the sense of police law exists if there is sufficient probability of damage to an asset protected by the police if things proceed unhindered.¹³ The intensity of the damage can vary just as much as the probability of the damage occurring. Incidentally, this definition is also used in foreign security and policy as well as business risk management.¹⁴

¹³ BVerfG, 2020. The Federal Constitutional Court (Bundesverfassungsgericht) has specified the requirements for danger in the context of police measures and emphasised the balancing of fundamental rights (1 BvR2795/19); Dietlein, 2022.

¹⁴ Gleißner and Romeike, 2005, p. 27.

In terms of threats to European and NATO soldiers, the risk of being seriously wounded in a lightly armoured vehicle or on infantry patrol, for example, must be assessed on a completely different probability basis depending on the intensity of the mission. Taking an example, if the risk in a mission in Kosovo or Bosnia-Herzegovina is relatively low in the context of the Kosovo Force and not significantly greater than that when serving in Germany, then the risk in Afghanistan is considered significantly higher. Moreover, the risk has increased immensely in Ukraine since 2022 or in the war between Armenia and Azerbaijan — the first real drone war. In other words, the risk of being killed or seriously wounded there is high. This is particularly evident in the most recent war — the Gaza war against Hamas from 7 October 2023. If we now apply the insight that better equipment, and particularly the availability of equipment appropriate to the situation on the ground, reduces risk, the best example is of the Canadian troops in Afghanistan: While the weapon carrier concept resulted in numerous dead and wounded (in addition to the destroyed weapon carriers themselves), this rate fell exponentially when the Leopard 2A6 with superior effective and protection technology was adopted — in addition to increasing the probability of success in the specific deployment scenarios.¹⁵ There were no more casualties, and the number of wounded fell rapidly.

Not only the Canadians have experienced this, but so have the British, American, and Dutch allies.

4. Armament quality and European legal and national constitutional law through the example of Germany

What does this mean in terms of constitutional law?

4.1 Legal regulations examined: National constitutional law, using Germany as an example, and European regulations

This section examines national constitutional law, taking Germany as an example, as well as EU law and European treaty law such as the European Convention on Human Rights (ECHR). This because the latter applies in all EU Member states, in some cases as constitutional law, such as in Austria.¹⁶

¹⁵ Cadieu and Adams, 2010, p. 32.

¹⁶ Gimmmler, 2017b, p. 628, 633.

The following analysis is based on the German Basic Law—the German constitution. However, the principles are applicable in all European states due to the ECHR, which applies throughout the EU.

German constitutional law is chosen for various reasons: First, the author of this study is German and has studied German law, which is why it is most familiar. Moreover, the German Federal Constitutional Court is probably the most active and the constitutional court with the most decisions in the EU, with more than 166 volumes of decisions.

4.2 Examination of the legal situation and the relevant jurisdiction in Germany

4.2.1 General constitutional regulations

The Basic Law contains provisions on defence and external security in various articles, such as Article 12a on compulsory military service, Articles 87 a and b on the establishment of armed forces and the separation of military administration and troops, Articles 24 (2) and 26 on alliances and the prohibition of aggressive war, and particularly Article 115 ff on the case of defence.

However, none of these constitutional norms make any *direct* statements on the material quality of armaments or deployment-related decisions. Nevertheless, the Federal Constitutional Court has repeatedly pointed out that the Basic Law has made a basic decision for effective national defence in this respect.¹⁷ However, these articles do not help us in our concrete assessment. Yet, the decision of the Federal Constitutional Court on Article 24 of the Basic Law contains a very important statement: The fact that Bundeswehr is mentioned in the German Constitution means, that it must also be operational.¹⁸

4.2.2 Relevant Article 2 (2) of the Basic Law: The Federal Constitutional Court's case law on threat prevention

First, we must assert, that — as in probably most countries of the world — there are no special regulations for threat prevention, which must always be

¹⁷ BVerfG, Dienstpflichtverweigerung (1 BvR 83, 244, 345/69).

¹⁸ BVerfG, 1978. Wehrpflichtnovelle (2 BvF 1, 2, 4, 5/77); von Mangoldt, Klein, and Starck, 2010, p. 1.

checked methodologically. As with many other constitutionally relevant issues, no ruling has yet been issued on the specific question at hand regarding the quality of the military equipment and other decisions. However, in its ground-breaking decision on the NATO Double-Track Decision and its implementation in Germany, the Federal Constitutional Court clearly stated the following:

Assessments and evaluations of a foreign and defence policy nature are the responsibility of the Federal Government. The Basic Law only limits the power of assessment to which the Federal Government is entitled in this respect to obvious arbitrariness. Within these extreme limits, the Federal Constitutional Court does not have to review whether the assessments or evaluations of the Federal Government are correct or incorrect, as there is a lack of legal standards in this respect. They are to be decided politically.¹⁹

This is a throwback to the famous political question regarding the theory of the US Supreme Court from 1803—over 200 years ago. Therein, the US Supreme Court ruled in the case of *Marbury v. Madison*²⁰ that political questions cannot be decided by law.

These statements fully endorse and provide decisive support for the view expressed here.

The aforementioned decision, as well as the decision on the admissibility of the storage of chemical weapons in Germany²¹ and other similar decisions, were always based on the following argumentation: The applicants requested the Federal Constitutional Court to determine the ‘unconstitutionality of a certain decision to act’. In this case, the Federal Constitutional Court was presented with a specific theory or a conclusive train of thought regarding a threat.²² For example, in the case of the NATO rearmament decision,²³ this was the idea of ‘a significant increase in the threat posed by provoked Soviet countermeasures’.

¹⁹ BVerfG, 1985. NATO-retrofitting decision. (2 BvE 13/83).

²⁰ US Supreme Court Center, 1803, *Marbury/Madison* (5 US 137 (1803)). Justia US Supreme Court.

²¹ BVerfG, 1987. Lagerung chemischer Waffen (2 BvR 624, 1080, 2029/83).

²² BVerfG, 2010. “Cern” decision (2 BvR 2502/08).

²³ BVerfG, 1985. NATO-retrofitting decision. (2 BvE 13/83).

The application of this line of thought would have resulted in unconstitutionality of the contested measure in each case.

Here, the Federal Constitutional Court has always wisely exercised restraint and, in line with the scientific theory of “critical rationalism”²⁴ that prevails in western democratic constitutional states, has stated the following: A Constitutional Court does not have to determine which theory is more correct when there are several possibilities.²⁵ We must not substitute our own court-opinion for that of the politically responsible decision makers. *We do not have to verify, but we have to falsify as far as we can.* Only if something can be declared as false can it be investigated. Only then does the Federal Constitutional Court have to declare the measure as null and void. This is because there is a so-called high level of scrutiny in this respect; otherwise, only an “arbitrary review” takes place, which is a review to determine whether a decision was made by disregarding objective reasons.

As is so often the case, very tangible, concrete constitutional requirements for armament and deployment decisions arise from the state’s duty to protect fundamental rights—and this is one of the merits of the early environmental movement with its fight against nuclear power plants. The decisive factor here is Article 2 (2) sentence 1 of the German Basic Law: ‘Everyone has the right to life and physical integrity’.

For decades, the German Federal Constitutional Court has developed the following principles and relevant lines of decision from this simple sentence in constantly expanding case law: The state is obliged to protect human life in all its sovereign manifestations—the so-called objective duty of the state to protect.²⁶ Using the example of nuclear energy, this means that extreme efforts must be made, such as through extremely strict safety requirements, to prevent nuclear accidents, even if they have a probability of less than 1:1 billion. The state is therefore obliged to apply extreme safety standards when approving and monitoring nuclear power plants.

Even in the case of life-threatening illnesses (e.g. cancer), public health insurance funds are obliged under certain conditions under Article 2 para. 1 sentence 1 of the German Basic Law to cover non-standard therapies and possibly spend six- to seven-figure sums.²⁷

²⁴ Popper, 1994, p. 16.

²⁵ BVerfG, 1985. NATO-retrofitting decision. (2 BvE 13/83).

²⁶ BVerfG, 1998. Cassini-Weltraummission-Entscheidung. (1 BvR 1908/97).

²⁷ BVerfG, 2009. (1 BvR 316/09).

The intensity of the protective measures to be taken against hazards is mainly determined by the extent of the conceivable occurrence of damage. The more intensive the hazard, the greater the requirement for protective measures. Using the example of nuclear energy, a major accident would pose a fatal threat to an extremely large number of people, however unlikely it may be. Intensive protection must therefore be provided against it. Conversely, if no significant intensity of damage can be determined, no special protective measures are required.

Regarding security-related case law, the so-called Schleyer decision of 1977 was ground-breaking in this respect.²⁸ According to this decision, the state has a duty, even in terrorist kidnapping cases, to do everything possible to avert the threat to life and limb caused by unlawful acts by third parties. However, even in these cases — particularly in cases of blackmail and demands for the release of prisoners — the state has discretionary powers. Only rarely are individual specific measures the only possible measures. However, the so-called final kill shot may be the only permissible and necessary option in hostage-taking cases.

What is important here is that it is usually taken for granted that there is a considerable threat based on life experience or scientific knowledge: Cancer is a life-threatening disease from a medical point of view, and a serious terrorist abduction poses a threat to the life of the abductee. It has been scientifically and historically proven that nuclear energy poses considerable threats. It has a high hazard potential, even if there is no high probability of damage occurring (with optimum safety measures). This is based on clear empirical and/or scientific findings. Any other assessment would be inadmissible and therefore incorrect and legally void.

It is important to mention the most recent so-called climate decision of the Federal Constitutional Court of 24 March 2021.²⁹ Herein, the Federal Constitutional Court expressly established and affirmed the state's obligation to protect life from the threat of physical harm caused by negative climate developments ("climate catastrophe") and assumed extensive duties of protection on the part of the state. The state's duty to protect as an objective legal duty also includes the duty to protect against the threat of climate change. This objective duty to protect on the part of the state corresponds to a subjective right to protection on the part of the citizen. In particular, fundamental rights also provide subjective legal protection as

²⁸ BVerfG, 1977. Schleyer decision. (1 BvQ 5/77).

²⁹ BVerfG, 2021. Urteil (1 BvR 2656/18).

an intertemporal safeguard of freedom against risks being shifted into the future. It is not widely known that there is already a long-standing precedent ECHR case law in this regard,³⁰ which recognises preventive protection against life-threatening environmental disasters.

The latter decision can be applied one-to-one to the risk of armed conflict and, since 2022, also to the risk of a war of aggression against EU/NATO Europe: Against a life-threatening situation such as a major attack on EU Europe, the climate catastrophe is likely to be regarded as triviality in the foreseeable future.

However, for the questions raised here, this means that there are clear empirical or experiential standards, namely reliable findings and life experience. This is comparable to the above-mentioned examples, such as case law on nuclear power plants and cancer treatment. The knowledge is just there—*Superiority means minimising threat*, and the path is rocky but rewarding: *per aspera ad astra*.

All of these aspects were also impressively applied and confirmed in another decision of the German Federal Constitutional Court on security, this time in the field of nuclear physics research in the so-called “CERN” decision of 18 February 2010.³¹ In this case, a German applicant, referring to a scientific theory of a few nuclear physicists who regarded the CERN nuclear physics laboratory in Switzerland as a potential “doomsday machine,” had turned to the Federal Constitutional Court with an application to take the necessary measures for Germany to prohibit the commissioning of CERN. Most experts disagreed and saw no particular potential threat. The Federal Constitutional Court simply refused to play the role of “arbiter of physics” here and made it clear that reliable findings are required to arrive at an assessment of the risk and not to determine the risk situation merely by asserting the threat of major damage.

The following applies to the military sector based on obvious multi-disciplinary findings: The serious threat situation as such is evident, obvious, and undeniable. In view of these considerable threats, the political and military scope for assessment is now narrowing towards an intensification of the legal duty to protect.

Only decisions that correspond to empirical and scientific findings are permissible within a certain range. A practical example is as follows: Suppose that a decision was made under the rule of German constitutional

³⁰ ECHR, 2004.

³¹ BVerfG, 2010. “Cern” decision (2 BvR 2502/08).

law; then, the Canadian government's decision to replace the lightly armoured weapon carrier with the heavily armoured Leopard 2A6M, which "guarantees" survival of the crew, was a correct political/military decision. Whether this decision was the only possible one is an open question. Given the intensity of combat and the specific combat situations in southern Afghanistan, sticking to the "superficially" cheaper ("money before lives") weapons carrier concept would have been simply wrong and therefore illegal. Another typical example was the temporary failure to modernise the night-vision equipment for the German "Marder" armoured personal carrier and mine protection for the "Dachs" armoured engineer vehicle due to a lack of funds. This was simply unconstitutional according to the principles developed.³²

This also explains why the concept of inferior (in terms of the individual weapon) mass armament (mass instead of class) is inadmissible, as the lack of quality is compensated for by the human sacrifice of soldiers. A prime example in this respect is the armament of the Allies in the Second World War (Sherman versus Tiger) or the First Iraq War, albeit unsuccessfully. Under the rule of fundamental rights, money and thus a lack of armament quality cannot be replaced by human sacrifice.

Thus, the German Federal Constitutional Court summarised the following in one decision about using nuclear power plants: The more intense the possible encroachment on the right of life, especially because of the existing risk of death, the greater the duty to protect.³³

4.3 European regulations: Article 2 ECHR and Articles 2 and 3 EU Charter of Fundamental Rights

Due to the almost identical wording of Article 2 of the German Basic Law and Article 2 of the ECHR alone, the legal situation under European Law can be assumed to be the same as in the German Constitution. Furthermore, the Charter of Fundamental Rights of the EU (CFR) under the primary European law applies; according to Articles 2 (1) and Article 3 of the CFR, 'Everyone ... the right to life', and according to Article 3, para. 1 of the CFR, 'Everyone has the right to physical and mental integrity'. Moreover, the wording of Article 2, para. 1, sentence 1 ECHR is 'Everyone's right to life shall be protected by law'.

³² Steinmann, 2012, p. 9

³³ BVerfG, 2008. Atomausstieg (1 BvR 2821/11, 321, 1456/12).

In Austria, the ECHR is a constitutional law, that is it has constitutional status.³⁴ In Hungary, Articles 1, 2, and 5 of the Constitution of 8 April 2011 have constitutional rank and similar regulations. The ECHR is considered an ordinary statutory law in Hungary. These principles should therefore also apply to Hungary.³⁵

The non-European NATO countries of the United States and Canada are constitutional democracies with a wide range of constitutional human rights; therefore, these principles are valid and more or less similar. This is also indicated by the United Kingdom (UK) Supreme Court's decision of 2013,³⁶ as the UK belongs to the same Anglo-American legal sphere. The European Court of Human Rights has substantiated the right to life in numerous decisions.³⁷ For example, it has expressly established the protection of the entire population as well as of individuals or groups of individuals. This applies if there is a threat of injury from a third party, the prime example being acts of war by aggressors.³⁸ In particular, organisational fault can also be considered if forward-looking, future-oriented, and adequate planning, organisation, and equipment are neglected.³⁹ For EU-Europe, the Treaty of Lisbon is the third independent treaty under primary law and therefore has constitutional status. The CFR binds the EU and states insofar as they apply EU law.⁴⁰

4.4 Application to the special status of the soldiers in NATO/EU armies

Soldiers are obliged to accept risks to life and limb as part of their military service, particularly as a result of their duty of valour under Section 7 of the German Soldiers' Act. However, the soldier is not deprived of his fundamental rights under Article 2 para. 2 sentence 1 of German Basic Law.⁴¹ Like any other citizen, he is entitled to protection from interference by third parties. The ECHR has also expressly considered so-called special legal relationships such as military service to be subject to special protective

³⁴ Gimmler, 2017b, p. 628, 634.

³⁵ Gimmler, 2017a, p. 172.

³⁶ UK Supreme Court, 2013, Smith and others v. MOD (41/2013) p. 1.

³⁷ Karpenstein and Mayer, 2015, p. 36.

³⁸ *Case of Mccann and Others v. The United Kingdom* App. No. 18984/91, 27 September 1995; *Case of Van Colle v. The United Kingdom* App. No. 7678/09, 29 April 2013.

³⁹ *Case of Mccann and Others v. The United Kingdom* App. No. 18984/91, 27 September 1995; *Case of Keenan v. the United Kingdom* App. No. 27229/95 2001, 3 April 2001.

⁴⁰ Geiger, Khan, and Kotzur, 2017, paras. 5, 10.

⁴¹ von Mangoldt, Klein, and Starck, 2010, Art. 2 paras. 205, 224, 229.

measures.⁴² However—as in German constitutional law—there is no explicit decision on the direct question of the quality of armaments.

However, it should be noted that there is indeed a decision existing, namely by the UK Supreme Court dated 19 June 2013⁴³ on the direct legal question at issue, which was exactly along the lines advocated here. The British army had killed or injured soldiers through “friendly fire” during the Second Gulf War. Therefore, in view of the specific English legal situation, the responsibility had to be clarified in court. The court found that the UK should be obliged to pay, as these casualties would most likely have been prevented by an easily available technical means, namely an identification friend/foe system.

It is interesting to note that the so-called “doctrine of combat immunity,” which has long been advocated in the UK, was rejected for this. This theory briefly states that military operations are not justiciable. The UK Supreme Court rejected this in the case of armament decisions: The reason was that armament decisions do not correspond to concrete military combat due to the possibly lengthy decision-making processes that take place outside of concrete military operations,⁴⁴ where far-reaching decisions often have to be made within seconds. Based on the author’s experience in many tactical simulations, often tactical decisions must be made in minutes or shorter periods. Whole battalions (300–500 soldiers) or companies are doomed after a wrong decision of the military leader.

The decisive factor here is the following: The soldier has a duty to endure the threats of deployment “bravely” and, in the worst case, to accept the loss of his own life — that is, death. However, in contrast to this duty to bear the risk, the state as the employer has the duty to provide every possible protection, particularly against unlawful acts by third parties, such as the Taliban in Afghanistan or the Russian army in Ukraine.⁴⁵ Just as an aside, this duty to protect exists naturally if, for example, the action of the enemy in war were lawful under international law. In addition to and independently of the state’s constitutional duty to protect under Article 2 para. 2, sentence 1 of the German Basic Law, there is a mutual relationship of loyalty that can also be described as follows: The soldier must accept the risks of deployment, while the state must protect him as well as possible by,

⁴² Karpenstein and Mayer, 2015, p. 39.

⁴³ UK Supreme Court, 2013, *Smith and others v. MOD* (41/2013) p. 1.

⁴⁴ *Ibid.*

⁴⁵ Gimmmler, 1998, pp. 76–87.

among other things, giving him the best possible opportunities during action. Considering the scientific findings described above, the state must increase the probability of success and thus survival during action. The state must therefore do everything in its power to minimise risks to the life and limb of soldiers. In other words, if this requires improved effective and protective equipment, training, or deployment logistics appropriate to the situation, insofar as this is possible through correct political decisions, then this is precisely what must be provided. The principle of the duty to protect applies here: Someone who deploys another person for a dangerous activity must do everything possible to protect him from avoidable threats in this respect.⁴⁶ These principles particularly apply where a state has compulsory military service, as is the case in Austria, and the state actually forces citizens as soldiers to face the threat of military deployment, even more so than in volunteer armies such as the German Bundeswehr.

Of course, this also includes the actual use of existing suitable weapon systems, if this arises as part of an ongoing assessment of the situation. There is also room for discretion and judgement here. However, mere “political wishful thinking” to the detriment of the soldiers is inadmissible. The fact that the boundaries here are fluid needs no further explanation. For example, the decision to not send heavy equipment to Afghanistan was certainly justifiable for a long time. Particularly regarding protection technology, it is unlikely to be justifiable in the future to deploy infantry soldiers without mine-resistant boots in areas at risk of mines or improvised explosive devices once their effectiveness has been proven. The rapidly developing range of military protective equipment should also be mentioned here.⁴⁷

It can be argued that there is a greater or lesser degree of political or tactical/operational discretion and judgement in the assessment of complex military situations. In other words, for the question to be assessed here, this means that the decisions on armaments and weapons systems must be reviewed time and again and cannot be made within the framework of the free scope for assessment and discretion. This is because these decisions are bound by fundamental rights. Therefore, these require specific measures to be taken to fulfil the assumed protection obligations. This is because such decisions are open to falsification in the sense of scientific theory.⁴⁸ Of

⁴⁶ Edenfeld, 2009, p. 938.

⁴⁷ ‘Infanterist der Zukunft’, 2013.

⁴⁸ Gimmmler, 2016, p. 137, 143, 145.

course, it can be argued that the planning and realisation horizon—as well as the possible negative consequences for the battlefield due to obsolescence caused by the necessity of long-term planning, with the resulting future uncertainty—do not lead to any relevant technical or legally significant errors in the necessary *ex-ante* consideration. However, this train of thought is misleading: For example, as the UK Supreme Court’s 2013 decision⁴⁹ showed, it is possible to qualify the lack of retrofitting decisions as incorrect in the legal sense. The best example of this is the ongoing war in Ukraine, where new drone equipment is created and adapted almost monthly, including the related defence measures. There is precisely no decades-long planning here; action must—and will—be taken quickly in the legal sense.

5. Conventional and alternative procurement channels: New ways to glory

5.1 No dealing with public procurement law and the related primary and secondary EU law

The following *does not* examine European and national public procurement law such as Article 346 of the treaty of the functioning of the European Union (TFEU) or European Community Directive 81/2009 for the coordination of supply contracts in the areas of defence and security.

5.2 Universal state’s armament interests and goals

In the past, states extensively relied on state-owned companies, known as arsenals, to supply armaments. As far as can be seen, this hardly exists in the western world today. Instead, armaments come almost exclusively from private arms companies. This means that the means of procurement is the contract. The purchase contract is the classic contract for procurement, but is it the ideal form of procurement? It is useful to understand the fundamental interests of the state in the procurement of military equipment and then assess the contractual procurement channels. Of course, a complex defence procurement contract is not a simple purchase contract; it also includes a long-term contract for the supply of spare parts, upgrades, and possibly maintenance services. The term “purchase contract” is only used here in simplified form, as it represents the basic procurement transaction: The weapons system is purchased.

⁴⁹ UK Supreme Court, 2013, *Smith and others v. MOD* (41/2013) p. 1.

5.2.1 Secure, robust availability of armament

First, the universal armament interests of each state must be established. The state wants to have large-scale military equipment available under all circumstances, without any possibility for a third party — who does not act based on orders and obedience but on a contractual level of equality — to withdraw or restrict its use or to influence the way in which it is used in any way. In short, the state must be able to dispose of its army's equipment in every respect. This applies to not only exercises, manoeuvres, and normal operations but also conceivable defence or external deployment (e.g. in Afghanistan). Here, further essential interests can arise from the fact that procurement decisions should also be implemented quickly once a decision has been made in favour of a specific procurement project as being necessary for defence purposes. This is why commercial or previously established criteria, used in logistics and all long-term supply and performance relationships, must be used to assess a specific usage or performance situation.⁵⁰

Applied to armed forces, this means that armament must always be available. This is based on logistics, understood as a secure supply chain or secure logistics and supply chain. It must not be fragile, that is, easily interruptible.

5.2.2 Future proof, sustainable armament

The requirements of the future can also be reliably mapped; this means that changed, particularly updated, products can be requested and are reliably available. The armament item is subject to the “revolution in military affairs”⁵¹ from the very first moment. Translated to military procurement, this means that the armament item must also be able to be “upgraded” and thus kept up to date in the future. A prime example is the retrofitting of Leopard 2A4 with anti-tank/guided missile protection, based on Turkey's experience against the so-called Islamic State, and especially mine protection, which is now available on the Leopard 2A8 (2024).

⁵⁰ Gimmler, 2022, p. 74.

⁵¹ Anand, 1999; Müller and Schörnig, 2001, p. 8.

The two criteria of “safe delivery” and “future-proof” are also summarised under resilience. Resilience is the ability to withstand future developments of a negative nature. It requires, on the one hand, that the armed forces protect themselves against known or foreseeable risks and, on the other hand, that they be able to adapt to as yet unknown developments as far as conceivable and possible, that is, not in the case of disruptive, devaluing developments. These also require contractual provisions, such as a special right of termination with compensation for the disadvantages for the landlord in case of a rental contract about a tactical aircraft. Regarding the universal interests and goals so far, the optimisation of long-term service contracts, such as logistics contracts, has hundreds of different contract design points⁵² to optimise resilience on a best-practice basis. It is the art of best practice contractual drafting to reach the goal of resilience.

5.2.3 Commercial efficiency

The criteria for the fulfilment of the above requirements — “Secure, robust availability of armament” and “Future proof, sustainable armament” — means that armament must be available at a reasonable price. In public procurement law, the point of commercial efficiency is often still assessed independently of the criteria of “secure, robust supply through delivery or performance” and “future proof, sustainable armament,” which is already wrong from the outset. That is, an uncertain availability situation or an availability situation that is not sustainable cannot be commercial, as it is burdened with unforeseeable risks. Depending on the requirement and classification, the aspect of the quality requirement for the service must also be considered. This aspect is not discussed further here.

5.3 Conventional procurement: Purchase contract as a system contract where applicable

For purchasing armaments, the conventional solution is analysed for pros and cons. The property-oriented conventional view (where the army buys an armament item) is as follows: The usually extremely durable large-scale combat equipment (Leopard, Eurofighter, etc.) is purchased. However, the purchase method is de facto an obstacle to modern armour or equipment, such as the German BW fleet of non-fighting fleet of cars and trucks, since the necessary high amounts are often not available. That is, the necessary

⁵² Gimmmler, 2022, p. 169.

purchase price amount does not exist in the yearly budget, or it has not been included in the budget.

Due to the specific situation of the full transfer of all risks (apart from warranty), purchase-based solutions are, in principle, suitable for passing on the costs of later adaptations, renewals, etc., to the defence companies at a higher price. The decisive factor is that these are deliveries after the transfer of risk within the meaning of §§ 446 ff. of the German Civil Code. With the handover, the Federal Republic of Germany or another EU or NATO state is not only the owner but also has no claims to further services, unless these are contractually included in special regulations or correspond to legal regulations.

5.4 Alternative rental/leasing procurement model

In the following, only the alternative procurement model of “renting/leasing” as a time-bound, usage-based procurement model is discussed. Many other methods, such as pooling and sharing or privatisation of special services, are only referred to but are not dealt with here.⁵³ This is because while the advantages of renting/leasing solutions can be presented very well, there is not enough space for a full discussion.

5.4.1 Business assessment of the alternative “rental/leasing” procurement model

Rental or the closely related leasing is a strictly *time-based* transfer of use. Here, the transfer of use for a limited period is synallagmatically linked to the payment of the purely time-oriented rent as remuneration for the tenant. The reciprocal and linked main services are therefore the transfer of use for a limited period and the payment of rent for the actual period of use. Of course, these use-related contracts have their own special features. To eliminate the risk of finding no possible rental successor after the first rental period, which must be priced in by the armament manufacturer (and thus the lessor) after the return of the armaments, it is practically necessary to conclude the contract for the full conceivable period of use, possibly with options. A short-term lease, as with cars or trucks, is therefore practically impossible; the uncertainty of a secondary market requires a life-cycle rental period.

⁵³ Clement, 2012, p. 7; Kaldrack, 2013, p. 19, 21.

This is a real paradigm shift. Instead of infinite property, the use-oriented consideration applies. To present the advantages, an example with some realistic assumptions must be analysed: The military equipment is rented for 20 years (a “life-cycle contract” as a best practice long-duration contract). The amount of the rent is determined by the cost of depreciation, normally calculated using the same annual rates. In addition, the financing costs, especially the interest to be paid and the calculated profit, are part of the rental rate.

The term “rent” is used when referring to the classic rental model, that is without any kind of transfer of ownership or purchase provision. The term “lease” is used when referring to a long-term lease, usually with some kind of provision for a right of purchase or right to sell, possibly to be exercised under certain circumstances, combined with a normally very long contract term.

For Germany, the author is guided here by the leasing decrees of the Federal Ministry of Finance from 1971 onwards, particularly the leasing decree for the income tax treatment of movable property leasing of 19 April 1971⁵⁴ and the decree on the tax attribution for partial amortisation leasing of movable property of 22 December 1975.⁵⁵ The legal situation for Austria is practically identical to that in Germany, particularly regarding the VAT-relevant allocation to purchase on the one hand (full VAT is incurred at the beginning) and to rent on the other (VAT is incurred *pro rata temporis*).⁵⁶ In other EU countries, the legal situation is likely to be similar or identical.

5.4.2 Historical examples of arms procurement and current proliferation issues in the NATO area

The rental model was already common in ancient Rome for state events, especially when it came to combat equipment. For example, gladiators and their equipment were hired for gladiatorial games.⁵⁷

The most important *historical example* is the so-called Lend-Lease Act of 1941 in the United States, dated 18 February 1941. This law allowed

⁵⁴ Bundessteuerblatt (1971) I. p. 264.

⁵⁵ Bundesministerium der Finanzen (1975) IV B2 161/75, p. 2170.

⁵⁶ For explanations on the leasing law situation in Austria’s Administrative Court, see Einkommensteuer-Richtlinien (EStR), 2000, Rz. p. 135; Rechtsinformationssystem des Bundes (RIS) Bundeskanzleramt, 28 May 2002; von Rosen, 2009.

⁵⁷ Gedeon, 2019.

the US President to sell, donate, or lease any type of weapon to any nation whose 'defence he deemed vital to the United States' at his plain discretion. The option of loaning rather than renting/leasing was used in favour of Great Britain.⁵⁸ The commercial basis was that Great Britain had essentially exhausted its financial resources after losing the French campaign in 1940 and because of the further burden of war, including against Italy.

This procurement method is also currently being used, at least in part, in NATO. See the following examples:

- Hungary leased 14 modern Saab Gripen fighter aircraft from Sweden.
- The Czech Republic also leased Saab Gripen fighter aircraft for EUR 62 million per year for the Czech Air Force.
- Great Britain procured air refuelling aircraft on a leasing basis.
- Germany procured its non-combat vehicle fleet via the federally owned BwFuhrparkService GmbH and also rented Israeli Heron drones.
- Norway procured submarines on a leasing basis.

All of these transactions have the classic tenancy law basis of a synallagmatic exchange relationship involving "temporary transfer of use in return for *pro rata temporis* payment." As mentioned under section 5.4.1, all these rental solutions are long-term contracts as far as military equipment is rented. As a consequence, the producer does not want to bear the risk of a second-hand market. Therefore, the German White Fleet typically goes contrary to short-term rental contracts, as obviously there is a working second-hand market.

5.4.3 "Objection": Typical objections from conventional procurers to the rental/leasing model

A) Temporary use

Temporary use is terminable, and the landlord may terminate it at the worst moment for the army. Although this is true, this situation can be avoided by numerous permissible contractual means and clauses, such as by an extremely long basic lease term of 30 years in Germany.

⁵⁸ Wikipedia (2025) Leih- und Pachtgesetz, [Online]. Available at: https://de.wikipedia.org/w/index.php?title=Leih-_und_Pachtgesetz&oldid=249515695 (Accessed: 16 January 2025).

Ordinary termination rights are excluded for this period by definition, and extraordinary termination rights can be excluded to the greatest possible extent. The landlord's residual existing or perceived possibility of termination can be countered by a call option to be exercised in this case. This also counters the argument that the lessor can terminate the armaments, especially tanks, in the event of a concrete threat of war due to the so-called force majeure situation of war or deny its obligation to perform. However, these arguments are absurd for experienced contract lawyers because the underlying provisions are fully dispositive. There is practically no mandatory law in this area — all such rights that may exist by law can be excluded. This applies, for example, to the provisions in Sections 543 BGB (Germany) and 1118 ABGB (Austria).

B) Risks from the person of the landlord

The area of risks that result from the person of the landlord is mentioned. Then, what about insolvency and similar risks? Here, too, special regulations in national law must be disregarded, although they would have to be examined. On the one hand, insolvency could be averted from the outset using the takeover rights (call option) of the tenant, that is the state, in the event of insolvency with full coverage of the debt. On the other hand, the same could be achieved by a state guarantee declaration or by measures in advance of conceivable insolvency, which could and would have to be agreed upon. Here, too, the purchase call option should be mentioned.

C) Hostile takeover

The sale of shares by way of share deals to other private companies or even “dangerous foreign countries” such as China is repeatedly mentioned as a spectre. This must also be countered by pre-emptive rights and, in the case of foreign sales, by measures under the Foreign Trade and Payments Act (Germany), such as prohibitions on sale.

D) Obsolescence and risk of loss

Finally, a key aspect is maintenance and loss in the event of deployment and for future proofing (which is the ability to retrofit; e.g. Leo 2A1 is now retrofitted to Leo 2A8 as the German Leopard main battle tank). This, too, presents an illusory problem: Maintenance/repair can be contractually regulated through system repairs by the manufacturers on the one hand and, on the other hand, through troop maintenance itself. The spectre of the loss

of this armament in the event of war is again a simple misconception and a pseudo-problem. The problem is the same as with the loss of one's own purchased combat vehicle: It simply has to be procured anew. The lessor must be obliged to provide a new vehicle/equipment and lease it. In the event of purchase, a new piece of equipment would have to be bought, so it is the same financial situation.

5.5 Holistic optimisation view of defence procurement, using the example of VAT optimisation⁵⁹

We can state that the procurement of military equipment, which is expensive but at the same time relevant to fundamental rights, requires a legally multidimensional approach and encompasses numerous special aspects. Many aspects are suitable for optimisation.

Overall, the aspects of public procurement law, pricing law, civil law aspects of contract design, and the basic rights (under public law) of any soldiers who may fight must be considered.

Surprisingly, one special optimisation point is VAT law, as this area can be used for further optimisation in conjunction with rental and leasing procurement. In the following, some relevant aspects of the VAT legal situation are examined. These are the main VAT legal possibilities for procurement optimisation. In 2024, the defence expenditure of the EU member states amounted to around EUR 326 billion; thus, the use of VAT structuring options results in significant benefits.⁶⁰ In other words, the efforts of complex legal optimisation analysis are worthwhile.

5.5.1 VAT as a typical special agenda for optimising defence procurement

At first, it may seem surprising to look at VAT. However, the common German catchphrase of “*Linke Tasche, Rechte Tasche* = left pocket, right pocket”—meaning that it is not worthwhile for the state to save VAT, as it loses precisely this VAT as tax revenue—is patently false.

⁵⁹ Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax.

⁶⁰ Europäische Verteidigungsbereitschaft (2024) Europäische Verteidigungsausgaben erreichen 2024 neues Rekordhoch in europa.rlp.de, [Online]. Available at: <http://europa.rlp.de/service/presse/detail/europaeische-verteidigungsausgaben-erreichen-2024-neues-rekordhoch> (Accessed: 22 November 2024).

This is because VAT is by no means neutral from a commercial perspective; it would only be neutral if the Federal Republic of Germany paid VAT, as it would benefit from it correspondingly.

In accordance with Article 106 (3) of the German Basic Law, the German system of fiscal equalisation provides a split of the VAT revenue between the federal government, federal states, and municipalities. Accordingly, as per the figures for 2022,⁶¹ only around 48% of the VAT is due to the federal government. In other words, only 48 cents of every euro paid in VAT flows back into the federal budget — a bad “deal” from a commercial perspective. However, this deal becomes catastrophic when you realise that of these 48 cents, only about 5 cents (about 10%) actually flow back into the defence budget. However, this has a much greater impact when you realise that a portion of the combat vehicles supplied must actually be financed by a loan with regard to the national debt, which burdens the investment part of the defence budget at the time they are used.

5.5.2 EU-Directive on the harmonisation of the VAT-System Directive: VAT assessment of the reference model “sales contract”

The following describes that the direct legal provisions are based on the German tax law situation. A very similar legal situation is likely to apply to Hungary, subject to a more detailed examination, as all European VAT laws are based on the VAT-System Directive and the follow-up directives.⁶² The main provisions of the VAT-System Directive apply directly if states do not transpose the provisions of the directive or do not transpose them correctly and the provisions are sufficiently clear. In this case, the provisions take precedence over national VAT law.⁶³

Regardless of whether the procurement is “stretched” within the framework of a long-term purchase contract for newly manufactured products or is also carried out *uno actu* for existing systems, the full purchase price (if applicable, less certain retained security amounts for

⁶¹ Wikipedia (2025) Gemeinschaftssteuer (Deutschland), [Online]. Available at: [https://de.wikipedia.org/w/index.php?title=Gemeinschaftsteuer_\(Deutschland\)&oldid=251576795](https://de.wikipedia.org/w/index.php?title=Gemeinschaftsteuer_(Deutschland)&oldid=251576795) (Accessed: 16 January 2025).

⁶² Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax; Lohse and Peltner, 2007, p. 1.

⁶³ C-651/11, *Staatssecretaris van Financiën v X BV*, 30 May 2013. See the established case law of the ECJ: Bunjes, 2018, p. 1, para. 9.

service disruptions due to material defects) must be paid in each case, including VAT.

In this respect, the state acts as a non-entrepreneur and is therefore not entitled to deduct VAT input tax with regard to VAT in accordance with Sections 2 and 15 of the German VAT Act. In other words, both the net purchase price and VAT must be financed in full and are therefore charged to the investment part of the defence budget, which in Germany is given in Section 14. This means that the purchase price of EUR 15 million for a “Puma” infantry fighting vehicle system to be financed includes EUR 2.4 million in VAT.

5.5.3 Advantages of the rental model from a VAT perspective: Military procurement as an object of typical commercial optimisation, in this case through contracts for VAT-favourable structuring

The structure of the rental agreement allows only a fraction of the initial VAT to be financed *pro rata temporis*—up to 30 years in extreme cases—and this alone has a considerable interest-saving effect.

The focus here is also on the VAT aspect. As long as the current European VAT law situation exists, according to which investments in the defence sector are also subject to VAT and the defence budget is thus burdened, it should be recognised that the defence ministries must also include VAT-favourable structures in their considerations.

For that, the following short sample calculation should be made. The roughly simplified alternative calculation for the amount with a purchase price of EUR 10 million and VAT of 20% is as follows:

- Purchase consideration: EUR 10 million purchase price for an armament item + 20% = EUR 12 million, as a burden on the Ministry of Defence budget in the year of purchase.
- Consideration of rental procurement: Assumed annual rental amount of EUR 550,000 + VAT (calculation assumptions: EUR 500,000 depreciation with a normal useful life of 20 years, 5% interest, and 5% profit) + 20% VAT = EUR 660,000 as an annual burden on the budget.
- Regarding the first year: Instead of EUR 12 million for one tank, we can get more than 18 tanks for the same amount (EUR 12 million/660,000 = ~18).

Bibliography

- [1] Anand, V. (1999) 'Impact of Technology on Conduct of Warfare in Strategic Analysis'. *A Monthly Journal of the IDSA*, 23(1). [Online]. Available at: https://ciaotest.cc.columbia.edu/olj/sa/sa_99anv02.html (Accessed: 16 January 2025).
- [2] Bortz, J., Döhring, N. (2002) *Forschungsmethoden und Evaluation für Human und Sozialwissenschaftler*. 3rd edn, Springer.
- [3] Bunjes, J. (2018) *UStG-Kommentar*. 21. Edn, Munich: C.H. Beck.
- [4] Cadieu, T., Adams, J. (2010) 'Der Kampfpanzer Leopard 2A6M in Afghanistan', *Das Schwarze Barett*, 10(43).
- [5] Clement, R. (2012) 'Sicherheitspolitik in Europa vor dem Hintergrund der Euro-Krisen', *Der Mittler Brief*, 3.
- [6] Dietlein, J. (2022) *Allgemeines Polizei- und Ordnungsrecht*. 16th edn. Munich: C.H. Beck.
- [7] Dupuy, T. N. (1980) *The Evolution of Weapons and Warfare*. Indianapolis, Indiana: Bobbs-Merrill Co.
- [8] Edenfeld, S. (2009) 'Die Fürsorgepflicht des Arbeitgebers bei Auslandseinsätzen', *Neue Zeitschrift für das Arbeitsrecht*, 09(17).
- [9] Gedeon, M. (2019) 'Sparsame Sportveranstaltungen im antiken Rom und heute', in Valdár, V. (ed) *Perpauca terrena blande honori dedicata (Gedankenschrift für Peter Blaho zum nicht erlebten 80. Geburtstag)*, Trnava: Trnavská Univerzita, pp. 157-165.
- [10] Geiger, T., Khan, M., Kotzur, S. (2017) 'Anhang 1 Grundrechte-Charta, Einführung' in *EUV-AEUV-Kommentar*.

-
- [11] Gimmler, K. H. (1998) 'Grundlegende rechtliche Rahmenbedingungen und Gestaltungsmöglichkeiten des BW-Beschaffungswesens' in *Finanzierungsnot der Streitkräfte*, Dokumentation des Symposiums Bad Marienberg, pp. 76-87.
- [12] Gimmler, K. H., Bösch, Reinhard E. (eds) (2016) 'Grundrechtliche Pflichten zur Gefahrenabwehr im Verteidigungs- und Sicherheitsbereich', in *Wehrpflicht*, Vienna: FPÖ-Bildungsinstitut, pp. 137-145.
- [13] Gimmler, K. H. (2017a) 'Alternative Rüstungsbeschaffung in zivilrechtlicher Gestaltungsbetrachtung'; 'Miet- und Leasingmodelle für die Deutsche Bundeswehr und das Österreichische Bundesheer', *ÖMZ*, 17(2).
- [14] Gimmler, K. H. (2017b) 'Verteidigungs-, insbesondere Rüstungsentscheidung zwischen Recht und Politik in Deutschland, Österreich und Ungarn', *ÖMZ*, 17(5).
- [15] Gimmler, K. H. (2022) *Theorie und Praxis des Kontraktlogistikvertrages und verwandter Vertragsform der Logistik, zugleich ein Beitrag zur Best-Practice Gestaltung von langfristigen Wirtschaftsverträgen*. Miskolc, PhD Dissertation.
- [16] Gleißner, W., Rom, Meike, F. (2005) *Risikomanagement*, Freiburg: Haufe Verlag.
- [17] Infanterist der Zukunft (IdZ) (2013) *High Tech Warriors*. Vienna: Truppendienst.
- [18] Jarausch, K. H., Armingier, G., Thaller, M. (1985) *Quantitative Methoden in der Geschichtswissenschaft*. Darmstadt: Wissenschaftliche Buchgesellschaft.
- [19] Kaldrack, G. (2013) 'Die Krise als Chance', *Europäische Sicherheit und Technik*, 10.

-
- [20] Karpenstein, U., Mayer, F. (2015) *EMRK – Kommentar*. Munich: C. H. Beck.
- [21] Lohse, C., Peltner, H. M. (2007) *Mehrwertsteuersystemrichtlinie*. Cologne: Verlag Dr. Otto Schmidt KG.
- [22] Macksey, K. (1986) *Technology in War: The Impact of Science on Weapon Development and Modern Battle*. London: Simon & Schuster.
- [23] Müller, H., Schörnig, N. (2001) 'The revolution of military affairs', *Hessische Stiftung Friedens- und Konfliktforschung*, HSVK-Report, 8.
- [24] Popper, K. (1994) *Alles Leben ist Problemlösen*. Berlin: Piper Taschenbuch.
- [25] Potter, E. B., Nimitz, C. W., Rohwer, J. (eds) (1974) *Seemacht: Eine Seekriegsgeschichte von der Antike bis zur Gegenwart*. München: Bernard & Graefe Verlag Wehrwesen.
- [26] Regele, O. (1968) *Gericht über Habsburgs Wehrmacht*. Berlin: Herold.
- [27] Steinmann, T. (2012) 'Sparzwang gefährdet Sicherheit der Gruppe', *Financial Times Deutschland*, 08.06.2012.
- [28] Thorne, K. (2015) 'Historical battles and survivor rates' *Journal of military History*, 78.
- [29] van Creveld, M. (1991) *Technology and War*, New York: Free Press.
- [30] von Mangoldt, H., Klein F., Starck, C. (2010) *Kommentar zum Grundgesetz*. 6th edn, Munich: C. H. Beck.
- [31] von Rosen, C. (2009) *Finanzierungsinstrumente im Vergleich: Kauf versus Miete/Leasing*, Bachelor Thesis, University of Graz.
- [32] European Court of Human Rights (ECHR), 2004, (4839/1999).

STJEPAN GROŠ*

Social engineering warfare as a tactic of information warfare**

ABSTRACT: Information warfare encompasses a set of tactics and techniques used to spread disinformation. Adversaries use these strategies to run information operations to manipulate individuals, groups, and society. Owing to the current widespread information warfare, studying the phenomenon to identify effective and efficient means of combating information operations is very important. One prerequisite for the efficient and effective suppression of information operations is an awareness of the tactics and techniques of information warfare. Identifying these tactics and techniques will take some time because of the large number of options at the disposal of those who spread disinformation. This study contributes to this endeavour by analysing social engineering as a technique of information operations. Treating social engineering as a technique of information warfare is a novel approach because social engineering is usually associated with cyber security and is rarely discussed in conjunction with information warfare. We show that social engineering can be used in information operations without requiring significant adaptations. We also argue that social engineering should be treated as a distinct domain and activity, separate from both cyber security and information warfare. While both cyber security and information warfare can use social engineering in their operations, they remain distinct activities that require unique knowledge and skillsets.

KEYWORDS: information warfare, information operations, social engineering, cyber warfare, TTP.

1. Introduction

In the book chapter “Information Warfare Tactics and Techniques”,¹ we defined “warfare” as a set of tactics and techniques. Depending on the

* Associate Professor, Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia. stjepan.gros@fer.hr.

** The research and preparation of this study was supported by the Central European Academy.

nature of these tactics and techniques, various types of warfare can be identified, such as information warfare, cyber warfare, psychological warfare, and cognitive warfare. We also defined the relationship between information warfare and other types of warfare. Specifically, we determined that other types of warfare can either be used by information warfare, such as in cyber warfare (a technical method used during information operations), or use information warfare, such as in psychological operations that use information warfare to spread specific information to a target.

After this framework was established in the book chapter, a pertinent question arose: how can it be expanded? One of the claims made in the chapter was that cyber warfare is only a means of achieving a position from which cyber methods or other means are used to pursue broader objectives. This led to the question: Can social engineering be used as a means of information warfare in the same way that cyber warfare is used?

In this study, we address the relationship between social engineering and information warfare. Social engineering is frequently associated with cybersecurity, where it is used to compromise systems by attacking humans instead of technical systems. The use of social engineering has been hijacked by the cyber security community. However, when the term was introduced in the late 19th century, it meant “manipulating society”; only in the second half of the 20th century did it become closely associated with cyber security.

Social engineering has been extensively studied within the cyber security community because of its importance to the field. Although this body of research generates knowledge useful for cyber security purposes, it is sufficiently broad to be applicable to the domain of information warfare as well. Therefore, we analysed whether and how social engineering can be used as a tactic of information warfare. In doing so, we relied mainly on literature generated within the cyber security community. This restriction is intentional, as we want this knowledge to be used broadly, beyond the cyber security field. We argue that social engineering is an activity useful not only in cyber security but also in information warfare. Furthermore, we argue that social engineering is a form of warfare according to the definition given in our book chapter because it involves tactics and techniques.

The remainder of this paper is organised as follows. In Section 0, we provide the background knowledge required for the rest of this chapter. We define “social engineering” and also draw on definitions used in the book

¹ Groš, 2024.

chapter on information warfare tactics and techniques.² Section 0 describes the tactics and techniques employed in social engineering. In Section 0 we explain how social engineering can be used as a technique of information warfare. In Section 0 we discuss selected cases that illustrate the use of social engineering in information warfare. Finally, Section **Hiba! A hivatkozási forrás nem található.** provides our conclusions.

2. Background

In this section, we discuss the terminology necessary for the rest of the paper and present analyses of related work that we consulted while preparing for and conducting our research.

2.1. Terminology

The term “warfare” refers to the activity of fighting a war, including the weapons and methods used. Thus, warfare encompasses sets of tactics and techniques. The weapons and methods used determine the type and subtype of warfare being waged, such as cyber warfare, space warfare, ground warfare, naval warfare, aerial warfare, information warfare, and hybrid warfare. Tactics comprise the reasons why something is being done, while techniques are the specific ways of implementing a set of tactics. The most well-known database of tactics and techniques is arguably the MITRE ATT&CK pattern for cyber warfare.³ Many resources have been invested in its development and maintenance. The main component of the database is a set of tactics and techniques. It includes 14 tactics and numerous techniques,⁴ all of which are used by different threat groups. The database also includes lists of threat groups, descriptions of the tactics and techniques they use, and the tools used during attacks. A simple Google search will yield many materials related to the MITRE ATT&CK pattern, and Google Scholar research will yield many scientific papers that use the MITRE ATT&CK pattern. This pattern has become a lingua franca for communicating and understanding cyberattacks.

An “operation” is a chain of tactical steps used to achieve a goal. There are various types of operation depending on the type of warfare

² Ibid.

³ MITRE Corporation, 2024.

⁴ Interestingly, social engineering appears in the form of several techniques listed under the Initial Access tactic of MITRE ATT&CK.

involved. For example, the tactical and technical steps in MITRE ATT&CK are those of cyber operations. A cyber operation is executed by the operator, whether an individual or a group, responsible for its control and management.

Information warfare is a set of tactics and techniques used by adversaries to manage disinformation and information flow to achieve certain objectives. An adversary will use a set of tactics and techniques to run an information warfare operation that achieves a given goal. These tactics include generation, production, publication, dissemination, and blocking.⁵ All these tactical steps use disinformation or information as munitions.

The Council of Europe defines “misinformation”, “disinformation”, and “malinformation” as follows:⁶ Misinformation occurs when false information is shared without the intent to cause harm, such as when satire is taken seriously, typos occur, or other unintentional errors are made. Disinformation occurs when false information is knowingly shared to cause harm or when fabricated/deliberately manipulated content is designed to mislead. Finally, malinformation occurs when genuine information is shared to cause harm, often by exposing content intended to remain private in the public sphere, such as the publication of private information via leaks and the deliberate changing of the context of genuine content.

The *Oxford English Dictionary* gives two definitions for “social engineering”.⁷ In the first, social engineering is defined as an attempt to change society and deal with social problems according to certain political beliefs, such as by changing the law. In the second, it is defined as the act of making everybody believe something false in order to make them provide personal information that may be used to cheat them.

The idea of manipulating society using social engineering is an old concept, emerging in 1845.⁸ It has been used in politics and economics to transform societies through policymaking for a greater good. Interestingly, social manipulation is also an approach adopted by adversary nations and various other groups today. This activity goes by several names, such as “propaganda”, “psychological warfare”, and “information warfare”. Today, social engineering is typically understood to fall under the second meaning:

⁵ Groš, 2024.

⁶ Wardle and Derakhshan, 2017.

⁷ Oxford Learner's Dictionaries, 2024.

⁸ Hatfield, 2018.

manipulating individuals to compromise information systems, particularly within the domain of cyber security.

It is interesting that the first meaning, about changing society, fits well with the goal of information warfare – specifically information operations – as defined by several organisations. For example, Facebook defines information operations as⁹ actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion (we refer to these as “false amplifiers”).

Though the social manipulation goal is common to both information warfare (in the broad sense)¹⁰ and social engineering as defined by the *Oxford English Dictionary*, the means used to achieve it are different. The social engineering of a society, as defined in the *Oxford English Dictionary*, is done for its welfare and is achieved through legislation and similar means. In information warfare, societal changes are made through nefarious means. Thus, there is some overlap, and information warfare could be treated as a means of social engineering but for malicious purposes. Although this could be an interesting research direction, we did not pursue it in this study.

The second meaning provided by the *Oxford English Dictionary*, concerning the manipulation of individuals, is the one that predominates today.¹¹ The social engineering concept is used heavily in cyber security, where it has several definitions, such as “a set of applied psychological and analytical techniques used to manipulate a victim”.¹² The definitions all emphasise its human (specifically, psychological) elements, and highlight that it involves manipulation by an attacker for the attacker’s purposes.

Social engineering involves manipulating individuals using psychology and uses technology only as a means. In other words, technology is used as an enabler that allows those using social engineering (known as “operators”, or “social engineers” when the operators are individuals) to reach their targets more easily and increase their access.

⁹ Weedon, Nuland, and Stamos, 2017.

¹⁰ We define information warfare broadly to encompass activities such as psychological/cognitive warfare and propaganda. For details, see Groš, 2024.

¹¹ Hatfield, 2018.

¹² Yasin et al., 2021.

The term “social engineering” was hijacked by the cyber security community, where its use predominates today. Nevertheless, social engineering is a separate discipline that can be used in areas other than those identified by the *Oxford English Dictionary* definition. We aim to show how social engineering, as used in cyber security, can also be used in information warfare and discuss specific information warfare cases as instances of its application.

2.2 Related work

Three research streams are related to our study. The first comprises research on social engineering in cyber security. The second comprises research on influence and cyber operations. The third comprises research on the use of social engineering in information operations.

Many studies examine social engineering as used in cybersecurity, which is a highly active area of research. The most influential works are arguably those of Kevin Mitnick.^{13,14} Mitnick is well-known for his cyberattacks in the 1990s and early 2000s, when he used social engineering to successfully penetrate many secure systems. After being caught by the FBI and serving a prison sentence, he turned into a very successful information security consultant. Through his books, he laid the foundation for social engineering tactics, but he referred to social engineering as an “art”. The body of knowledge on social engineering has grown considerably, and some of it has been used in our research. These studies all deal with the use of social engineering in cyber warfare.

The second research stream comprises studies on information operations and cyber methods.^{15,16} This study investigated the use of cyberspace for influence operations. The studies in this stream discuss social engineering frequently but mainly as a method of cyberattack used in influence operations.

The third stream is the one closest to our work; however, it has produced few papers. The closest to ours is the work by Aurelian Stoica.¹⁷ His research is centred on a hypothesised distinction between social engineering and social influence, which are frequently considered to be the

¹³ Mitnick and William, 2003.

¹⁴ Mitnick and Simon, 2005.

¹⁵ Cordey, 2019.

¹⁶ Palmertz, 2021.

¹⁷ Stoica, 2021.

same. Stoica argues that social influence is a much broader concept than social engineering and was studied by the intelligence community before social engineering appeared in cyber security. Furthermore, he claims that intelligence agencies have perfected their social influence. He also claims that much of this knowledge has been transferred to the social engineering community. Although he provides evidence that intelligence agencies have developed social influence skills and knowledge, he provides no evidence that this knowledge has spread to the civil sector. In addition, his division of social engineering users into state and non-state actors and his exclusive focus on the former ignores the fact that social engineering and social influence are available to a much broader set of actors. To borrow his terminology, we study whether social engineering knowledge can be applied to social influence, but within a restricted scope. We are interested specifically in the use of social engineering to spread disinformation.

3. Social engineering tactics and techniques

Mitnick was probably the first to describe the social engineering process.¹⁸ He claims that a social engineering attack occurs in four steps. The first is Research. In this step, the attacker attempts to obtain as much useful information about the target as possible. The attacker then plans the attack based on the information obtained. The second step is Develop Rapport and Trust by contacting the target, developing a rapport, and gaining the target's trust. The third step is Exploit Trust. By exploiting an established trust, the attacker can make the victim do something. The final step is Utilise Information in a way that advances the attacker's position.

Since these steps were codified by Mitnick, a number of papers have tried to describe the methodology of social engineering.^{19,20,21} They have tried to make it less of an art so that the process can be predictable and repeatable. In this study, we used the methodology developed by Mouton et. al.²² Their attack cycle consists of six steps, each of which is further divided into sub-steps. The first step is Attack Formulation, which is further subdivided into Goal Identification and Target Identification. The next step

¹⁸ Mitnick and William, 2003.

¹⁹ Steinmetz, Pimentel, and Goe, 2021.

²⁰ Bullée, Montoya, Pieters, Junger, and Hartel, 2018.

²¹ Zouguang, Hongsong, and Limin, 2021.

²² Mouton, Leenena, and Venter, 2016.

is Information Gathering, which consists of three sub-steps: Identify Potential Sources, Gather Information from Sources, and Assess Gathered Information. These three steps are run iteratively until sufficient information is collected as determined in the Assess Gathered Information sub-step. The third step is Preparation, which consists of the sub-steps Combination and Analysis of Gathered Information, and Development of an Attack Vector. If the development of the attack vector is unsatisfactory, the process loops back to the Information Gathering step. The fourth step is Develop Relationship, which consists of two sub-steps: Establishment of Communication and Rapport Building. After a relationship is developed, the fifth step is Exploit Relationship by Priming the Target and Elicitation. The last step is Debrief, which consists of Maintenance, Transition, and, finally, Reaching Goal Satisfaction. If the Transition sub-step is unsuccessful, the process can go back to the Preparation phase.

Fundamentally, social engineering is based on psychology – specifically, on persuading victims or targets to do something. It is well-established in psychology that persuasion rests on six principles: authority, conformity, reciprocity, commitment, liking, and scarcity.²³ Under the authority principle, the social engineering operator creates a situation in which the target believes the operator to be in a superior position and thus considers the operator's requests beyond question. The conformity principle refers to people's tendency to behave as their group behaves; thus, if everyone is doing it, the social engineering operator's target is likely to do it as well. Reciprocity is the human tendency to perform an act to whomever has done it to them. For example, if one person opens a door to another, that other person will reciprocate by opening the door for the first. The first door might be one that anyone can open, and the second might be one that only some people can open, including a social engineering target who is reciprocating on behalf of an attacker. Commitment refers to people's tendency to fulfil a promise made either explicitly or implicitly; if they said they will do something, they will persist until they have done it. Liking refers to the human tendency to be more willing to do something if we like the person for whom we are doing it. Finally, scarcity is the human tendency to prefer and value things that are, or are perceived to be, rare.

Thus, social engineering operators abuse human behaviour according to the six principles and through the six steps described above, which allows them to be methodical and increase their chances of success.

²³ Cialdini, 2003.

4. Use of SE in information warfare

We have outlined social engineering tactics and techniques and explained the six principles of persuasion. In this section, we aim to integrate these principles into the tactical steps of publishing and spreading of disinformation within the context of information operations.²⁴ Again, unlike social engineering in cyber security, the goal is to make a target spread disinformation after making the target believe it. Alternatively, the target may not believe it or have an opinion about it, but the target must be unaware of being a social engineering target.

Through the analysis in this section, we will assess the use of social engineering in information warfare. In Section 0 we will explore additional examples that may be treated as social engineering attacks as part of information operations.

4.1. An example of an attack

This section demonstrates how social engineering can be used as a technique of information warfare. We go through all the steps in a social engineering attack described in Section 0 and examine how they might be applied to a real-world case. We use the example of the recent UK riots.²⁵ Their main instigator was identified as Stephen Christopher Yaxley-Lennon, better known as Tommy Robinson. Robinson shared a post on X (formerly Twitter) claiming that the ‘lad who organised Middlesbrough march been locked up on terrorism charges’.²⁶ That someone might have been Bonnie Spofforth,²⁷ but investigations are still ongoing, and exactly what happened is not clear. We will use this case to illustrate how social engineering might have been used to support the riots.

This process would start with the mission given by the information operation operator to the social engineering operator. The mission may include directions on what needs to be done and how to do it. Note that the

²⁴ Groš, 2024.

²⁵ Reuters, 2024.

²⁶ Lindsay and Grewar, 2024.

²⁷ Oppenheim, 2024.

social engineering operator does not have a big picture of the situation beyond the scope of the information operation²⁸ and thus requires directions.

In our example, as soon as the killings occur, an adversary state starts an information operation campaign to spread false accusations. The claims are prepared by someone who knows the political and economic situation in the target country and thus knows what will have the most severe consequences. This narrative is then given to the information operation operator, who starts to spread this disinformation using appropriate tactics.²⁹ The operator determines that it would be beneficial if far-right influencers such as Tommy Robinson spread this disinformation given the number of social media followers they have. Thus, the information operation operator tasks the social engineering operator with persuading Robinson (and possibly other similar people) to spread the disinformation. After receiving this task, the social engineering operator goes through the six steps of the social engineering process.

4.1.1. Attack formulation

The first step is determining who can be targeted using a social engineering attack and why. In this context, let us remind ourselves that the goal of information warfare is to spread disinformation that will influence the behaviour of a group, which can be as small as a few individuals or as large as a nation. The literature offers the potential for segmentation on a societal level via sociodemographic and psychographic targeting,³⁰ but it is not sufficiently fine-grained to be useful in our case.

Several potential targets are identified. The first category comprises influencers, individuals and media with large numbers of connections (e.g. social media followers). This also includes influential individuals who may not be active on social media. The advantage of targeting influencers is its multiplier effect: targeting an influencer effectively also targets their network of followers. Orthogonal to the number of a person's connections, we can divide people according to how suggestible they are. Based on this criterion, there are "believers", people who already believe in a theory

²⁸ For details on the big picture (i.e. how information operations are used in other kinds of warfare), see Groš, 2024.

²⁹ Groš, 2024.

³⁰ Stoica, 2021.

beneficial to an adversary. At the other end of the spectrum are “critics”, who actively oppose such theories.

The next question is where to find the members of each group. The answer is that they are easily found in social networks, forums, interest groups, and other venues.

In our example of the 2024 UK riots, even though the goal is set as a mission statement—spreading disinformation about the false identity and origin of the murderers—social engineering operators might be able to select additional targets. In our case, it is relatively easy to find additional potential targets by simply searching for people who are connected to Tommy Robinson.

4.1.2. Information gathering

The goal of information gathering is to find as much useful information as possible about the target. This can be done using open sources on the Internet. However, an operator might already have a dossier of high-profile people identified as possible targets, perhaps from an earlier operation. As the goal is to inject disinformation, it is important to identify potential obstacles that might jeopardise operations, such as if the target refuses to accept the disinformation or if the disinformation is publicly exposed. This step is not significantly different from that used when social engineering is used for cyber warfare.

In our example, Tommy Robinson had visited an adversary country at some point. This has two implications. First, he is likely inclined to believe narratives spread by that country’s government and its agencies. Second, those agencies likely have a dossier on him and know him well, which makes this step easy to accomplish. In addition, Robinson openly opposes the presence of Muslims in the United Kingdom, especially those who arrived via boats across the English Channel. This means that he is more susceptible to the allegation that they were responsible for this incident (via confirmation bias). This makes Robinson a relatively easy target.

4.1.3. Preparation

In the Preparation phase, all the collected information is combined, and the attack vector is defined. The nature of this step differs little between the use of social engineering in cyber warfare and in information warfare.

In our example, it may be decided that all communication will occur via Internet – specifically by having a trusted acquaintance under the operator’s control tweet something that will appear on Tommy Robinson’s Twitter feed, either because Robinson follows that person or because Twitter’s algorithms will recommend it to him. Someone who hosted Robinson while he visited the adversary country could be engaged for this purpose. In this case, the proxy is very likely to cooperate; if that is not the case, a separate social engineering attack could be mounted against the proxy.

4.1.4. Develop relationship

Again, this step differs little between cyber warfare and information warfare. In our example, relationship development might occur through email. The proxy sends an email to Robinson greeting him and alerting him to explosive news that is about to appear on Twitter. This note may increase the attention Robinson pays to Twitter and thus increase the chances of implanting the disinformation into him.

Another important technique in this step is making in-person contact with the target. For example, Robinson was in Russia in February 2020. This would be an ideal opportunity to develop a close relationship with a target. This relationship development does not need to be exploited immediately but can be prepared for some future social engineering operation, when the relationship-development process will be rapid due to this advance preparation.

4.1.5. Exploit relationship

After the relationship is developed, it is exploited. In our case, a tweet can be published, to which Robinson can be expected to react. To increase the chances of success, an exact time or timeframe for the tweet can be established during the relationship development phase.

An additional option, which might have been used for the UK riots, is publishing disinformation on websites under the control of the social engineering operators and bringing it to the attention of individuals who are likely to spread it to their followers without critically assessing its content.³¹

³¹ Courea, 2024.

4.1.6. Debrief

In the Debrief phase, we check whether the attack was successful. This is done by monitoring the consequences. Some consequences take time to manifest. When time is of the essence, several attacks may be planned to increase the chances of success and shorten the time required for the consequences to appear.

4.2. Discussion

This example shows the similarity between social engineering designed to exfiltrate information from a target and social engineering designed to get a target to perform an action that will benefit the operator. The social engineering steps followed in the performance of an attack are identical.

Moreover, it is difficult to show the presence of social engineering in information warfare. People who are socially engineered via information warfare and spread disinformation—as in our example of Tommy Robinson—may refuse to reveal the source of the disinformation they are spreading, or they may deny that the disinformation was received from a third party.

Finally, social engineering can be used as a technical step in information warfare. This implies that social engineering is a discipline separate from cyber security, with which it is frequently associated. A third use case for social engineering, to circumvent physical security, is not related to information warfare or cyber security.

5. Other cases of probable use of SE in IW

In the previous section, we used the UK riots of August 2024 as an example of how social engineering can be used in information operations without needing to make significant adaptations. The currently available information does not allow us to claim that this was a case of social engineering, but it showcases the possibilities of social engineering as a tool in information operations.

In the subsection below, we will describe two additional possible cases of social engineering used in information warfare. The first involves an informant who provided false information to the FBI, and the second occurred in the Republic of Croatia at the beginning of 2024. Again, there is

no conclusive evidence that these cases involved social engineering; however, there are strong indications that they did.

5.1. Lying FBI informant

On February 21, 2024, news broke that an FBI informant was arrested.³² The informant claimed that US President Joe Biden and his son Hunter had received bribes from the Ukrainian government. This claim had been the centrepiece of a Congressional investigation into and impeachment of former US President Donald Trump. The prosecution claimed that the informant had been in contact with Russian intelligence, which had been feeding informants with disinformation regarding President Biden and his son.

In this case, the targets of social engineering operations were Republican representatives in the US Congress. Information operations targeted the entire country, likely with the goal of destabilising it and lowering Joe Biden's chances of re-election for a second term in office.

Looking at this case as an information operation, the input was false information about President Biden and his son Hunter having received a bribe, along with additional details such as the amount received and the company that paid the bribe. To be effective, this disinformation must reach people who are susceptible to it, such as Representatives in the US Congress and the right-wing media, who are all likely to accept it without checking to confirm the validity of its claims.

The information operation planner must determine how this disinformation should be delivered to the targets. The channel used must be at least somewhat reputable. After reviewing the available assets, the information operation planner probably identified Alexander Smirnov, who had either been used previously or was identified as being very likely to cooperate. It is unknown if Smirnov believed this disinformation—in which case, he was socially engineered—or if he wittingly cooperated with Russian intelligence—in which case, he knowingly helped socially engineer US Congressmen and Congresswomen, as well as many US right-wing media figures. Thus, this may have been a case of social engineering.

5.2. Accusations against Fortenova Group's CEO

The second case happened at the beginning of 2024, when Croatian MPs Nikola Grmoja and Zvonimir Troskot of the right-populist party Most,

³² Yamat and Whitehurst, 2024.

accused Fortenova Group's CEO of damaging the company.^{33,34} In the Republic of Croatia, the Fortenova Group has been controversial and subject to considerable misinformation. The previous owner of Fortenova Group (then called "Agrokor") brought the company to the brink of bankruptcy. Because of the significance of this large company to the Croatian economy, the government intervened and took it over to stabilise it and avoid bankruptcy, which would almost certainly have destabilised the country. This was done hurriedly due to the emergency of the situation. This approach generated much speculation, mis/disinformation, and accusations, all of which targeted the government party. Opposition politicians, such as Nikola Grmoja and Zvonimir Troskot took every possible opportunity to attack the ruling party using the Fortenova/Agrokor situation. This strategy worked for a non-negligible portion of the public.

The sequence of events in this case, which might have involved the social engineering of Grmoja and Troskot, was as follows. On December 16, 2022, the company SBK Art LLC was placed on a list of sanctioned Russian legal entities.³⁵ SBK Art LLC had a 42.5% stake in Fortenova Group and was owned by Sberbank. Through fictitious transactions, Sberbank sought to protect its investment in Fortenova Group and avoid sanctions. SBK Art LLC brought suit against Fortenova Group. In December 2023, a court in the Netherlands rejected the claims made by SBK Art LLC. At the beginning of 2024, Grmoja and Troskot went public with accusations against Fortenova Group's CEO, which were almost identical to the arguments SBK Art LLC had made in court.

Proving that this was a case of social engineering is difficult because Grmoja and Troskot may have read court documents or been advised by someone who had. However, the court had rejected SBK Art LLC's arguments, and using them in public benefited the firm, as well as Grmoja and Troskot, who had an incentive to gain political points by misleading the public. It is uncertain whether Grmoja and Troskot believed these arguments. If they did, they were socially engineered; if they did not, they were witting agents of social engineering.

³³ Fortenova Group, 2024.

³⁴ Hina, 2024.

³⁵ Fortenova Group, 2022.

6. Conclusions

This study continues the work begun in the “Information Warfare Tactics and Techniques” chapter of our book, where we pointed out that generation, production, publication, dissemination, and blocking are tactics used in information warfare. This study considers social engineering as a potential technical component of publication and dissemination. This study seeks to foster cross-pollination across various research areas and draw from existing studies to help combat social engineering used in information operations and, ultimately, information operations themselves.

To achieve this, we first examined the social engineering process and outlined a six-step model. Subsequently, we analysed the potential application of social engineering in recent real-world cases, illustrating how each step of the social engineering process was reflected. We found that social engineering can indeed be used as a technical tool in information warfare without requiring significant changes. It may be more difficult to determine whether social engineering is being used in such cases than it is when social engineering is used in cyber security. In addition, it is important that the targets of social engineering remain unaware of being attacked; otherwise, the target becomes a collaborator, and either someone else is being socially engineered or no social engineering is occurring. We also examined two additional recent cases that might have involved the use of social engineering by adversaries.

This study shows that social engineering is a discipline distinct from cyber security, despite being regarded by the cybersecurity community as an integral component. This distinction is evident in the MITRE ATT&CK pattern, which includes several social engineering tactics. The MITRE ATT&CK pattern should, however, separate social engineering-specific tactics and recognise cyber warfare and social engineering as orthogonal activities that can be combined in various ways.

Bibliography

- [1] Bullée, J. W., Montoya, L., Pieters, W., Junger, M., and Hartel, P. (2018) 'On the anatomy of social engineering attacks - A literature-based dissection of successful attacks', *Journal of investigative psychology and offender profiling*, 15(1), pp. 20-45; <https://doi.org/10.1002/jip.1482>.
- [2] Cialdini, R. B. (2003) *Influence. At Work*.
- [3] Cordey, S. (2019) *Cyber Influence Operations: An Overview and Comparative Analysis*. Zurich: ETH Zurich.
- [4] Courea, E. (2024) Far-right disorder had 'clear' Russian involvement, says ex-MI6 spy. [Online]. Available at: <https://www.theguardian.com/politics/article/2024/aug/11/far-right-disorder-had-clear-russian-involvement-says-ex-mi6-spy> (Accessed: 20 August 2024).
- [5] EU Council puts SBK ART on sanctions list. Retrieved from Fortenova Group – News. [Online]. Available at: <https://fortenova.hr/en/news/eu-council-puts-sbk-art-on-sanctions-list/> (Accessed: 21 December 2022).
- [6] Fortenova Group on false accusations of Nikola Grmoja and Zvonimir Troskot, MPs, representatives of Most political party. [Online]. Available at: <https://fortenova.hr/en/news/fortenova-group-on-false-accusations-of-nikola-grmoja-and-zvonimir-troskot-mps-representatives-of-most-political-party/> (Accessed: 8 January 2024).
- [7] Groš, S. (2024) Information Warfare Tactics and Technics. in K. Zombory and J. E. Szilágyi (eds.), *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*, Budapest: Studies of the Central European Professors' Network, CEA Publishing. https://doi.org/10.54237/profnet.2024.zkjeszcodef_16

-
- [8] Hatfield, J. M. (2018) 'Social engineering in cybersecurity: The evolution of a concept', *Computers & Security*, 73, pp. 102-113.
- [9] Grmoja optužio Peruška da je oštetio Fortenovu u korist Vujnovca. Fortenova: Nije. [Online]. Available at: <https://www.index.hr/vijesti/clanak/grmoja-optuzio-peruska-da-je-ostetio-fortenovu-u-korist-vujnovca-fortenova-nije/2527220.aspx> (Accessed: 16 August 2024).
- [10] Lindsay, M., Grewar, C. (2024) *Social media misinformation 'fanned riot flames'* [Online]. Available at: <https://www.bbc.com/news/articles/c70jz2r4lp0o> (Accessed: 9 August 2024).
- [11] Mitnick, K. D., Simon, W. L. (2005) *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (2nd ed.). Wiley.
- [12] Mitnick, K. D., William, S. L. (2003) *The art of deception: Controlling the human element of security*. John Wiley & Sons.
- [13] Mouton, F., Leenena, L., Venter, H. (2016) 'Social engineering attack examples, templates and scenarios' *Computers & Security*, 59, pp. 186-209.
- [14] Oppenheim, M. (2024) *Woman named as first to share false Southport suspect rumour before riots says mistake 'destroyed' her*. [Online]. Available at: <https://www.independent.co.uk/news/uk/home-news/riots-southport-stabbings-suspect-bonnie-spofforth-b2593226.html> (Accessed: 9 August 2024).
- [15] Oxford Learner's Dictionaries. Social engineering. [Online]. Available at: <https://www.oxfordlearnersdictionaries.com/definition/english/social-engineering?q=social+engineering> (Accessed: 9 August 2024).

-
- [16] Palmertz, B. (2021) Influence operations and the modern information environment. in M. Welssmann, N. Nilsson, B. Palmertz, P. Thunholm, *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: Bloomsbury Collections. pp. 113-131; <https://doi.org/10.5040/9781788317795.0014>.
- [17] Explainer: Why are there riots in the UK and who is behind them? [Online]. Available at: <https://www.reuters.com/world/uk/why-are-there-riots-uk-who-is-behind-them-2024-08-07/> (Accessed: 8 August 2024).
- [18] Steinmetz, K. F., Pimentel, A., and Goe, R. (2021) 'Performing Social Engineering: A Qualitative Study of Information Security Deceptions' *Computers in Human Behavior*, 124; <https://doi.org/10.1016/j.chb.2021.106930>.
- [19] Stoica, A. (2021) 'Social engineering as the new deception game', *Romanian Journal of Information Technology and Automatic Control*, 31(3), pp. 57-68; <https://doi.org/10.33436/v31i3y202105>.
- [20] Wardle, C., Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* (Vol. 27). Strasbourg: Council of Europe.
- [21] Weedon, J., Nuland, W., Stamos, A. (2017) *Information operations and Facebook*. [Online]. Available at: <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf> (Accessed: 8 August 2024).
- [22] Yamat, R., Whitehurst, L. (2024) *Ex-FBI informant charged with lying about Bidens had Russian intelligence contacts, prosecutors say*. [Online]. Available at: <https://apnews.com/article/hunter-biden-fbi-informant-joe-biden> (Accessed: 30 July 2024).
- [23] Yasin, A., Rubia, F., Liu, L., Wang, J., Ali, R., Wei, Z. (2021) 'Understanding and deciphering of social engineering attack scenarios', *Security and Privacy*, 4(4); <https://doi.org/10.1002/spy2.161>.

- [24] Zouguang, W., Hongsong, Z., Limin, S. (2021) ‘Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods’, *IEEE Access*, pp. 11895-11910; <https://doi.org/10.1109/ACCESS.2021.3051633>.

ATTILA HORVÁTH*

New Types of Higher Airspace Flight Operations and Their Legal Challenges**

ABSTRACT: The absence of an internationally recognised legal boundary between airspace and outer space has long been acknowledged but has seldom resulted in practical operational issues. This was largely due to the clear technological distinctions between air and space activities. However, advancement in materials, propulsion and manufacturing technologies now enable operations in the transition zone between conventional aerial flight and spaceflight. It is only a matter of time before activities in this specific region around our Earth will be facing legal challenges. The lack of clear legal delimitation between outer space and airspace does not stem from an absence of natural phenomena that could define such a boundary but rather the existence of multiple valid criteria, each of which has counterarguments. To address this issue, it is proposed that an intermediate or transition zone be codified to establish a secure legal framework for these emerging higher airspace operations. Such a framework would provide legal security for investors, while fostering research, development and innovation. Although this measure would not resolve all legal ambiguities concerning spaceflight, it could alleviate challenges faced by developers and operators of stratospheric, mesospheric, and lower thermospheric flight technologies. This article explores practical examples and the technological contexts of these operations to inform developers about regulatory developments.

Keywords: air law, space law, higher airspace operations, spaceflight, hypersonic flight.

1. Introduction

As technology progresses, applications once deemed theoretical are becoming practical realities, while new theories emerge to push the

* Branch head, Capability Development Office, Hungarian Defence Forces Defence Staff, Hungary. attila@horvath.space.

** The research and preparation of this study was supported by the Central European Academy.

boundaries of innovation even further. This dynamic creates new operational frontiers, which often leaving regulatory gaps in their wake. Ideally, legal and regulatory frameworks should evolve in tandem with technological advancements. However, this alignment remains a challenge, particularly in the domains of outer space and high-altitude airspace operations.

These two physical domains cannot be easily separated, as there is no internationally accepted legal boundary between airspace and outer space. While various physical phenomena or arbitrarily defined locations could theoretically serve as the basis for delimitation, each is subject to challenges¹. Historically, this lack of delimitation did not pose significant issues, as air and space operations were distinct and did not overlap². The overlapping physical zone—encompassing the higher stratosphere, mesosphere, and lower thermosphere—was not operationally utilised due to technological constraints. Today, however, this scenario is rapidly evolving, and such developments are expected to accelerate.

This article examines technologies and operations that challenge the current lack of regulation, proposing that these case studies be used to refine existing legal frameworks or develop new ones for these emerging activities. Rather than seeking a rigid boundary between airspace and outer space—which may prove unattainable—this work introduces the concept of an intermediate zone. Such a zone could accommodate operations that challenge the established air and space regulatory regimes, foresting the growth of innovative technologies and applications.

2. The Higher Airspace

The atmosphere is structured into layers³ defined by variations in temperature with altitude. The lowest layer, the troposphere, has temperature descending with altitude, as it is heated by the Earth's surface illuminated mostly by the visible and infrared wavelengths of sunlight. Conventional air operations typically take place within this layer. The

¹ Bartóki-Gönczy and Sipos, 2022, pp. 39-59.

² The atmospheric phases of spacecraft, namely, launch and re-entry, have been regulated separately from conventional atmospheric flight operations, as they are considered integral to spaceflight activities.

³ Earth's atmosphere: A Multi-Layered Cake, no date.

troposphere is bounded by the tropopause, located at an altitude of approximately 10-15 km, depending on geographical latitude.

Above the tropopause lies the stratosphere, where temperature increases with altitude. This warming is due to the absorption of ultraviolet sunlight by the ozone layer, which is found in the upper stratosphere. The stratosphere also contains the jet stream system in its lower regions. The stratopause, which marks the upper boundary of this layer, is situated at an altitude of around 50 km.

Beyond the stratopause lies the mesosphere, where temperature again decreases with altitude. This decline comes about because the ozone concentration diminishes, reducing the primary source of heating. The mesosphere acts as a transitional layer between airspace and outer space. Sustained aerodynamic flight is impractical in this region, where rocket-powered vehicles dominate. Furthermore, aerobraking—the deceleration of spacecraft or meteoroids from orbital speeds to atmospheric freefall—takes place in this layer. The mesopause, at an altitude of approximately 80-90 km, marks the upper boundary of the mesosphere.

Above the mesopause lies the thermosphere, which, despite containing atmospheric gases, is practically a vacuum due to their low density. Temperatures in the thermosphere increase with altitude due to solar radiation absorption. While the lower thermosphere exhibits similar dynamics to the upper mesosphere, sustained orbital flight (unpowered spaceflight) becomes possible above approximately 250-300 km⁴.

The Kármán line, often considered as the boundary between airspace and outer space⁵, lies roughly at the interface of the mesosphere and

⁴ Physics does little to assist legislators in defining spaceflight. The term “sustained orbital flight” is inherently vague. A spacecraft can complete several orbits at an altitude of 200 km, but whether this qualifies as “sustained” depends largely on the intent behind the launch and mission objectives. For an experimental spacecraft testing, for instance, launch and re-entry technologies, a duration of mere hours or days at this altitude may be sufficient. For a crewed spacecraft using 200 km as a temporary parking orbit, the limited time available here at this altitude may be advantageous. In the event of a propulsion system failure, natural orbital decay into the denser atmosphere would occur before the onboard life-support consumables are depleted. Conversely, if a satellite designed for a multi-year mission becomes stranded at 200 km due to a launch vehicle malfunction or underperformance, this would constitute a mission failure. In such cases, the orbital condition would typically be described as “unsustainable”.

⁵ The numerical value of the Kármán line is often cited as 100 km. However, this is technically inaccurate and should be regarded as a simplified approximation or a “rough order of magnitude” value.

thermosphere, at altitudes ranging from 80-90 km. Its precise location depends on the actual state of the atmosphere and the ballistic coefficient of a given vehicle; for most spacecrafts, it lies within this range, though extreme vehicle configurations may have a slightly different Kármán line⁶.

The region between approximately 20-25 and 200-250 km is currently underutilised. Conventional atmospheric flight typically occurs below 20 km, while conventional spaceflight operates above 200-250 km. Spacecraft traverse this volume during ascent to operational orbits or re-entry into denser atmospheric layers. However, emerging technologies – enabled by advancements in materials and manufacturing – are beginning to unlock the potential for activities within this underexplored region.

3. Higher Airspace Flight Operations in the Stratosphere

Current aircraft rarely exceed altitude of 18-20 km (60,000-66,000 feet, or Flight Level 600 to 660). Commercial airliners and business jets typically operate below 15 km, while high performance military fighters can reach 20 km. Historically, the airspace above these altitudes has been the domain of specialised mission aircraft, such as the SR-71 and U-2 reconnaissance planes, alongside their counterparts—the MiG-25 and MiG-31 fighters—tasked with intercepting them. Experimental aircraft, such as the Ye-66 (a record-breaking variant of the MiG-21) or the Ye-266 preproduction version of the MiG-25, achieved altitudes of approximately 35 km. However, these were unique, purpose-built machines designed for special applications.

An emerging approach to stratospheric aerodynamic flight involves slow-flying, ultra-light aircraft resembling gliders in appearance⁷. Unlike earlier experimental aircraft requiring high speeds to generate sufficient lift, these modern planes utilise elongated wings to counterbalance their minimal weight even at low speed. This slower pace allows for the use of propellers rather than jet engines, with propulsion provided by electric motors. Powered by solar panels and rechargeable batteries, these aircraft do not rely on consumable fuels, limiting operational constraints to mechanical wear on the drivetrain and the degradation of battery chemistry. Current models can reach the lower stratosphere (approximately 20-23 km), with further advancements in structural and battery materials expected to enhance this capability.

⁶ McDowell, 2018, p. 674.

⁷ In-flight breakup, 2020.

In addition to these aerodynamic vehicles, high altitude airships and balloons using aerostatic lift⁸ can also operate within the stratosphere and the lower mesosphere⁹. The current altitude record for such vehicles belongs to the gas balloon BS13-08, launched by the Japanese Aerospace Exploration Agency in 2013¹⁰, which ascended to 53.7 km¹¹. Airships and balloons can remain operational for weeks or even months, using solar energy for power. While propellers of the airships rely on electric motors for propulsion, balloons operate without propulsion. Their operational duration is primarily limited by the gradual loss of lifting gas through the envelope and degradation of propulsion and power systems (where applicable).

These stratospheric vehicles, commonly referred to as high altitude platform stations (HAPS) or pseudo-satellites¹², provide services such as Earth observation and telecommunication akin to those of satellites. However, their operational patterns differ significantly, offering distinct service profiles. Notably, pseudo-satellites are recoverable, enabling payload servicing and replacement, particularly for propeller-driven aircraft and the airships. HAPS vehicles can be strategically transported to their operational areas via airlift or rely on their own propulsion for relocation.

Earth observation satellites typically operate in Sun-synchronous low Earth orbits, ranging between 450 and 650 km above the Earth's surface. These polar orbits allow satellites to survey nearly the entire globe, with the exception of small areas near the poles. However, data collection is constrained by on-board storage capacity (sensor memory) and downlink throughput. Moreover, a satellite can only observe a given target for a brief period—for seconds or minutes—before revisiting it hours or even days later, depending on its trajectory and sensor agility. The predictability of these revisiting times is particularly critical for military and national security Earth observation (referred to as Intelligence, Surveillance, Reconnaissance or ISR) satellites, as potential targets can plan their activities to avoid detection or employ deceptive tactics.

⁸ Airships can also use a combination of aerodynamic and aerostatic lift of special envelope design.

⁹ Colazza and Dolce, 2005, p .4.

¹⁰ Ultra-thin film balloon, 2013.

¹¹ Rocket-powered flying vehicles, notably the X-15 and the VSS SpaceShipTwo (and related vehicles), reach higher altitudes; however, they are launched by rocket engines onto suborbital flight trajectories and do not rely on aerodynamic lift at these altitudes. Steering is achieved through thrusters rather than aerodynamic forces.

¹² Aragón-Zavala, Cuevas-Ruíz and Delgado-Penín, 2008.

Pseudo-satellites, in contrast, have a more limited observational range than space satellites. At an altitude of 22 km, a high altitude platform station (HAPS) payload can monitor a circular area with a diameter of roughly 45 km (using a sensor with a 45-degree conic half-angle) to 75 km (with a 60-degree conic half angle), although coverage at the edges will be significantly oblique¹³. Pseudo-satellites can manoeuvre to cover larger areas but operate at much lower speed than satellites, typically between 50 and 80 km/h. Their most significant advantage lies in their ability to perform station keeping—maintaining a small, closed flight track that allows constant observation of a specific target. This capability provides uninterrupted and persistent data flow.

Space satellites are legally permitted to overfly any territory without prior consent from any sovereign state. HAPS, as atmospheric vehicles, are governed by aviation regulations. Nevertheless, even current pseudo-satellites can perform observation missions across international borders or into the airspace and territorial waters of a state from international airspace. With technological advancements, the service ceiling of HAPS is expected to increase. At an altitude of 30 km, a 60-degree conic half-angle sensor could cover a circular area of a 100 km diameter, enabling a standoff distance of 50 km. While a flight altitude of 20-30 km at a 50 km distance remains within the engagement range of modern air defence missile systems, these cross-border observational capabilities, afforded by sensor range, offer pseudo-satellites a degree of legal protection during peacetime.

However, the persistent surveillance offered by HAPS operating near international borders or from international airspace might raise concerns among sovereign states. For instance, radar-based observation can be directly evidenced through the identification of emitted radio frequencies, but passive sensing (e.g., optical imaging or signals intelligence) leaves no comparable trail. While states could infiltrate HAPS operations by using human or cyber intelligence to gather evidence, such findings would likely remain contested or dismissed as fabricated.

At the same time, persistent surveillance can enhance regional stability by delivering timely information about potential malicious activities, either pre-emptively or in real-time. These capabilities are valuable in counterinsurgency and counterpiracy operations, as well as in responding to widespread civil unrests, where high-performance surface-to-air missiles are

¹³ HAPS deployment scenarios have been simulated using the ANSYS Systems ToolKit software by the author.

unlikely to be deployed. Persistent overhead surveillance can also aid disaster response, including environmental or industrial catastrophes and mass displacement events. Beyond defence and security applications, HAPS platforms offer commercial and governmental uses.

One major commercial application for HAPS is telecommunication. The limited range of HAPS platforms (typically covering a 300-400 km diameter area depending on the radiocommunication system) is advantageous for spectrum management compared to satellites. Pseudo-satellites can rapidly augment or replace terrestrial communication services in disaster zones or remote areas during military or security operations.

These platforms support critical command-and-control functions within their coverage area and can free up satellite capacity for long-range communications. An increasingly popular application is the integration of HAPS with terrestrial cellular networks, enabling lightweight base stations to provide mobile connectivity where ground-based infrastructure is unavailable.

A few commercial operators have also begun marketing high-altitude balloon flights as “near-space” or “edge of space” experiences. While these flights are useful for testing space-related technologies and materials or in scientific research, their primary appeal at present lies in providing leisure experiences for passengers¹⁴.

4. Mesospheric Hypersonic Flight Operations

Fixed-wing aircraft, airships and balloon-based HAPS vehicles cannot operate in the mesosphere due to an extremely low air density¹⁵. In this layer useful lift can only be generated by flying at extreme speeds, many times faster than the speed of sound. Such speeds can be reached by rocket-launched vehicles (e.g. hypersonic gliders¹⁶) or scramjet-powered aircraft¹⁷.

¹⁴ David, 2005.

¹⁵ Although, in theory, helium or hydrogen could still generate lift in the mesosphere, a structural system is required for operation. This includes an envelope to contain the lifting gas, a gondola to carry the payload, energy and control systems, and the payload itself. Without these components, the balloon cannot exist or function.

¹⁶ Good practical examples of hypersonic gliders are the specialised nuclear warhead re-entry vehicles. For more information, see <https://missilethreat.csis.org/missile/avangard> and https://scholar.harvard.edu/files/bunn_tech_of_ballistic_missile_reentry_vehicles.pdf (Accessed: 26 February 2024).

¹⁷ Henry and Slaars, 2022.

Hypersonic gliders are launched as payloads of purpose-built rockets or modified space launchers. They may be released directly onto mesospheric trajectories or launched beyond the mesosphere into the lower regions of what is commonly understood as outer space. These vehicles then perform a re-entry and extend their aerobraking flight into a glide phase that allows them to take on operational activities. As gliders, they convert potential and kinetic energy to generate lift, descending and decelerating in the process. They may transition into supersonic and eventually subsonic flight, akin to the Space Shuttle Orbiter or the Buran, for landing or continue freefall, akin to ballistic warheads.

The scramjet¹⁸ engine operates at hypersonic airspeeds¹⁹, providing continuous thrust to the vehicle. It can sustain re-entry glide or serve as the primary propulsion for a vehicle ascending under its own power into the mesosphere²⁰. With thrust vectoring, a scramjet can augment the lift generated by the vehicle's aerodynamic surfaces if necessary.

While air density limits the service ceiling of pseudo-satellites by restricting available lift, hypersonic vehicles face a different constraint: the air density must remain below a certain threshold to prevent overheating from friction and compression heating. The upper operational limit is dictated by the availability of atmospheric oxygen, required by scramjets for combustion. Gliders simply follow their re-entry trajectory until they reach denser layers of the atmosphere, where hypersonic gliding becomes feasible.

The key distinction between a hypersonic vehicle and a ballistic or quasi-ballistic trajectories lies in manoeuvrability. Hypersonic vehicles can alter their flight paths to fulfil operational objectives through atmospheric interactions. In military applications, this capability is used to evade air defence systems, such as anti-ballistic missile interceptors, or to enable

¹⁸ The scramjet (supersonic combustion ramjet) engine is a variant of the ramjet engine. Ramjets are air-breathing jet engines that have no moving parts in their internal structure, unlike conventional turbojet engines where the compressor and turbine sections contain moving parts. While ramjets operate at supersonic airspeeds with subsonic airflow in the combustor, scramjets are designed for hypersonic speeds and feature supersonic airflow through the combustor. For further details, see <https://skybrary.aero/articles/scramjet> (Accessed: 26 February 2024).

¹⁹ Hypersonic flight usually means airspeeds higher than Mach 5.

²⁰ As ramjets, and thus scramjets cannot be launched from a standing start, there needs to be a different initial propulsion system that accelerates the vehicle to enable the take off. This propulsion system can be an integral part of the vehicle or can be a part of a carrier vehicle that supports the early part of the flight of the main vehicle.

precision strikes. Hypersonic vehicles equipped with suitable sensors can also be employed for reconnaissance. In commercial contexts, hypersonic flight could revolutionise fast cargo and passenger delivery, including logistical support for military operations.

Regulatory challenges for hypersonic mesospheric vehicles stem from their flight altitude. Although technically aerial vehicles, their flight altitude at 70-80 km places them beyond the range of most air defence missile systems and outside the detection capabilities of most air defence radars. For most European states, there is little practical difference between a space satellite in orbit at 400 km and a hypersonic vehicle at 75 km: both are effectively undetectable and untargetable with current defence capabilities.

Boost-glide hypersonic vehicles²¹ introduce further complexities. Their flights begin as payloads on space-capable launch vehicles, akin to conventional space mission. Depending on the capabilities of their launch vehicles and operational requirements, they may follow ballistic suborbital trajectories, fractional orbits²², or even complete multiple orbits. During re-entry, their behaviour resembles that of spacecraft; however, their operational phase begins once they re-enter denser atmospheric layers.

With sufficient kinetic energy for gliders or adequate thrust for scramjet vehicles, it is theoretically possible to dip into the atmosphere, execute hypersonic flight in the mesosphere, and to generate additional lift to exit the denser atmosphere, continuing on a suborbital or orbital trajectory²³. This atmospheric phase could be used to complete specific

²¹ Sanger and Bredt, 1944, p. 6.

²² A fractional orbit vehicle is launched onto a trajectory that could theoretically allow multiple orbits around the Earth (unlike a suborbital trajectory, which lacks the combined energy for even a single orbit). However, the vehicle executes a re-entry braking burn to decelerate and initiate atmospheric re-entry. Fractional orbit vehicles (warheads) were conceptualised during the Cold War to avoid detection by ballistic missile defence radars. The Soviet R36O missile-warhead system was developed, tested, deployed and eventually withdrawn, largely due to the advent of simpler alternatives and restrictions imposed by the SALT-II Treaty, which prohibited the development and deployment of such weapons systems.

²³ This manoeuvre is also employed during the re-entry of spacecraft that reach the entry interface – the region in the atmosphere where aerodynamic effects begin to significantly influence the flight trajectory – at higher than usual speeds. Known as skip re-entry, this technique involves the spacecraft entering the atmosphere and initiating aerobraking while simultaneously generating aerodynamic lift to raise its trajectory back into outer space. This intermediate space leg, being suborbital due to the loss of speed during the first atmospheric flight segment, inevitably results in a second re-entry and further aerobraking.

missions, utilise aerodynamic forces for directional changes, or alter orbital inclination. Such manoeuvres have significant military applications.

Ballistic missile defence systems use sensors – ground-based and space-based optical systems and radars – to calculate a weapon's trajectory, predict its impact point, and identify its launch site. Hypersonic vehicles capable of sudden directional changes followed by exoatmospheric flight complicate these calculations, reducing the preparation time available for terminal defence interceptors. Similar effects can be achieved with endoatmospheric hypersonic manoeuvring. Combined, these capabilities allow multiple directional changes across atmospheric and exoatmospheric phases, making interception efforts more challenging. The termination of the INF Treaty and the proliferation of intermediate-range ballistic missiles have enabled countries outside the treaty to deploy such re-entry-capable vehicles.

For satellites, changing orbital inclination (or orbital plane change)²⁴ is a fuel-intensive manoeuvre and is rarely performed²⁵. However, such adjustments can enhance coverage areas or revisit times for Earth observation satellites. They may also help avoid hazardous zones containing adversarial counterspace weapons or evade co-orbital threats. Satellites capable of dipping into the atmosphere for directional changes reduce the cost of these adjustments. By decelerating to enter the atmosphere and subsequently accelerating to re-establish a stable orbit, they consume far less fuel than a direct orbital plane change. The legal and regulatory challenges stem from the fact, that from a physics perspective, entering the atmosphere during a manoeuvre is functionally identical to any re-entry, while exiting the atmosphere resembles a conventional launch. Although the atmospheric segment occurs at altitudes far above those of traditional

Skip re-entry reduces the thermal load on the spacecraft, thereby decreasing the weight and volume of the thermal protection system required. The Orion spacecraft, developed for the Artemis Moon programme, will routinely utilise skip re-entry during its operations.

²⁴ Braeunig, 2013.

²⁵ An inclination change is always required to place geostationary satellites into their operational orbit unless they are launched directly from the equator. Historically, Sea Launch was the only launch vehicle operator to routinely launch from the equator; however, its operation ceased due to the conflict between Ukraine and Russia. For geostationary satellites, the inclination change is accounted for as part of the launch sequence rather than the satellite's operational lifetime. Other satellites are usually launched onto trajectories that position them directly in their intended orbital plane, obviating the need for inclination changes post-launch. Orbital plane changes during satellites' operational phase are exceedingly rare.

aviation activities, the overall operation fundamentally remains a spaceflight endeavour. Importantly, there is no intention to remain within the denser atmospheric layers or to terminate the spaceflight, even if the vehicle performs actions characteristic of atmospheric flight at altitudes not commonly considered part of the outer space.

A relevant historical precedent is the case of the Soviet DS-MO satellites, specifically Kosmos 149 and 320, which exploited aerodynamic forces in orbit for stabilisation, effectively using these forces for steering purposes²⁶. These satellites operated at an altitude of approximately 250-300 km, typically regarded as spaceflight. While their orbits were Keplerian and atmospheric effects did not significantly sustain their flight, these effects were sufficient to act on the stabilising skirts of the satellites, enabling them to maintain a mission-specific attitude relative to the Earth. Though this is not physically identical to the manoeuvring involved a skip-re-entry-style dip into denser atmosphere, it is conceptually comparable. In both cases, aerodynamic forces are deliberately utilised to achieve a specific objective. The absence of an internationally recognised legal boundary between airspace and outer space further complicates the issue. One could argue that skip-re-entry manoeuvring is analogous to the use of aerodynamic forces for spacecraft stabilisation, thereby blurring the lines between atmospheric and space operations.

5. Propulsion-Supported Flight Operations in a Very Low Earth Orbit

The lower region of the thermosphere, roughly at altitudes of 150-200 km, does not support aerodynamic flight, nor is it necessary. At these altitudes, the thin atmosphere permits travel at orbital velocity without significant compression heating of the vehicle's outer surfaces, negating the need for aerodynamic lift to sustain the flight. However, the residual atmospheric drag still decelerates spacecraft significantly, rendering such orbits inherently unstable. Re-entry into the denser atmosphere occurs within hours or, at most, days. Altitudes around 200 km are typically used as initial (parking) orbits for spacecraft destined for higher altitudes. These parking orbits allow for system checks and provide a safety margin; if the mission cannot proceed, natural orbital decay removes the spacecraft from the orbit

²⁶ Krebs, no date.

within a relatively short and acceptable timeframe²⁷. The density of the thermosphere at these altitudes is variable, influenced by space weather, which in turn affects the atmospheric drag and makes predicting spacecraft trajectories in this region more challenging. For these reasons, extended operations are not commonly planned at such low altitudes.

Operating at a lower altitude, however, offers significant benefits. Sensor resolution improves²⁸, communication link budgets (e.g., for telecommand, data downlink, or telecommunications) are enhanced, and launch costs decrease due to reduced fuel consumption or simpler launch vehicle designs.

A potential solution for extended operations in this region is the use of continuous propulsion to counteract atmospheric drag²⁹. While chemical rockets could provide the necessary thrust, ion engines are better suited for such missions. Chemical rockets operate as heat engines, using the energy releases from combustion to eject reaction mass and generate thrust. In contrast, ion thrusters draw energy from an external source – typically solar or nuclear in space – and use it to eject inert reaction mass. Ion thrusters and their power systems are more efficient, making them expedient for long-term, uninterrupted operations. Additionally, refuelling ion thrusters is simpler, as they use a single inert propellant.

Satellites equipped with continuous propulsion in the lower thermosphere (150-200 km) could remain in orbit as long as their propulsion systems are operational. They could also adjust their altitude to conserve propellant during periods of reduced operational activity, for refuelling, or for maintenance. However, these satellites would perform their primary missions at lower altitudes. Traditional space tracking systems would struggle to predict their orbits effectively, as the variable thrust enables manoeuvring and invalidates standard drag models. Moreover, continuous propulsion facilitates inclination (orbital plane) changes, further complicating trajectory predictions.

This capability offers significant advantages in defence applications. Improved resolution and communication are natural outcomes of operating in lower orbits. The greater impact, however, lies in the limitation of

²⁷ This scenario was used during the Apollo program for safety reasons, because even without propulsion, the Command Module would have re-entered within the timeframe enabled by the consumables of the life support system.

²⁸ The same angular resolution means better linear resolution at the surface.

²⁹ Chen and Lansard, 2023, p. 3.

existing space tracking and orbit determination systems. These systems are optimised for the calculation of Keplerian orbits perturbed by aerodynamic and gravitational forces in low Earth orbit³⁰. They rely on discrete measurements of position and velocity to extrapolate orbits. Continuous propulsion offsets many of these perturbations, rendering standard orbit determination models ineffective. Unless such spacecraft are tracked continuously, their predicted trajectories will be inaccurate, leading to potential errors in applications relying on this data.

For instance, orbit data is used to predict the time windows a reconnaissance satellite can observe a given ground target. Such predictions allow the observed party to time activities so as to avoid detection or to conduct deceptive observations to mislead adversaries. If the satellite's orbit changes after the last tracking observation, these predictions will fail. Units prepared to avoid detection may not be overflown, while unprepared targets may be observed unexpectedly.

Very low Earth orbit satellites with continuous propulsion will necessitate unique traffic management systems. It is worth noting that universally applicable traffic management regulations do not yet exist for conventional satellites. However, established tracking, orbit determination, and collision avoidance protocols for higher operational altitudes generally provide sufficient lead time for analysis and negotiations. For propulsion-supported satellites in very low Earth orbit, such lead times are unlikely due to limited tracking and inaccurate orbit modelling.

The agility facilitated by continuous propulsion and thrust vector control provides manoeuvrability comparable to that of atmospheric vehicles, albeit with much lower intensity. The freedom of movement, unconstrained by the traditional laws of orbital mechanics, distinguishes these satellites from conventional space vehicles. As with the stratospheric and mesospheric vehicles discussed earlier, propulsion-supported satellites in very low Earth orbit require tailored flight rules to ensure safe and efficient operations.

6. Regulatory Challenges of Higher Atmospheric Flight Operations

Conventional aerial flight operations typically occur within the troposphere and occasionally in the lower stratosphere. Only a limited number of aircraft

³⁰ Vetter, 2007, p. 246.

operate above 20 km, predominantly military reconnaissance or counter-reconnaissance vehicles and governmental scientific research missions.

Conversely, traditional spaceflight operations take place in the middle and upper thermosphere, generally above 200 km. Spacecraft entering the lower thermosphere almost invariably do so during re-entry, whether controlled or uncontrolled, as part of terminating their spaceflight.

Flight activities in the higher stratosphere and the mesosphere that do not align with these conventional categories require specific regulatory frameworks. The case studies presented here illustrate the technological differences between traditional air and space activities and the unique challenges posed by these operations, such as inability to apply Kepler's laws for orbit determination in the case of propulsion-supported satellites.

However, as discussed earlier, physics does not provide clear-cut boundaries for regulatory purposes. For example, a stratospheric balloon or airship interacts with the atmosphere in the same way as similar vehicles operating in the troposphere. Similarly, a spacecraft undergoing re-entry at an altitude slightly above the entry interface—at approximately 400,000 feet³¹—experiences the same aerodynamic forces as a hypersonic vehicle operating in the upper mesosphere.

The distinguishing factor for these new flight activities, and the basis for the regulation, lies in the intent behind the operations. A shared understanding of the objectives and nature of these activities is crucial for developing rules and regulations. The difficulty, however, is that legal definitions cannot rely solely on such “common understandings”; they must be precise and robust enough to withstand scrutiny and challenges.

Despite these complexities, the altitude boundaries discussed earlier effectively separate these unconventional flight operations from the lower airspace (used for conventional aviation) and the higher outer space (used for traditional spaceflight). Establishing a distinct intermediate zone with specific regulations would not resolve all longstanding issues, such as the legal status of suborbital flights. However, it would provide a framework for managing new activities in this region, addressing current regulatory gaps.

Experts have explored the concept of an intermediate zone between airspace and outer space. H. Liu and F. Tronchetti described³² this as the “Exclusive Utilization Space” situated between 18 and 100 km, comparable to the Exclusive Economic Zone in maritime law. However, this proposal

³¹ Rea, 2016, p. 1.

³² Liu and Tronchetti, 2019

excludes operational altitudes of boost-glide vehicles and propulsion-supported satellites. Furthermore, its upper limit of 100 km, based on the assumption that this altitude marks the lower boundary of outer space, lacks codification and fails to address key issues discussed earlier.

T. Gangale in his “Draft Space Delimitation Convention”³³ proposed an international “mesospace”³⁴ between 30 km (the practical average upper limit for enforcing state sovereignty) and 81 km (the minimum perigee for a satellite to complete at least one orbit at the time of writing, though this value is dynamic). This proposal also centres on conventional spaceflight technologies and perceives mesospace as a transitional region between airspace and outer space. However, as shown in the case studies, these new flight activities are primarily operational, rather than merely transitional.

J.N. Pelton introduced the concept of a “proto-zone” encompassing altitudes between 21 and 160 km³⁵. His reasoning aligns with the perspectives in this article. Pelton further subdivided the proto-zone to address security concerns, drawing on the zoning approach in the Law of the Sea Convention. Below 21 km, existing air traffic control rules would apply. Between 21 km and 42 km (or another arbitrary chosen altitude), a “contiguous zone” could support law enforcement activities, albeit adapted to proto-zone operations³⁶. From 42 km to the top of the proto-zone (proposed as 160 km by Pelton, but potentially extendable to 200 km to include the operating range of propulsion-supported satellites), regulations could mirror the Exclusive Economic Zone concept in maritime law, although with a focus on traffic management rather than economic considerations. For instance, regulations might mandate continuous status reporting, akin to ADS-B in air traffic management, to supplement ground- and space-based tracking systems.

³³ The book ‘How High the Sky?: The Definition and Delimitation of Outer Space and Territorial Airspace in International Law’ by Thomas Gangale contains in its 20th chapter an excellent historical summary of proposals to define an intermediate zone between airspace and outer space.

³⁴ Gangale, 2018, pp. 424-458.

³⁵ Pelton, 2016.

³⁶ The contiguous zone in sea law is the area to enforce the customs, fiscal, immigration and sanitary regulations of the sovereign state. In the proto-zone, the vertical contiguous zone would most likely serve as the volume to enforce identification, overflight restrictions, traffic rules and environmental protection rules (air pollution in the stratosphere can have serious consequences like increased global warming and ozone depletion).

Codifying the proto-zone could address most existing and emerging challenges related to higher atmospheric or “near-space” operations, irrespective of the unresolved delimitation issues between airspace and outer space. Among the various proposals for defining the intermediate zone, J.N. Pelton’s approach stands out for its comprehensiveness, practical adaptability, and potential to address real-world concerns effectively.

7. Summary

Technological advancements continue to transform ideas into practical applications. To regulate and harmonise these emerging operations, it is essential to establish universally applicable rules for all stakeholders. The absence of regulations and transparency fosters distrust and promotes unfriendly competition. Without clear guidelines, any new development risks are being perceived as offensive or destabilising. Conversely, well-defined rules and regulations can facilitate the adoption of innovative technologies and operations while minimising unnecessary friction.

The social implications of any new technological activity must also be carefully considered. In the absence of regulations, these activities become subject to interpretation and can easily become targets of disinformation or misinformation campaigns by those opposing their implementation.

In this article I have highlighted three examples of emerging technologies that, while distinct in nature, collectively illustrate the challenges arising from the lack of clear legal and regulatory boundaries. These examples represent only a fraction of the advancements currently under development, and we can be certain that innovation will continue to drive the invention of new concepts and technologies, perpetuating this cycle. These operations all transpire within a physical region around the Earth that can be regarded as part of the atmosphere and outer space simultaneously. Establishing a clear boundary between airspace and outer space is practically impossible due to the lack of an unequivocal factor defining such a demarcation. However, as demonstrated through this article, this intermediate zone exhibits characteristics that distinguish it from both airspace and outer space.

It is therefore recommended that this intermediate zone, referred to here as the “proto-zone”, be formally delimited from the neighbouring spaces. This would pave the way for the development of specific rules and regulations tailored to its unique challenges. While such a framework would

not resolve all the issues stemming from the existing space legal regime, it could address key questions concerning stratospheric flight operations, mesospheric hypersonic flight and propulsion-supported satellites. Each of these activities is fundamentally different from operations in adjacent zones, even if they may appear superficially similar. By emphasising these distinctions, this article seeks to draw attention to the necessity of a separate regulatory regime for the proto-zone.

Finally, it is important to underscore that regulatory challenges cannot be resolved solely by technologists. These efforts require international collaboration among legal and social experts, with the support and input of technologists. Modern technologies are inherently complex and multifaceted; oversimplification, as seen during the development of the current legal framework of space, risks producing unsustainable regulations. A holistic approach, combining technical expertise with legal and social insight, is essential to create a robust and adaptable regulatory environment for the future.

Bibliography

- [1] Aragón-Zavala, A., Cuevas-Ruiz, J. L., Delgado-Penín, J. A. (2008) *High-Altitude Platforms for Wireless Communications*. New York: John Wiley & Sons, Ltd.
- [2] Bartóki-Gönczy, B., Sipos, A. (2022) 'A világűr és a légtér elhatárolása' in Bartóki-Gönczy A., Sulyok G. (eds.) *Világűrjog*. 1st edn., Budapest: Ludovika Kiadó, pp. 39-50.
- [3] Braeunig, R. A. (2013) *Orbital Mechanics*, [Online]. Available at: <http://www.braeunig.us/space/orbmech.htm#maneuver> (Accessed: 17 April 2023).
- [4] Chen, S., Lansard, E. (2023) *Orbit Manoeuvre Strategies for Very Low Earth Orbit (VLEO) Satellites*, [Online]. Available at <https://www.researchgate.net/publication/375027798> (Accessed: 21 April 2023).
- [5] Colozza, A., Dolce, J. L. (2005) *NASA/TM—2005-213427 High-Altitude, Long-Endurance Airships for Coastal Surveillance*, [Online]. Available at <https://ntrs.nasa.gov/api/citations/20050080709/downloads/20050080709.pdf> (Accessed: 27 February 2024).
- [6] David, L. (2005) *Sky Trek To The 'Near Space' Neighborhood*, [Online]. Available at: <https://www.space.com/1761-sky-trek-space-neighborhood.html> (Accessed: 27 February 2024).
- [7] Gangale, T (2018) *How High the Sky?: The Definition and Delimitation of Outer Space and Territorial Airspace in International Law*. Leiden: Brill Nijhof pp. 424-441; <https://doi.org/10.1163/9789004366022>.

-
- [8] Henry, J., Slaars, E. (2022) *Hypersonic Missiles: Evolution or Revolution?*, [Online]. Available at <https://www.navalnews.com/naval-news/2022/11/hypersonic-missiles-evolution-or-revolution/> (Accessed: 14 March 2024).
- [9] Krebs, G. D. (no date) *DS-MO (Opticheski)*, [Online]. Available at https://space.skyrocket.de/doc_sdat/ds-mo.htm (Accessed: 17 April 2023).
- [10] Liu, H., Tronchetti, F (2019) *The Exclusive Utilization Space: a new approach to the management and utilization of the near space*, [Online]. Available at <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1983&context=jil> (Accessed: 29 July 2024).
- [11] McDowell, J. C. (2018) ‘The edge of space: Revisiting the Karman Line’, *Acta Astronautica*, 151, pp. 668-677; <https://doi.org/10.1016/j.actaastro.2018.07.003>.
- [12] Pelton, J. N. (2016) *Urgent Security Concerns in the “Proto-zone”*, [Online]. Available at: https://www.mcgill.ca/iasl/files/iasl/3._j._pelton.pptx (Accessed: 28 December 2023).
- [13] Rea, J. R. (2016) *Orion Exploration Mission Entry Interface Target Line*, [Online]. Available at: <https://ntrs.nasa.gov/api/citations/20160001438/downloads/20160001438.pdf> (Accessed: 27 July 2024).
- [14] Sänger E., Bredt, I. (1944) *A rocket drive for long range bombers Deutsche Luftfahrtforschung UM 3538*, [Online]. Available at: <http://www.astronautix.com/data/saenger.pdf> (Accessed: 28 December 2023).

- [15] Vetter, J. R. (2007) ‘Fifty Years of Orbit Determination: Development of Modern Astrodynamics Methods’, *Johns Hopkins APL Technical Digest*, 27(3), [Online]. Available at: <https://secwww.jhuapl.edu/techdigest/content/techdigest/pdf/V27-N03/27-03-Vetter.pdf> (Accessed: 21 April 2023).
- [16] *Earth’s Atmosphere: A Multi-layered Cake*, [Online]. Available at: <https://science.nasa.gov/earth/earth-atmosphere/earths-atmosphere-a-multi-layered-cake/> (Accessed: 16 February 2024).
- [17] *In-flight break-up involving Airbus Zephyr unmanned aerial vehicle*, (2020) [Online]. Available at: https://www.atsb.gov.au/sites/default/files/media/5778702/ao-2019-056_final.pdf (Accessed: 26 February 2024).
- [18] *Ultra thin film balloon*, (2013) [Online]. Available at: <https://stratocat.com.ar/fichas-e/2013/TAK-20130920.htm> (Accessed: 27 February 2024).

MARKO JURIC^{*}

Legal regulation on the use of artificial intelligence for national security purposes in Europe^{}**

ABSTRACT: This paper analyses the regulation of the use of AI for national security purposes in Europe. After a brief mapping of most relevant uses of AI for national security purposes, applicable legal framework is analysed. Both the EU AI Act and the Council of Europe's AI Convention provide for broad exceptions regarding the use of AI for national security purposes. This covers activities of both public and private entities acting in the national security domain. In such circumstances, personal data protection law is seen as possessing the most direct impact on the use of AI for national security purposes. In this context, the notion of personal data is explained, emphasizing that any information relating to an identified or identifiable person qualifies as personal data under both the GDPR and Convention 108. The processing of this data, which is broadly defined, can be subject to data protection laws even in national security contexts, provided it meets certain criteria.

The research shows that while there is a lot of uncertainty when it comes to the application of personal data rules to national security situations, existing case-law indicates that application of those rules is not fully excluded. On the contrary, it is to be expected that at least when private entities are involved in data processing operations, personal data protection law might prove to be very effective. Also, it is to be anticipated that the ECHR will play a major role in ensuring that uses of AI for national security purposes remain in line with requirements of democratic society.

KEYWORDS: AI, national security, AI Act, AI Convention, personal data protection.

^{*} Associate professor, Faculty of Law, University of Zagreb, Croatia.
<https://orcid.org/0000-0001-8499-4193>, marko.juric@pravo.unizg.hr.

^{**} The research and preparation of this study was supported by the Central European Academy.

1. Introduction

Artificial intelligence (AI) promises to revolutionise governance in many aspects of private and public affairs. One area that seems particularly ready for such changes is national security.¹ As expressed by the United Kingdom's Government Communications Headquarters (GCHQ), 'an increasing use of AI will be fundamental to GCHQ's mission of keeping the nation safe'.² However, at the same time, it is well understood that the use of AI for national security presents many ethical and legal challenges. This study focusses on the latter. In doing so, we attempt to analyse how the use of AI for national security purposes is regulated from the perspective of European law. This is a rather complicated task, for various reasons.

First, as others have noted, the notion of national security is vague and ambiguous,³ and it ultimately depends on the specific national legal and institutional framework. To simplify things for the purpose of this study, we draw the line between military and non-military actions. Therefore, we consider national security to be a broader concept concerned with protection from non-military threats. Consequently, in this study, we do not analyse specific issues related to the use of AI in the context of military (e.g. most prominently, the use of lethal autonomous weapons systems) and defence activities. Likewise, we also exclude ordinary law-enforcement activities conducted during investigations and prosecution of criminal offences.

Second, when it comes to the regulation of AI, we see a very complicated system of national and supranational legal rules in Europe that impact AI either directly or indirectly. Attached to this is also a complex system of shared competences between organisations such as the European Union (EU) and Council of Europe and their member states, with the Court of Justice of the EU (CJEU) and European Court of Human Rights (ECtHR) playing very prominent roles.

When it comes to regulation of AI, the year 2024 has been very productive for European legislators. First, after several years of

¹ See extensively in Montasari, 2022.

²² GCHQ, (no date) *Pioneering a New National Security: The Ethics of Artificial Intelligence*, [Online]. Available at: <https://www.gchq.gov.uk/files/GCHQAIpaper.pdf> (Accessed: 10 September 2024) p. 4.

³ Dieu and Montasari, 2022, p. 20; CCBE, 2019, note the lack of a common European concept of "national security" and various national interpretations.

negotiations, the EU AI Act was finally enacted in June 2024.⁴ Second, at almost the same time, the Council of Europe's *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CoE AI Convention) was also prepared.⁵ With these legal instruments in place, it is possible to argue that Europe is becoming a global leader in the regulation of AI.⁶ However, it is open for debate to what extent and how the use of AI specifically for national security purposes will be impacted by these new rules.

To provide a broader overview of the legal rules applicable to the use of AI in the national security domain, this study first seeks to elaborate the possible uses of AI in that domain and the corresponding legal considerations. Second, we analyse which legal sources of the EU and Council of Europe law might prove relevant for regulating AI for national security purposes. In doing so, in addition to the abovementioned AI Act and CoE AI Convention, we consider conditions and safeguards arising under human rights law and the impact of personal data-protection rules. We finish by outlining the most important findings regarding crucial moments of applying legal rules to the use of AI in the context of national security.

2. Possible uses of AI in the national security domain and corresponding legal considerations

The potential of AI in the national security domain seems almost unlimited, but at the same time, even a cursory overview of the relevant literature clearly indicates that it is accompanied by many legal, ethical, and policy considerations.⁷ As indicated in section 1, the focus of this study is on legal challenges, specifically those that might arise from the perspective of European law.

However, to identify the legal challenges, it is necessary to first determine the actual uses of AI in national security, and that is not

⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act, hereinafter: the AI Act), OJ L, 2024/1689, 12.7.2024.

⁵ Council of Europe, 2024.

⁶ For a historical overview of AI regulation in Europe, see Jurić, 2024.

⁷ See, for instance, Dieu and Montasari, 2022.

necessarily an easy task. There are multiple challenges here. First, problems arise because the notion of national security itself is relatively broad and vague. Therefore, whether some AI is used for national security purposes depends on how we define those purposes. Second, and more importantly, activities of national security authorities are done, almost by default, in closed and relatively secret environments. Although there are typically at least some elements of transparency, they usually do not go as far as to provide very precise elaborations of the technologies used, and there are solid reasons for such an approach. For instance, it was successfully argued during negotiations for the AI Act that registering certain AI systems used by law enforcement in public databases would pose a security risk, affect the capabilities of the authorities, and expose the capabilities of law enforcement to criminals and hostile states.⁸ These reasons are emphasised even more in the national security domain. Therefore, while it is known that AI can be very useful in combining and correlating various data sources to create actionable intelligence, it will not be known to the public which data sources are analysed and using which technologies, or this will be described in only very general terms. Therefore, in this study, we describe possible uses of AI in the national security domain in only relatively broad terms based on the findings of other academic works.⁹

The use of AI in national security is sometimes classified into (1) automation of administrative and organisational processes, (2) cybersecurity purposes, and (3) intelligence analysis.¹⁰ Although the benefits of AI in the national security context are usually described in defensive terms, it is necessary to emphasise that the sword cuts both ways. That is, 'state's security can both be strengthened and threatened by the recourse to AI'.¹¹ For instance, AI can be used to not only facilitate attacks on critical information infrastructure but also prevent such attacks. Looking from an adversarial perspective, AI can very be used well for purposes that compromise national security. The Royal United Services Institute categorises threats in this category into those against (1) digital, (2) political, and (3) physical security.¹²

⁸ Palmiotto, 2025.

⁹ Babuta, Oswald, and Janjeva, 2020; Benzie and Montasari, 2022; Dieu and Montasari, 2022.

¹⁰ Babuta, Oswald, Janjeva, 2020, pp. 8–16.

¹¹ Dieu and Montasari, 2022, p. 24.

¹² Babuta, Oswald, and Janjeva, 2020, pp. 16–19.

2.1. *Intelligence analysis*

Advancements in intelligence analysis seem to be at the top of the expected benefits when it comes to possible uses of AI in the context of national security.¹³ The reason for this lies in the fact that national security agencies increasingly face the problem of “information overload.”¹⁴ Namely, with improvements in their ability to tap into richer and deeper data sources, they now have the possibility of collecting data on a previously unimaginable scale. However, collecting data on a massive scale is much easier than processing it and turning it into actionable information. Moreover, not only the quantity but also the complexity of data are increasing. This is because data are very frequently found in unstructured and disparate datasets.¹⁵ All information—be it from public registers, communication networks, webpages and other open sources, or various sensor systems—can prove very valuable to national security agencies, especially if it is possible to correlate it. Therefore, what is really at stake is the ability ‘to make sense of the data lives of thousands of people in ... real time’.¹⁶

In our opinion, intelligence analysis using AI for national security purposes might trigger personal data considerations and generally raise issues of interference with fundamental rights, particularly privacy. Whether this will be the case depends on whether personal data are being processed (see section 3.4) or whether the data or the manner of their processing fall within the notion of private life (see section 3.3).

2.2. *Behavioural analytics*

Behavioural analysis might be seen as a subset of intelligence analysis. However, the focus here is on the application of AI to data regarding individuals, with the aim of generating forecasts about human behaviour.¹⁷ Such predictions might include ‘threat detection, predicting threats to individuals in public life, identifying potential intelligence sources who may be susceptible to persuasion and predicting potential terrorist activity before it occurs’.¹⁸

¹³ See also extensively in Jensen, Whyte, and Cuomo, 2019.

¹⁴ Babuta, Oswald, and Janjeva, 2020, p. 2.

¹⁵ Ibid, p. 11.

¹⁶ Ibid, p. 3.

¹⁷ See extensively in Ferdin et al., 2024.

¹⁸ Babuta, Oswald, and Janjeva, 2020, p. 13.

Such practices can be seen as interfering with many human rights. For instance, they could, under certain conditions, be characterised as profiling in the context of personal data-protection law, and they also give rise to other considerations under that branch of law. Similarly, application of such technologies could be seen as a (particularly serious) interference with fundamental rights to privacy and, in certain scenarios, freedom of expression. Finally, it is particularly due to risks inherent in such practices that they are considered as the ones posing “unacceptable risk” in the context of the AI Act and are therefore prohibited. However, as shall be seen below, that limitation is not applicable to the use of such technologies in the national security context.

2.3. Content moderation

When it comes to threats against political security, one main concern seems to be the use of deepfakes in the form of images or videos, including the ones produced using generative AI.¹⁹ When employed in the context of political campaigns or public debates, such content ‘can be used to fuel disinformation, erode trust and compromise democracy’.²⁰ Generally, although there is a lot of debate about the exact impact of misinformation and disinformation, it is recognised that they can lead to harmful consequences.²¹ The same goes for various types of racist or xenophobic content,²² genocide denial, incitement to extremism or terrorism, etc.

In terms of legal issues, using AI for content moderation purposes will very likely give rise to freedom of expression considerations. Moreover, when moderation is done by analysing the content of electronic communications, it is equally likely that privacy and personal data considerations will arise.

¹⁹ Benzie and Montasari, 2022, pp. 6–11.

²⁰ Babuta, Oswald, and Janjeva, 2020, p. 18.

²¹ Benzie and Montasari, 2022, p. 11.

²² Around which there is strong international consensus that it should be prohibited. See Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

3. How is the use of AI for national security purposes regulated at the level of European law?

Some typical use scenarios for AI in the national security domain have been outlined above. We now turn to the issue of legal regulation of those activities. In doing so, we focus on the regulation at the European level, through legal instruments of the EU and the Council of Europe, and we begin by outlining the scope of application and possible impact of the most relevant and recent EU and Council of Europe sources of AI regulation.

3.1. *AI Act*

After several years of negotiations, the EU AI Act was finally enacted and entered into force in July 2024. Even though it will take until 2 August 2026²³ for it to become fully operational, it is already starting to impact European AI producers and deployers, as they have approximately two years to bring their activities in compliance with the new law. The AI Act is a complex piece of regulation, seeking to provide for a comprehensive risk-based regulatory framework for AI in the EU. In a nutshell, it does so by categorising AI systems into systems of unacceptable, high, limited, and minimal risk and subjecting them to a specific regulatory regime. Systems posing unacceptable risk are prohibited from use, and most of the regulation covers high-risk systems and general-purpose AI models.

From the perspective of the topic discussed in this study, the key question is to what extent and how the AI Act can impact the use of AI for national security purposes. At first sight, it appears that the answer to this question is rather simple, as activities pertaining to national security are excluded from its scope.²⁴ Namely, Article 2(3) of the Act prescribes as follows:

3. This Regulation does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.

This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with

²³ AI Act, Art.113.

²⁴ For an overview of the legislative process leading to this outcome, see Palmiotto, 2025.

or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

While there is some interesting legislative history to this provision in terms of competing proposals,²⁵ the fact is that the AI Act contains a broad exception for national security, prescribing that it applies ‘regardless of the type of entity carrying out those activities’. Such phrasing seems different from the one in other sources of secondary EU law, which usually only stipulate that an act shall not apply to activities falling outside the scope of EU law. According to explanations provided in Recital 24, the purpose of this clarification is to make it explicit that it is irrelevant whether the entity putting into service or using the AI system for national security purposes is a public or private entity. While the reasons for this clarification are not fully elaborated in the AI Act, they might have some connection with the fact that in certain cases related to surveillance of electronic communications, the CJEU has drawn a distinction between activities undertaken for national security purposes based on the type of entity conducting those activities (see section 3.4).

In any case, the intention to provide for a broad exception for using AI in the context of national security was successful. However, this has profound consequences, as it places certain categories of AI completely out of scope of the regulation. This includes AI systems posing what is described as “unacceptable risk,” which might play an important role in the context of national security. These include AI systems that²⁶

- are used for the evaluation or classification of natural persons or groups of persons based on their social behaviour or known, inferred, or predicted personal or personality characteristics, with the social score leading to certain negative outcomes;
- are used for making risk assessments of natural persons to assess or predict the risk of a natural person committing a criminal offence;

²⁵ Palmiotto, 2025.

²⁶ AI Act, Art. 5.

- create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;
- categorise natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation; and
- represent “real-time” remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement.

In such circumstances, we can only conclude that the AI Act provides for no limitation when it comes to the use of AI for national security purposes. This of course comes with an important caveat—supervision of the CJEU. Being the ultimate interpreter of EU law, it is likely that the CJEU will eventually be asked to interpret the scope of exceptions from the AI Act’s Article 2(3). If the CJEU’s approach in other areas is any indication, it is not impossible that it will seek to interpret that exception narrowly. On the other hand, the AI Act and its drafting process clearly indicate that there was strong consensus about the idea that national security remains the sole responsibility of member states, and therefore the Act should not impact those activities, notwithstanding whether they are done with the assistance of private entities.

3.2. *CoE AI Convention*

While a comparative analysis of the AI Act and CoE AI Convention is outside the scope of this study, it is important to note that the latter has the potential of a much wider geographical impact for at least two reasons. First and obviously, many European countries that are not member states of the EU will rely on the CoE treaty as their main source of international law for AI regulation. Second, as is the case with many other CoE treaties, the AI Convention is, in line with its Article 31, open for accession to countries that are not parties to the CoE. While it remains to be seen whether the AI Convention will be able to gain traction among non-CoE parties,²⁷ such a development should in any case be seen as welcome.

As it is an international treaty, the CoE AI Convention creates obligations for its parties and requires them to give effect to its provisions through national law. Majority of its provisions are concerned with principles applicable to AI,²⁸ including respect of human dignity and

²⁷ As is, for instance, the case with the Convention on Cybercrime, which with time became truly a global legal instrument for the fight against cybercrime.

²⁸ CoE AI Convention, Art. 6.

individual autonomy, transparency and oversight, accountability and responsibility, equality and non-discrimination, privacy and personal-data protection, reliability and safe innovation, and remedies.²⁹ Moreover, the CoE AI Convention calls for its parties to ensure effective procedural guarantees, safeguards, and rights to persons whose fundamental rights and freedoms have been impacted by the use of AI systems.³⁰ In terms of risk management, which is the main policy in the AI Act, the CoE AI Convention provides for several general rules that need to be developed further in national law.³¹

When it comes to the issue of using AI in the context of national security and corresponding human rights considerations, it is necessary to start from the fact that the CoE AI Convention is intended to be a framework that, as explained in its preamble, means that it ‘may be supplemented by further instruments to address specific issues relating to the activities within the lifecycle of artificial intelligence systems’. However, while it is possible that additional instruments impacting the use of AI in national security domain might be agreed upon in the future, that does not seem particularly likely at the moment. This is because it is clear from the approach of the EU and, to a significant extent, of the CoE (see below) that there is generally strong support for the idea of excluding the use of AI for national security purposes from the scope of regulatory instruments.

Regarding the issue of human rights, the CoE AI Convention recognises the challenges of AI very clearly. Therefore, it specifically mentions in its Preamble that activities based on AI may ‘undermine human dignity and individual autonomy, human rights, democracy and the rule of law’, with particular emphasis on issues of discrimination and creation or aggravation of inequalities, including those against women and persons in vulnerable situations. Maybe even more relevant for the topic discussed in this study is the threat of using AI for repressive purposes in violation of human rights law, including through ‘arbitrary or unlawful surveillance and censorship practices that erode privacy and individual autonomy’.

However, when it comes to the applicability of the CoE AI Convention in the domain of national security, Article 3(2) clearly prescribes that

²⁹ Ibid, Arts. 7–14.

³⁰ Ibid, Art. 15.

³¹ Ibid, Art. 16.

A Party shall not be required to apply this Convention to activities within the lifecycle of artificial intelligence systems related to the protection of its national security interests, with the understanding that such activities are conducted in a manner consistent with applicable international law, including international human rights law obligations, and with respect for its democratic institutions and processes.

Therefore, parties to the CoE AI Convention are not required, but also not precluded, to apply the convention to their national security activities. While the phrase stating that they should not be precluded from doing so opens the door for application if a particular state so desires, it is not very realistic that countries would follow such an approach. Moreover, pursuant to elaborations in the Explanatory Report, this exception applies ‘regardless of the type of entities carrying out the corresponding activities’. It therefore follows that the CoE AI Convention generally pursues the same approach as the one taken in the AI Act when it comes to the regulation of private entities acting in the domain of national security.

Article 3(2) might seem puzzling in part where, in the context of the exception for national security purposes, reference is made to the ‘understanding that such activities are conducted in a manner consistent with applicable international law’. However, in our opinion, this signifies nothing more than what is stated in the Explanatory Report—that national security activities, while excluded from the CoE AI Convention, are nevertheless subject to the European Convention on Human Rights (ECHR; and other applicable international treaties, including other regional human rights treaties for parties that are not member states of the Council of Europe).

Moreover, the Explanatory Report makes it clear that dual-use AI systems are generally within the scope of the CoE AI Convention when they are ‘intended to be used for other purposes not related to the protection of the Parties’ national security interests and are within the Party’s obligations under Article 3’. Likewise, it is made explicit that

... all regular law enforcement activities for the prevention, detection, investigation, and prosecution of crimes, including threats to public security, also remain within the scope of the

Framework Convention if and insofar as the national security interests of the Parties are not at stake.

To sum up, although there are many differences between the EU approach in the AI Act and the CoE's AI Convention, both pursue the approach of non-applicability to national security situations. This brings us to a question: Which legal standards then remain relevant in such circumstances? In our opinion, it is necessary to first consider the general sources of European human rights law. Among these, the ECHR³² has the most important role.

3.3. ECHR

The proposal that human rights considerations are relevant in the context of national security is not controversial. To begin with, there can be no dispute that protection provided under the ECHR extends to the area of national security. In the ECHR, this follows clearly from its Articles 8, 10, and 11, all of which provide in their respective paragraphs 2 that the respective rights can be restricted in the pursuance of, *inter alia*, national security aims. Moreover, applicability of the ECHR to national security situations was confirmed by the ECtHR in numerous cases where that court considered national security needs as a legitimate aim for restricting fundamental human rights.³³ Therefore, we do not see any reason for concluding that the use of an AI system for national security purposes would somehow be outside the scope of the ECHR. On the contrary, applicability of the ECHR to such situations is reinforced by the CoE AI Convention, which in Article 3(2) refers to the understanding that when using AI for national security purposes, states must act 'in a manner consistent with applicable international law, including international human rights law obligations, and with respect for its democratic institutions and processes'.

Currently, there are no cases in which the ECtHR would discuss the use of AI in the context of national security. However, when that becomes the case, it is bound to happen in a legal context different from the one established by the AI Act or CoE AI Convention. Namely, while the AI Act (and national legislation that will implement the CoE AI Convention) are regulatory legal instruments, the ECHR is a human rights tool. Looking from the perspective of the ECHR, AI is nothing more than another

³² Council of Europe, 1950.

³³ For an overview of ECtHR's cases in the domain of national security, see ECtHR, 2013.

technology: It gives rise to human rights considerations only if and when it impacts one of the fundamental human rights recognised in the ECHR.

When analysing possible violations of the rights protected under Articles 8 and 10 of the ECHR, the ECtHR pursues the approach in which the following is analysed:

- 1) Whether there has been interference with a fundamental right protected under the relevant article of the ECHR
- 2) Whether the interference is prescribed by law
- 3) Whether the interference pursues a legitimate aim
- 4) Whether the interference is necessary in a democratic society

The catalogue of fundamental human rights and freedoms that can be impacted using AI is very broad. For instance, it is not unimaginable that the rights to life, fair trial, freedom of religion or association, free elections, and equality and non-discrimination might be, in certain cases, interfered with through the use of AI systems.³⁴ However, in the context of national security, we consider that the most likely challenges will be in relation to the protection of private and family life, home and correspondence (Article 8 of the ECHR), and freedom of expression (Article 10 of the ECHR). Although, depending on the specifics of the case, only one or both of these rights can be interfered with, the approach in either situation is generally the same and in line with the criteria mentioned above.

Recognising that national security is an accepted legitimate aim under the ECHR, the key debate will, in our opinion, be about clarity and foreseeability of the legislation governing the use of AI for national security purposes and the necessity of doing so.

In our opinion, the approach pursued by the ECtHR is sufficiently flexible to provide an adequate framework for interferences caused using AI as well. Although AI is a technology and therefore not in question, its specific characteristics are likely to be considered by the court, which has previously emphasised issues raised by new or intrusive technologies. For instance, in *S. and Marper v. United Kingdom*, the court concluded, in relation to the use of modern scientific techniques in the law enforcement sector, that

... the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any

³⁴ Dieu and Montasari, 2022, pp. 21–29.

cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.³⁵

Moreover, any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.³⁶

In addition, we can generally observe that the ECtHR does not struggle with applying the ECHR to new technologies, as it was able to address challenges posed by various new technologies in cases concerning the use of gross domestic product trackers (*Uzun v. Germany*³⁷ and *Ben Faiza v. France*),³⁸ authorities using the “surveillance database” that collects information about persons’ movements by train or air (*Shimovolos v. Russia*),³⁹ use of facial-recognition technologies (*Glukhin v. Russia*),⁴⁰ secret surveillance (*Szabó and Vissy v. Hungary*),⁴¹ etc.

In addition to the abovementioned general standards, there are several specific ones in the case law of the ECtHR that might prove valuable for addressing AI-related cases in the context of national security.

First, the ECtHR has a very permissive approach in cases regarding secret surveillance when it comes to establishing the applicant’s victim status and the existence of interference with a fundamental right. Namely, the challenge here is that, due to secrecy of measures at the national level, applicants sometimes have difficulties in proving that they have been subject to some form of surveillance. To address these challenges, the ECtHR has developed a specific test that, if satisfied, can enable applicants to have their case heard without demonstrating with certainty that they have been victims of illegality.⁴² Since activities in the domain of national

³⁵ *Case of S. and Marper v. United Kingdom* App. Nos. 30562/04 and 30566/04, 04 December 2008, para 112.

³⁶ *Ibid.*

³⁷ *Case of Uzun v. Germany* App. No. 35623/05, 2 September 2010.

³⁸ *Case of Ben Faiza v. France* App. No. 31446/12, 08 February 2018.

³⁹ *Case of Shimovolos v. Russia* App. No. 30194/09, 21 June 2011.

⁴⁰ *Case of Glukhin v. Russia* App. No. 11519/20, 04 October 2023.

⁴¹ *Case of Szabó and Vissy v. Hungary* App. No. 37138/14, 06 June 2016.

⁴² As explained in *Zakharov v Russia*, it is necessary to consider:

- 1) the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, and
- 2) availability of remedies at the national level, with the understanding that the degree of scrutiny of the ECtHR depends on the effectiveness of such remedies.

security are conducted in secrecy almost by default, criteria such as this one might also prove useful in future AI-related cases.

Second, in surveillance cases, the ECtHR found it problematic when authorities had direct access to communication data (i.e. when access was possible without further assistance from the service providers). According to the court, such systems are particularly prone to abuse, and ‘the need for safeguards against arbitrariness and abuse appears therefore to be particularly great’.⁴³ Similarly, issues of national security authorities’ direct access to various sources of data, with the aim of cross-referencing and intelligence analysis, should be analysed with these considerations in mind. Dangers of abuse are particularly relevant here, as the use of AI could greatly enhance the possibility of reviewing and analysing communication data.

Third, when it comes to the activities of national security agencies, probably the most important safeguard is an effective oversight mechanism. Security services have always had, and continue to have, fundamental importance for functioning of the state. All European countries have these institutions and task them with various duties, from intelligence collection to protection of the national security, economic well-being, and other critical interest of the state. However, since these services, due to the nature of their work, mostly operate in secret, it is also widely recognised in Europe that their proper oversight is fundamental to ensuring that these institutions both contribute to the protection of the populations they serve and respect the rule of law and human rights.⁴⁴ National practices of European countries regarding oversight of these services vary greatly, but some important elements have been identified by the ECtHR. As repeatedly stated by the court, the most important factors in this context are the (1) the independence of the supervisory authorities, their competences, and their powers and (2) the possibility of effective public scrutiny of these authorities’ work.⁴⁵ In addition to the ECtHR, very useful guidance regarding the effectiveness of oversight arrangements is provided by the Venice Commission.⁴⁶

See *Case of Zakharov v Russia* App. No. 47143/06, 04 December 2015, paras. 170–172.

⁴³ *Case of Zakharov v Russia* App. No. 47143/06, 04 December 2015, paras. 268–271.

⁴⁴ Commissioner for Human Rights, 2015, p. 5.

⁴⁵ See, for instance, *Case of Ekinzhiev v Bulgaria* App. No. 70078/12, 11 April 2022, paras. 334–347.

⁴⁶ Venice Commission, 2015.

To conclude this section, we are of the strong opinion that the ECHR remains as relevant as always, and it provides a very adequate tool for addressing human rights issues posed through the use of AI in the national security domain.

3.4. Personal data-protection law

As elaborated in section 2, be it intelligence analysis, behavioural analytics, detection of cybersecurity threats, or content moderation, AI will be about processing data. For that reason, it is impossible to outline the legal framework for the use of AI without considering the legal framework governing the use of data. While the European law might not address AI as a technology in the context of national security, it does not necessarily follow that the situation is the same regarding the regulation of data.

When it comes to data regulation, there are multiple sources of the EU and Council of Europe law that might be relevant. However, initially, it is important to start with a very basic but crucial distinction—between personal and non-personal data. Namely, what the EU and CoE legal frameworks regulate is personal data. Non-personal data are regulated only minimally in the EU's legal order and not at all in the CoE's.

In essence, data processing by AI systems for national security purposes will come into the scope of personal data protection law, provided that the following conditions are fulfilled:

1. The relevant source of personal data-protection law is applicable to processing of data in national security situations.
2. Data being processed are “personal.”
3. Personal data are being “processed” in a manner that falls within the scope of relevant source of law.

3.4.1. Relevant sources of personal data-protection law and their applicability to national security situations

In the context of the Council of Europe's legal framework, the relevant source of personal data-protection law is the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108).⁴⁷ It is also the first comprehensive international legal instrument for personal data protection on the European continent, and for that reason alone, it deserves to be mentioned first. However, looking from

⁴⁷ Council of Europe, 1981.

the perspective of enforceability, there are important differences between that convention and the EU's General Data Protection Regulation (GDPR; see below), with the most relevant one being that the GDPR is a regulation and is therefore directly applicable in all EU member states. On the other hand, Convention 108 is an international treaty that needs to be transposed into national legislation to become effective. In terms of substance, legal solutions from Convention 108 are in most part in harmony with the GDPR. Therefore, while Convention 108 is extremely important in relations with third countries, its relevance for the EU member states is partially reduced, as the GDPR will be the one applied in practice. On the other hand, for non-EU member states, Convention 108 remains particularly important as currently the only functioning data-protection mechanism with global aspirations. Considering that both the CoE AI Convention and Convention 108 are open for accession to countries that are not parties of the Council of Europe, the later convention can also serve as an important data-protection standard in the context of the use of AI.

When it comes to its scope of application, Convention 108 does not contain an exception for national security purposes, but its state parties have the right to limit the application of certain provisions when such limitation is necessary for, *inter alia*, national security purposes. Such limitations can impact the application of data-protection principles, notification obligations, transparency obligations, data subjects' rights, some provisions on transborder flows of data, and powers of supervisory authorities.⁴⁸ However, even where such exceptions are made, Convention 108 explicitly requires that personal data-processing activities undertaken for national security purposes must be subject to independent and effective review and supervision, as prescribed by the domestic law of every party.⁴⁹

On the side of the EU law, there are several sources of EU law applicable to the processing of personal data. However, for the purpose of this study, it is not necessary to provide a comprehensive analysis of the whole EU *acquis* in this sector. Rather, we consider it necessary to focus on the following sources:

⁴⁸ Council of Europe, 1981, Article 11.

⁴⁹ *Ibid.*

- The *GDPR*,⁵⁰ which is generally applicable to all personal data-processing situations, as well as several sources of sectoral legislation, including the
- *Directive on Privacy and Electronic Communications* (e-Privacy Directive)⁵¹ and
- *Law Enforcement Directive* (LED).⁵²

As mentioned above, the first key question here is whether the abovementioned sources are applicable to processing of data in the context of national security. It appears on first sight that this is not the case. Namely, the GDPR prescribes in Article 2(2)(a) that it does not apply ‘in the course of an activity which falls outside the scope of Union law’, which is of course related to Article 4(2) of the Treaty on EU, and which, to remove any doubt and pursuant to Recital 16, includes ‘activities concerning national security’. However, this relatively clear provision is complicated by the fact that Article 23 of the GDPR allows member states to restrict by way of a legislative measure the scope of the personal data-protection principles, obligations of data controllers, and rights of data subjects under certain conditions and for the purposes of, *inter alia*, national security.⁵³ As shall be seen from the explanations below, the relationship between these provisions gives some ground to arguments that activities pertaining to national security are not *fully* excluded from the scope of the GDPR, as then there would be no need to create additional room for the exceptions in Article 23.

⁵⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

⁵¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37–47.

⁵² Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89–131.

⁵³ Pursuant to Article 23 of the GDPR, every such restriction must (1) respect the essence of the fundamental rights and freedoms and (2) be a necessary and proportionate measure in a democratic society to safeguard one of the legitimate aims listed therein.

Essentially, the same structure is found in the context of the LED, with its Article 2(3)(a) excluding processing of personal data ‘in the course of an activity which falls outside the scope of Union law’⁵⁴; at the same time, some specific national security exceptions are provided in Articles 13, 15, and 16. The same goes for the e-Privacy Directive, which contains a general national security exception in Article 1(3). But there is an additional exception in Article 15 that allows member states to restrict some rights protected under the directive when pursuing, *inter alia*, national security objectives. Article 15 therefore brings into question Article 1(3), because if national security situations would be fully excluded on the basis of that Article, why would Article 15 be necessary? In such circumstances, the CJEU had to interpret the scope of the national security exception, which was done in a relatively narrow manner. Namely, the position of the CJEU has been that

Although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.⁵⁵

In other words, the mere fact that a decision concerns state security cannot result in EU law being inapplicable.⁵⁶ On these grounds, the CJEU

⁵⁴ However, the interesting thing with this exception is that a slightly different explanation is provided in that directive’s Recital 14, which stipulates that

Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security... [and] activities of agencies or units dealing with national security issues ... should not be considered to be activities falling within the scope of this Directive.

Namely, it could be inferred from this recital that the intention of the drafters was broader, namely, to exclude from the scope all activities of agencies or units dealing with national security. Still, it appears that this distinction did not result in any different interpretations regarding the scope of the e-Privacy Directive, compared to other sources of personal data-protection law.

⁵⁵ Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others v. Premier ministre and Others*, 06 October 2020, para 99, and the cases cited there. See also Klamert, Kellerbauer, and Tomkin, 2019, p. 45.

⁵⁶ C-300/11, *ZZ v. Secretary of State for the Home Department*, 04 June 2013, para 38.

concluded in cases such as *Tele 2 and Watson*,⁵⁷ *La Quadrature du Net* (quoted above), and others that the processing of personal data for, *inter alia*, purposes of national security falls within the scope of the e-Privacy Directive.

This leads us to question how it is possible to differentiate between cases of processing of personal data for national security purposes, which would be covered by general exceptions such as those in Article 2(2)(a) of the GDPR and Article 1(3) of the e-Privacy Directive, and those which, while somehow related to national security, are still within the scope of personal data-protection rules. One important criterion developed in the case law of the CJEU regarding surveillance of electronic communications is whether personal data needed for national security purposes are being processed with or without the involvement of private parties. Namely, we see from the cases cited above that when private parties (e.g. service providers) are required to undertake certain activities in the context of national security activities, the e-Privacy Directive remains applicable. On the other hand, situations in which member states directly implement measures that derogate from personal data-protection rules, without imposing processing obligations on private parties, should according to the CJEU remain outside the scope of EU personal data-protection rules.⁵⁸ In *La Quadrature du Net and others*, the CJEU (even though it was not directly relevant for the case) made it explicit that the same criteria would be applicable in the context of the GDPR, arguing in the context of exceptions that the GDPR should not ‘apply to processing operations carried out “by competent authorities”...’, but ‘that the processing of personal data carried out by individuals for those same purposes falls within the scope of that regulation’.⁵⁹

Coming back to the processing activities relevant from the perspective of national security, the abovementioned standards could be relevant in the context of activities of security agencies. Provided that the CJEU maintains its approach of differentiating between activities undertaken by national authorities themselves and those imposing obligations on other parties, it

⁵⁷ Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, 21 December 2016, paras. 65–81.

⁵⁸ Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others v. Premier ministre and Others*, 06 October 2020, para. 103.

⁵⁹ *Ibid.*, para. 102.

would follow that at least in cases where security authorities are “tapping into” data sources held or operated by private entities, the EU personal data-protection rules would apply. On the other hand, those rules would not apply in cases where authorities collect and process data fully by themselves. The challenge, from the national security perspective, is that in many cases, data held or collected at the point of private entities will be relevant for national security authorities. For instance, collection of information from electronic communications networks, from systems of essential or important entities that are subject to private law in the context of cybersecurity, or even from open sources such as the internet would come within the scope of EU personal data-protection rules. The situation might be more complicated with data held by other public authorities, such as those contained in public registries, but if the exception is interpreted narrowly, it would not come as a surprise that tapping into these sources is subject to personal data-protection law.

3.4.2. Notion of personal data and processing of personal data

Having concluded that activities in the domain of national security can, in many cases, be subject to EU data-protection rules, the crucial next element for the applicability of those rules is the notion of personal data. Pursuant to Article 4(a) of the GDPR,⁶⁰ personal data are defined as

Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The definition in Convention 108 is compatible with this one; therefore, we can say that the concept of personal data in the convention corresponds to the one in the GDPR and other sources of EU law.

By simplifying this considerably, it can be said that personal data encompass (1) any information that is (2) related to (3) an identified or

⁶⁰ A substantially identical definition is found in Art. 3(1) of the Law Enforcement Directive.

identifiable (4) natural person.⁶¹ All of these elements have been extensively analysed in academic works and case law, so there is no need to repeat here what is already elaborated elsewhere. It is sufficient to say that any information that does not have to be private or sensitive in any standard meaning of those words will be considered “personal” if it “relates” to a natural person. As the CJEU explained in the *Nowak* case, the condition of “relates to” is satisfied where the ‘information, by reason of its content, purpose or effect, is linked to a particular person’.⁶² It appears that in providing this explanation, the CJEU also considered the earlier opinion of WP29, pursuant to which information is personal data if (1) it is ‘about a person’ or (2) if it is processed with a purpose to ‘evaluate, treat in a certain way or influence the status or behaviour of an individual’ or (3) if its processing ‘is likely to have an impact on a certain person’s rights and interests’; this impact does not have to be major, as it is sufficient that the individual may be treated differently from other persons as a result of the processing of data.⁶³ Putting these criteria in the context of national security operations, it seems reasonable to conclude that they will frequently be satisfied, as such operations are very likely to seek to evaluate individuals in some way or have an impact on a person’s rights or interests. In such circumstances, it is reasonable to anticipate that the EU law on personal data protection might apply generally.

Once it is concluded that an information is personal data, the relevant law will apply further under the condition that such data are processed. The notion of “processing” is even broader than the one of “personal data,” so that it includes ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means’ (GDPR).⁶⁴ The definition of processing in Convention 108 is substantially the same.⁶⁵ In theory, there is one small exception regarding the type of processing, namely when it is done on unstructured data and by non-automatic means.⁶⁶ However, since we are talking about the processing by means of AI, such an exception is fully inapplicable in this context.

⁶¹ Article 29 Working Party, 2007.

⁶² C-434/16, *Peter Nowak v Data Protection Commissioner*, 20 December 2017, para. 35.

⁶³ Article 29 Working Party, 2007, pp. 10–11.

⁶⁴ GDPR, Art. 4(2).

⁶⁵ Council of Europe, 1981, Art. 2(b).

⁶⁶ GDPR, Art. 2(1).

3.4.3. How might the personal data-protection law impact the use of AI systems in the national security domain?

Provided that the conditions elaborated above are satisfied, the EU personal data-protection rules might become applicable to data processing in the context of national security. What consequences that might bring will of course depend on the particular elements of each specific case. However, in general, the following seems especially relevant.

First, all personal data processing must have a legal basis under Article 6(1) of the GDPR. In the context of national security activities, that legal basis should come in the form of legislation specifically authorising certain forms of data processing. Likewise, any restrictions that can be imposed for national security purposes, based on Article 23, would also have to be established by a legislative measure and, at the same time, satisfy the principle of proportionality.

Second, data-protection principles such as data minimisation, storage limitation, and purpose limitation (see Article 5 of the GDPR) would also apply to processing in the context of national security. This is provided that their application is not excluded based on national legislation in line with Article 23 and is subject to the standards and requirements mentioned above.

Third, data subjects' rights, unless derogated by national law, would become enforceable. For instance, individual citizens could try to enforce their right to access their personal data (Article 15 of the GDPR) or exercise their rights in relation to automated individual decision-making, including profiling (Article 22).

Fourth, data-processing operations done for the purpose of national security would come under the supervision of national data-protection authorities, in addition to any other oversight mechanism that might exist under national law.

The situation on the side of CoE law is slightly more complicated when it comes to human rights protection for personal data.

The important caveat here is that while Convention 108 corresponds to the GDPR, the ECHR does not correspond fully to these sources of data-protection law. Namely, the right to personal data protection is not an autonomous right under the ECHR. In the context of the ECHR, personal data processing can, under certain conditions, be protected under Article 8, which deals with the more general right to privacy (or precisely, to the

protection of personal and family life, home, and correspondence). On the other hand, the Charter of Fundamental Rights of the EU provides in its Article 8 for a standalone right to personal data protection, together with some explicit requirements regarding the scope of protection.⁶⁷

Moreover, the ECtHR does not have the power to supervise the application of Convention 108 directly, while the CJEU has the power to interpret the GDPR and sectoral EU data-protection legislation. The ECtHR therefore applies only the ECHR and, where appropriate, interprets it in light of Convention 108.

Therefore, the ECtHR will afford protection in cases concerning personal data when it finds that there is a case under Article 8 that goes beyond simply verifying whether data are “personal” in the sense of Article 2(a) of Convention 108. While the ECtHR has in many cases extended the protection provided under Article 8 of the ECHR to personal data-processing situations, such an outcome is not inevitable. In other words, the mere fact that personal data are being processed does not mean, per se, that Article 8 of the ECHR has been interfered with.

In its case law, the ECtHR found in many cases that certain categories of data or the manner of their processing merit protection under Article 8.

For instance, in *Rotaru v Romania*, the ECtHR reasoned that information about persons’ life merits protection under Article 8 ‘when systematically collected and stored in a file held by agents of the State’.⁶⁸ On the contrary, in *Mehmedovic v. Switzerland*,⁶⁹ the ECtHR did not consider that Article 8 has been interfered with, even though personal data have been processed, because the sparse information concerning the applicant, gathered coincidentally and without relevance to the investigation, in no way constituted systematic or permanent gathering of data.⁷⁰

⁶⁷ Art. 8 of the Charter of Fundamental Rights of the EU reads as follows:

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

⁶⁸ *Case of Rotaru v. Romania* App. No. 28341/95, 04 May 2000, para. 44.

⁶⁹ *Case of Mehmedovic v. Switzerland*, App. No. 17331/11, 17 January 2019.

⁷⁰ *Ibid.*, para 18.

In numerous cases, the ECtHR found that a specific category of data merits protection, such as data about gender identification, sexual orientation and sexual life (*Drelon v. France*),⁷¹ processing of global positioning system data (*Uzun v. Germany*),⁷² and use of geolocation devices installed on a car and obtaining of geolocation data from telecommunication services providers (*Ben Faiza c. France*).⁷³ There is abundance of ECtHR case law in which various methods of obtaining data through surveillance measures gave rise to Article 8 considerations.⁷⁴ In the very important case of *Glukhin v. Russia* (2023), the ECtHR found that processing of biometric personal data using facial-recognition technology interferes with Article 8.⁷⁵ Likewise, in *Shimovolos v. Russia*, the ECtHR found that collecting information about a person's movements by train or air through the so-called Surveillance Database also interferes with Article 8 of the ECHR.⁷⁶ In *Catt v the United Kingdom*,⁷⁷ the court reached the same conclusion regarding the collection and retention of the applicant's personal data in the co-called Extremism Database.

Admittedly, the number of cases in which the ECtHR explicitly declined to afford Article 8 protection to personal data-processing situations is rather small. However, it does follow from the court's case law that something additional is needed, in addition to personal data being processed, to trigger the application of Article 8. Therefore, as the ECtHR explained in *S. and Marper v the UK*, 'the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8'. However, it is important to note here that it is processing of 'data relating to the private life' and not 'personal data' that trigger the application of Article 8, and these concepts are not synonymous. Therefore, the court went on to explain that

in determining whether the personal information retained by the authorities involves any of the private-life aspects ..., the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature

⁷¹ *Case of Drelon v. France*, App. Nos. 3153/16 and 27758/18, 08 December 2022.

⁷² *Case of Uzun v. Germany* App. No. 35623/05, 2 September 2010.

⁷³ *Case of Ben Faiza v. France* App. No. 31446/12, 08 February 2018.

⁷⁴ See ECHR, 2024.

⁷⁵ *Case of Glukhin v. Russia* App. No. 11519/20, 04 October 2023.

⁷⁶ *Case of Shimovolos v. Russia* App. No. 30194/09, 21 June 2011, paras. 64–66.

⁷⁷ *Case of Catt v the United Kingdom* App. No. 43514/15, 24 April 2019.

of the records, the way in which these records are used and processed and the results that may be obtained.⁷⁸

However, with all these reservations, we consider it highly unlikely that the processing of personal data using AI for national security purposes would be characterised by the ECtHR as something that does not interfere with the right protected under Article 8 or 10 of the ECHR.

4. Conclusions

While the possible uses of AI in the national security domain seem almost unlimited, possibly the greatest impact is expected regarding the data processing for intelligence analysis and analytics. Considering how those activities might be subject to legal limitations, the following picture emerges.

To begin, impacts of the AI Act and CoE AI Convention are likely to be very limited when AI is used for national security purposes, since both documents seek to exclude their application to national security matters in a very broad manner. The most important factor here is that both the convention and regulation seek to extend the exception to not only public authorities but also private entities undertaking certain activities in the national security domain. In such circumstances, we see two major legal frameworks that might prove influential.

First, it is to be anticipated that the ECHR will play a major role in ensuring that the uses of AI for national security purposes remain in line with the requirements of democratic society. As elaborated in section 2, an overview of the existing ECtHR case law indicates that the court does not have difficulty in applying the convention's rules for emerging technologies. Moreover, there is abundance of relevant legal standards from the existing case law, most importantly in cases dealing with surveillance and personal data processing, which might be influential if applied by analogy to the use of AI systems.

Second, in the context of EU law, the most important conditions and safeguards related to the use of AI for national security purposes might come through the application of personal data-protection rules. Our research indicates that while there is lot of uncertainty when it comes to the

⁷⁸ *Case of S. and Marper v. United Kingdom* App. Nos. 30562/04 and 30566/04, 04 December 2008, para. 67.

application of personal-data rules to national security situations, existing case law indicates that the application of those rules is not fully excluded. On the contrary, it is to be expected that personal data-protection law might prove to be very effective, at least when private entities are involved in data-processing operations.

Bibliography

- [1] Benzie, A., Montasari, R. (2022) ‘Artificial Intelligence and the Spread of Mis- and Disinformation’, in Montasari, R. (ed) *Artificial Intelligence and National Security*. Springer, Cham, pp. pp. 1-18; https://doi.org/10.1007/978-3-031-06709-9_1.
- [2] Dieu, O., Montasari, R. (2022) ‘How States’ Recourse to Artificial Intelligence for National Security Purposes Threatens Our Most Fundamental Rights’, in Montasari, R. (ed) *Artificial Intelligence and National Security*. Springer, Cham, pp. 19-45; https://doi.org/10.1007/978-3-031-06709-9_2.
- [3] Ferdin, J. J., F., Regin, R., Chinnusamy, K., Suman Rajest, S., Paramasivan, P. (eds.) (2024) *Explainable AI Applications for Human Behavior Analysis*. Hershey, PA: IGI Global Scientific Publishing, <https://doi.org/10.4018/979-8-3693-1355-8>.
- [4] Jurić, M. (2024) ‘Legal Aspects of Military and Defence Applications of Artificial Intelligence Within the European Union’, in Zombory, K., Szilágyi, J. E. (eds) *Shielding Europe with the Common Security and Defence Policy: The EU Legal Framework for the Development of an Innovative European Defence Industry in Times of a Changing Global Security Environment*, Miskolc-Budapest: Central European Academic Publishing, pp. 395-436.
- [5] Jensen, B., Whyte, C., Cuomo, S. (2019) Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence, *International Studies Review*, 22(3), pp. 526–550.
- [6] Klamert, M., Kellerbauer, M., Tomkin, J. (2019) *Commentary on the EU: Treaties and the Charter of Fundamental Rights*. 2nd Ed, Oxford: Packmm.
- [7] Montasari, R. (ed) (2022) *Artificial Intelligence and national security*. Springer, Cham; <https://doi.org/10.1007/978-3-031-06709-9>.

-
- [8] Palmiotto, F. (2025) The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation. *European Journal of Risk Regulation*, 1–24; <https://doi.org/10.1017/err.2024.97>.
- [9] Szappanyos, M. (2023) ‘Artificial Intelligence: Is the European Court of Human Rights Prepared?’, *Acta Humana – Emberi Jogi Közlemények*, 11(1), pp. 93–110; <https://doi.org/10.32566/ah.2023.1.6>.
- [10] Article 29 Working Party (2007) *Opinion 4/2007 on the concept of personal data*, [Online]. Available at: <https://ec.europa.eu/justice/article-29/documentation> (Accessed: 10 September 2024).
- [11] Babuta, A., Oswald, M. Janjeva, A. (2020) *Artificial Intelligence and UK National Security: Policy Considerations*. *RUSI*, [Online]. Available at: <https://static.rusi.org/ai-national-security-final-web-version.pdf> (Accessed: 10 September 2024).
- [12] Council of Bars & Law Societies of Europe (CCBE) (2019) *Recommendations on the protection of fundamental rights in the context of ‘national security’*, [Online] Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_2019_0329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf (Accessed: 10 September 2024).
- [13] Council of Europe (1950) *Convention for the Protection of Human Rights and Fundamental Freedoms*, [Online]. Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG (Accessed: 10 September 2024).
- [14] Council of Europe (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, [Online]. Available at: <https://rm.coe.int/1680078b37> (Accessed: 10 September 2024).

-
- [15] Council of Europe Commissioner for Human Rights (2015) *Democratic and effective oversight of national security services*, [Online]. Available at: <https://rm.coe.int/1680487770> (Accessed: 10 September 2024).
- [16] Council of Europe (2024) *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, [Online]. Available at: <https://rm.coe.int/1680afae3c> (Accessed: 5 March 2025).
- [17] ECHR (2024) *Personal data protection* [Online]. Available at: https://prd-echr.coe.int/documents/d/echr/FS_Data_ENG (Accessed: 5 March 2025).
- [18] European Court of Human Rights (ECtHR) (2013) *National security and European case-law*, [Online]. Available at: <https://rm.coe.int/168067d214> (Accessed: 10 September 2024)
- [19] Taddeo, M., Ziosi, M., Tsamados, A., Gilli, L., Kurapati, S. (2022) *Artificial Intelligence for National Security: The Predictability Problem*, [Online]. Available at: https://cetas.turing.ac.uk/sites/default/files/2022-09/research_report_ai_predictability_problem_vfinal_3.pdf (Accessed: 10 September 2024).
- [20] Venice Commission (2015) *Report on the Democratic Oversight of Security Services*, [Online]. Available at: [https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2015\)010-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e) (Accessed: 10 September 2024).

BARBARA KACZMARCZYK*

Cybersecurity from a systemic perspective**

ABSTRACT: Cyberspace has become a place of aggressive attacks aimed at various areas of human life. Statistics indicate a dynamic increase in cyberattacks in European Union (EU) member states and NATO countries, where technologies are developing at a rapid pace; on the one hand, this contributes to economic growth and, on the other hand, to the creation of increasingly complex cyberattack algorithms. They are aggressive and can cause significant losses.

The following research methods were used to develop the article: analysis and synthesis of literature on the subject in the field of security, the state security system, cybersecurity, statistical data and legal acts. interviews were also conducted with experts in the field of security and cybersecurity systems.

A systemic approach can be considered in the context of two subsystems: management and executive. The management subsystem includes the decision-making bodies of NATO and EU structures that develop a cybersecurity policy for all members of their structures, while the executive subsystem includes the armed forces and other security entities of individual EU and NATO members, as well as society on an individual (citizens) and collective (private institutions, enterprises) basis.

Due to the nature of cyber threats, cyber security should be considered systemically, i.e. in a way that covers all its aspects; we should also improve cybersecurity strategies to counter threats, secure infrastructure and the green energy sector, develop technological and production resources, and enable the creation of cyber defense that is applicable both in one country and around the world.

* PhD., Associate professor in the field of social sciences in the discipline of security science in the field of social sciences in the discipline of security science, General Tadeusz Kościuszko Military University of Land Forces, Poland, ORCID: 0000-0002-6995-2961, barbara.kaczmarczykws@gmail.com.

** The research and preparation of this study was supported by the Central European Academy.

KEYWORDS: cyberspace, threats in cyberspace, cybersecurity, information, military sector, civilian sector, system.

1. Introduction

Threats in cyberspace are unpredictable and have no borders, which means that their scope is global, and they can cause significant losses in all important areas of human life. These factors affect the security of both countries and the world. Cyber incidents have become particularly important in the face of a dynamically developing world in which new-generation technologies create new opportunities for action. Therefore, the approach to this issue must have a holistic dimension: exploration of phenomena and event processes. The first and most important assumption is that everyone is responsible for security, including cybersecurity. This encompasses public institutions and bodies, non-governmental organisations, private sector institutions, and citizens. The effectiveness of actions is determined by many factors, one of them being the strategies that set the course of action to face threats and help secure the future of cyberspace. To ensure security on the Internet, countries develop cybersecurity strategies and legal provisions and cooperate with other countries.

The aim of these activities is not only the security of ordinary citizens, groups, nations, or nations but also the possibility of functioning in countries that have the ability to counter threats, develop the green energy sector, and develop economic and technological sectors. Internal and external cooperation remains an important element, as does everyone's awareness of the defence against cyberthreats. An action strategy should adopt systemic solutions that are similar across all countries. The National Cybersecurity Strategy, published by the Biden–Harris administration, announced on 2 March 2023, includes many aspects that can be included as elements of this system.¹ It focuses on building cooperation based on the defence and protection of critical infrastructure, effective use of technology, involvement of private entities, investments in resilience, and international

¹ USA – National Cybersecurity Strategy, 2024, [Online]. Available at: <https://cyberpolicy.nask.pl/usa-krajowa-strategia-cyberbezpieczenstwa/> (Accessed: 30 January 2024).

cooperation.² This approach is multifaceted and needs to be accurately defined.

In the opinion of the author and surveyed experts in the field of cybersecurity, this issue should be considered systematically. The systemic approach to security considerations, including cybersecurity, is supported by its features such as (a) holism (perceiving phenomena and processes as a whole), (b) comprehensiveness (revealing various connections and internal relations), (c) essentialism (studying phenomena or objects from the viewpoint of important characteristic features), (d) structuralism (identifying the properties of an object or area of interest based on those features of its structure that are considered unchanging and integrating), (e) contextuality (considering systems according to their place in a larger whole), (f) teleologism (considering phenomena from the viewpoint of their purposefulness in a given field, especially in reality), (g) functionality (considering systems in terms of the goals achieved and fulfilling functions), (h) effectiveness (considering systems from the perspective of the size of the results achieved and goals and functions performed), (i) synergism (consideration of properties resulting from cooperation and cooperation within the system of subsystems and elements of these subsystems, the essence of which is cooperation, which is more effective than the sum of their separate activities), and (j) development (consideration of systems in approach to transformations and changes related to the transition to states or forms that are more complex or, in some respects, more perfect).³ These system features are important when considered individually and collectively. They are so important that the issue of cybersecurity should be discussed considering all features related to the concept of the 'system'.

This study aims to comprehensively consider cybersecurity by considering the characteristics of the system. Therefore, in the context of the above, the research problem was defined as 'What assumptions should be made when defining the cybersecurity system and which of its elements (subsystems) play a key role in ensuring security'.

For this study, it was assumed that a cybersecurity system is a set of forces and resources understood as personal and material resources allocated by the state or states to carry out security tasks in cyberspace. This system

² Ibid.

³ Wiśniewski, 2013, pp. 115–116.

consists of a management subsystem and an executive subsystem,⁴ which includes the operational and support sectors. The operational sector includes the defence and protection departments, whereas the support sector includes the social and economic departments. Based on the above assumptions, a discussion of cybersecurity is undertaken from a systemic perspective.

2. Assumptions of the cybernetic security system – the management subsystem

European security systems are based on several interconnected components, as follows: (a) the North Atlantic Alliance (NATO),⁵ (b) the European Union (EU) with its Common Security and Defense Policy (CSDP),⁶ and (c) the Organization for Security and Co-operation in Europe (OSCE).⁷ NATO is treated as a political and military organisation capable of using its force to defend member states and strengthen the geopolitical bond between the United States and Europe by guaranteeing their presence on the European continent, which is strategic for European security in both political and military contexts. The role of the EU is to integrate its members and cooperate intensively and effectively with NATO. In turn, OSCE activities have focused mainly on the territory of the former USSR and have been limited because of Russia's policy. Therefore, it was considered that OSCE's participation in European security activities was marginalised.⁸

The management subsystem is a key element in the discussion of the cybersecurity system and is designed to direct its functioning. This includes the EU and NATO, which outline international cybersecurity policies within their structures. This subsystem is responsible for the implementation of groups of tasks such as (a) monitoring incidents and attacks in the network (the scale of their occurrence, trends, their nature, type, and place of

⁴ White Book of National Security of the Republic of Poland, 2024, [Online]. Available at: chat.openai.com, p.36; (Accessed: 30 March 2024).

⁵ NATO Communications and Information Agency, [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed: 23 April 2024).

⁶ The Common Security and Defence Policy, [Online]. Available at: https://www.eeas.europa.eu/eeas/common-security-and-defence-policy_en (Accessed: 23 April 2024).

⁷ Organization for Security and Co-operation in Europe, [Online]. Available at: <https://www.osce.org> (Accessed: 23 April 2024).

⁸ White Book of National Security of the Republic of Poland, 2024, [Online]. Available at: chat.openai.com, pp.123-127. (Accessed: 30 March 2024).

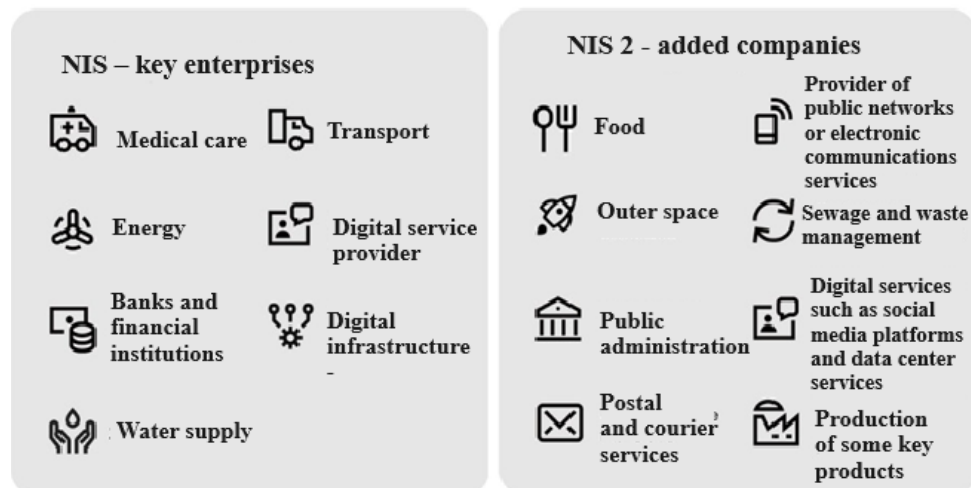
occurrence), (b) preventing the occurrence of incidents and attacks in the network of (EU and NATO countries), (c) improving cooperation between EU and NATO countries (exchange of information, implementation of best practices), and (d) strengthening the cyber resilience of EU and NATO countries.

The implementation of the aforementioned tasks is possible owing to appropriate legal, financial, planning, organisational, and technical conditions. Therefore, the first step that the EU took was to introduce the Directive on the Security of Network and Information Systems (NIS) in 2016, which concerned issues related to network infrastructure and IT systems. This document was the basis for the operation of many important enterprises such as medical care, transport, energy, digital service providers, banks and financial institutions, digital infrastructure, and water supply.⁹

The sharp increase in cyberattacks and incidents in Europe, as well as the identification of their negative impact on various areas of society, led to the introduction of Directive 2022/2555 of the European Parliament and Council on 14 December 2022 on measures for a high level of cybersecurity in the territory of the Union. This directive was repealed by the 2016 NIS Directive (NIS 1). The NIS 2 directive expanded the groups of enterprises to include food, public administration, space, providers of public networks or electronic communication services, postal and courier services, sewage and waste management, digital services such as social networking platforms and data centre services, and the production of key products (Figure 1).

⁹ What is NIS2 and what does it mean for your organization? [Online]. Available at: https://www.nomios.pl/materialy/czym-jest-nis2/?utm_term=dyrektywa%20nis&utm_campaign=PL-PL+%7C+NIS2&utm_source=adwords&utm_medium=ppc&hsa_acc=5882528235&hsa_campaign=21097975083&hsa_grp=163624375167&hsa_ad=693854520644&hsa_src=g&hsa_tgt=kwd-382086989990&hsa_kw=dyrektywa%20nis&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=Cj0KCQjwltKxBhDMARIsAG8KnqWdbSCmaCIWA9izjqe3UWZFYb5voEqHfqtYlPbsQHovG9JxBRBEOscaAixGEALw_wcB. (Accessed: 30 March 2024).

Figure 1 Comparison of key enterprises according to the NIS and NIS 2 Directives



Source: Based on: What is NIS2 and what does it mean for your organisation? [Online]. Available at <https://Czym jest NIS2 i co oznacza dla Twojej organizacji? Nomios Polska> (Accessed: 30 August 2024).

For example, Poland has 8,000 entities in 18 economic sectors. The requirements of the NIS 2 directive also assume the development of more stringent procedures for reporting cyberattacks and incidents as well as increasing cooperation between EU countries in relation to responding to cyber incidents, exchanging information about them, and implementing the best and most effective practices. EU countries were obliged to implement it by 17 October 2024. In summary, the purpose of the new regulations was to create and implement a uniform standard for the security of network and information systems in all EU countries and to strengthen the Union's cyber resilience, taking into account Russia's acts of aggression against Ukraine and its use of elements of cyber warfare.¹⁰

¹⁰ NASK Cyber Policy, [Online]. Available at: <https://cyberpolicy.nask.pl/aktualnosci/publikacja-dyrektywy-nis-2/> (Accessed: 30 April 2024).

2.1. Nato's role in cyberspace

NATO has imposed certain solutions and regulations to ensure international security in cyberspace. Therefore, it is qualified using a steering subsystem. To implement the above-mentioned tasks, on 1 July 2012, the NATO¹¹ Cybersecurity Center (NCSC) was established based on the many years of experience of its predecessors (civilians and soldiers). It is located at the Headquarters of the NATO Allied Command in Europe (SHAPE) in Mons,¹² Belgium. The aim was to assist effectively in the coordination and cooperation in the management of cybersecurity information between NATO member states and their partners. It is an extensive platform aimed at (a) analysing and monitoring network incidents and attacks, (b) technical and expert support aimed at increasing cyber defence capabilities, (c) supporting member states in improving competencies, (d) developing the best regulation rights enabling the implementation of security policy in cyberspace, and (e) strengthening international cooperation (political consultation platform, joint actions).¹³

The NCSC employs approximately 3,000 civilian and military personnel who perform tasks at 34 locations in Europe and North America. It cooperates with sectors such as industry, scientific and academic communities, and non-profit organisations. These practices enable the maintenance of technological advantages.

NATO also established the Cyberspace Operations Centre in Mons, Belgium. This centre was established to support military commanders in allied operations and missions. It coordinates NATO's operational activities in cyberspace and indicates the cyber defence goals that must be implemented by the allied countries. These activities were conducted as part of the NATO defence-planning process. NATO also has the NATO Cyber Rapid Reaction Teams, which have 24/7 response capabilities; their main task is to help their allies. Additionally, NATO has its own international research and training centre, The NATO Cooperative Cyber Defense Center

¹¹ NATO Communications and Information Agency, [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed: 23 April 2024).

¹² Supreme Headquarters Allied Power Europe, [Online]. Available at: <https://shape.nato.int> (Accessed: 23 April 2024).

¹³ NATO Communications and Information Agency, [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed: 23 April 2024).

of Excellence (CCDCOE) in Tallinn,¹⁴ which aims to support member states and their partners in the field of cyber defence. NATO operations are governed by the provisions of Doctrine AJP-3.20, the Allied Joint Doctrine for Cyberspace Operations. This doctrine outlines key aspects of cyberspace operations, including their fundamental characteristics, as well as their planning and execution.¹⁵ NATO has training and education facilities in the field of cyber defence at centres such as (a) The NATO Communications and Information (NCI) Academy in Oeiras, Portugal (training and education in the field of cyber defence); (b) The NATO School in Oberammergau, Germany (training and education in the field of cyber defence); and (c) The NATO Defense College in Rome, Italy (enabling the acquisition of skills in strategic thinking related to political and military issues, including cyber defence).

In summary, the management subsystem is strategic. The entities included in it are responsible for international security policies in cyberspace and, consequently, for cybersecurity, both in individual countries and in EU and NATO countries.

3. Assumptions of the cybernetic security system – the execution subsystem

The executive subsystem is crucial for every contractor, that is, the country. It consists of an operational sector (defence and protection) and a support sector (social and economic). The operational sector is crucial from the viewpoint of conducting activities aimed at preventing or responding to cyber-attacks or cyber incidents. The key role in the operational sector is played by the armed forces and, in the support sector, by society.

3.1. Armed conflicts and cyberspace

While analysing various armed conflicts, it should be emphasised that in addition to standard activities, propaganda, information, and media activities were also used. Therefore, the terms ‘media war’ and ‘propaganda war’

¹⁴ The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub, [Online]. Available at: <https://ccdcoe.org> (Accessed: 23 April 2024).

¹⁵ Allied Joint Publication-3.20, Allied Joint Doctrine for Cyberspace Operations, [Online]. Available at: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (Accessed: 30 August 2024).

were used to describe some conflicts. Such wars were as follows: (a) the Iran–Iraq War (1980–1988),¹⁶ (b) the Persian Gulf War (1990–1991),¹⁷ (c) the Iraq War (2003–2011),¹⁸ (d) the war against ISIS (2014–2017),¹⁹ and (e) the war with Russia (2018–2019). These wars were mainly based on propaganda, information, and media. The Vietnam War (1955–1975) was the first to have a significant presence in the media.²⁰

The participants in the conflict were politicians who provoked the war, soldiers taking part in it, and the media, in that order. The most important conclusion from this conflict in relation to the strategy of military operations was the statement that ‘in order to conduct foreign policy, it is necessary to control the information that the media transmit to the public’,²¹ which is why, from a political and military viewpoint, it is so important to control the information transmitted to the public. The media had access to it during the Vietnam War. This situation changed after the government, politicians, and commanders realised the media’s influence on armed conflicts. In several subsequent conflicts, they were not allowed to report events.

Currently, the media are treated as partners under certain rules. Journalists focus on providing information about the winning side of the conflict, and in many cases, any information intended to reach the public is censored by the government and military sectors. These assumptions have brought great success to the American government. The media effectively influenced Americans’ opinions, which were shaped by controlled media coverage. In summary, the role of the media is to create appropriately directed images to influence public opinion.

The Iran–Iraq War was an armed conflict that lasted from 1980 to 1988. Over one million people died during this war, and material losses

¹⁶ Iran–Iraq War, [Online]. Available at: <https://www.history.com/topics/middle-east/iran-iraq-war> (Accessed: 10 April 2024).

¹⁷ Persian Gulf War, [Online]. Available at: <https://www.history.com/topics/middle-east/persian-gulf-war> (Accessed: 10 April 2024).

¹⁸ The Iraq War, [Online]. Available at: <https://www.georgewbushlibrary.gov/research/topic-guides/the-iraq-war> (Accessed: 10 April 2024).

¹⁹ The Conflict with ISIS: Operation INHERENT RESOLVE, June 2014–January 2020, [Online]. Available at: <https://history.army.mil/html/books/078/78-2/index.html> (Accessed: 10 April 2024).

²⁰ The Conflict in Iraq and the media (media manipulation, or how beneficial it is sell your strategy), [Online]. Available at: [mak00 \(uw.edu.pl\)](http://mak00.uw.edu.pl) (Accessed: 30 April 2024).

²¹ Ibid.

were estimated to be over USD 400 billion.²² This conflict is believed to have caused the greatest losses in the 20th century. The main strategy was military operations on the front, but propaganda activities were also used to influence public opinion both inside and outside the country. It was the first war in which both sides manipulated information to gain support from each other and weaken the opposing side. These activities focused on presenting images from the battlefield and reporting them, as well as broadcasting propaganda messages from leaders. These goals were achieved through radio, television, printed materials, the Internet, and emerging media. Both Iraq and Iran had control over radio and television stations and the content published in articles and images was distributed to the public. Both sides use posters and leaflets depicting war heroes, patriotic slogans, and national flags. This aimed to encourage society to fight and think about it in terms of necessity. Although the Internet and media were still scarcely used at that time, activities were also undertaken to promote specific information, including photos and films depicting the course of the war and specific situations intended to influence public opinion.

The Iran–Iraq War is an example of the possibility of having a strong impact on society through the use of disinformation or propaganda.

Another example of media warfare was the Persian Gulf War (1990–1991). All parties involved in the conflict conducted propaganda and information activities. This war was reported on an ongoing basis. Journalists tried to provide reliable and current information, but this was hindered by the authorities, who wanted to promote an appropriately created message. Journalists had access only to selected combat zones or certain events, and the military often decided what was to be published. Interest among journalists was very high: 3,000 people from all over the world volunteered to cover the war. However, only 600 journalists were given access to the clash sites, 500 of whom were Americans.²³ A rule was also adopted in which journalists were assigned to military units to limit their freedom of action. The interests of the independent journalists were not those of either side of the conflict. The government wanted to provide the public with information aimed at confirming their belief in the right to wage

²² Iran-Iraq War, [Online]. Available at: The Iran-Iraq War - (bing.com) (Accessed: 30 April 2024) and Video The Iran-Iraq War, [Online]. Available at: Iran-Iraq War - Summary, Timeline & Legacy (history.com) (Accessed: 20 April 2024).

²³ The Conflict in Iraq and the media (media manipulation, or how beneficial it is selling your strategy) [Online]. Available at: mak00 (uw.edu.pl) (Accessed: 30 April 2024).

armed conflict. Despite these restrictions, journalists tried, often risking their own lives, to reach the frontline. Manipulation and propaganda have become variants of action on both sides. Thanks to media activities, information about the war in the Persian Gulf spread widely and sparked a global discussion on the legitimacy of war, its ethics, foreign policy, and international security. Widely discussed war has stimulated public discussion worldwide.

Another example of a media war was the war in Iraq (2003–2011), which was initiated by the United States under the pretext that Iraq possessed weapons of mass destruction (chemical and biological weapons and ongoing nuclear weapons development) and connections with terrorist organisations. During the war, photos and films were manipulated in such a way that military actions were perceived positively and enemy actions were perceived negatively. Both sides of the conflict controlled media messages. Journalists were given limited access to the areas where the war was taking place, and the content appearing in the press was censored by state media. Saddam Hussein's administration organised and carried out information and propaganda campaigns aimed at creating a positive image of the regime and condemning military invasions. Both sides promoted their own narratives to create positive images of their actions, events, and interests. The manipulation was performed using appropriately selected words, phrases, or sentences.

Another example of the use of information and propaganda activities is the war against ISIS (2014–2017). The Islamic State (a terrorist group) has extensive and well-functioning propaganda cells. The main goal was conscious or unconscious beliefs about the ideas being promoted. ISIS conducts propaganda activities in cyberspace and is characterised by a high level of technology. These tactics are intended to gain the interest of recipients and recruit them to join the organisation. Messages in the form of photos and videos, based on various social media platforms, such as Facebook and Twitter, are created with utmost care and use the latest technologies. The Internet and social media have become cheap channels of access to society worldwide, facilitating the coordination of tasks within a group, enabling real-time reporting of actions taken, and conducting propaganda activities. The State of Islam conducts large-scale information activities, trying to intimidate society and recruit new supporters of the "soldiers" ready to arrive at their areas or carry out activities as 'lone wolves'. Online activities also include the use of cryptocurrencies for

terrorist activities, the flow of which is much more difficult to detect than in traditional financial funds. Because of this solution, financing the activities of criminal organisations has become easier. Social networking sites were also used for these activities. Fictitious profiles were created, and Israeli soldiers were contacted to gain access to information about the army's activities and the prevailing mood among soldiers and society.²⁴

An effective tool for propaganda and disinformation is fake news, which is partially or completely false information intended to mislead the recipient to achieve financial, political, ideological, and prestigious benefits. Research shows that false, often negative, information spreads much faster than true, often positive, information.²⁵ Learning how society functions makes it easier to organise activities that have an expected impact on the recipient.

Propaganda activities were also conducted by the Russian Federation (2018–2019) in all possible information areas using the media. They provided information, disinformation, propaganda, and psychological operations. To achieve these goals, an extensive information apparatus was used, which included leaders, commanders, journalists, and special services. Russia used all available means to create content in cyberspace. The created content included portraying the policies of the United States and NATO countries negatively, depreciating Poland's defence capabilities, and shaping the negative image of the European Union and Ukraine. Russia constantly conducts information warfare in cyberspace to pursue its own interests. Russia is a brutal player in the international arena and is famous for its disinformation campaigns using false accounts on social media. These activities are usually aimed at democratic countries and their alliances. Their strategic goal is to weaken countries and alliances that condemn Russia's actions, as well as to promote Russia as a great power. Russia has used various means to achieve these goals. One of them is engaging in cyber warfare. They have well-trained hacker groups that attack political, economic, military, and other economic goals. Their main goals are to steal sensitive data, spy on strategic areas, and sabotage IT and

²⁴ Information Warfare as a Contemporary Tool of Irregular Operations, [Online]. Available at: [Wojna_informacyjna_jako_współczesne.pdf](#) (Accessed: 30 April 2024).

²⁵ Study: On Twitter, false news travels faster than true stories Research project find humans, not bots, are primarily responsible for spread of misleading information, [Online]. Available at: <https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308> (Accessed: 30 April 2024).

information systems, critical infrastructure, and other facilities crucial to the state's defence. Russia is suspected of interfering with elections in various European Union countries as well as in the United States through the use of social media, the Internet, and websites. The main goal of these actions was to weaken the country's position while simultaneously strengthening Russia's influence.

In summary, cyberspace has become a completely new and modern platform for conflict. In the literature, it was swiftly recognized as an additional arena of warfare, alongside land, sea, and air. This domain is, on the one hand, very challenging, and on the other hand, a remarkably accessible platform for waging war. Information has become a commodity because it is easily accessible. Anyone with basic knowledge of how to use computer hardware or software can create events, cause panic and chaos in societies, and influence the opinions of users. It is difficult to detect fake accounts and information inserted into a network, and this requires the involvement of many people or even extensive structures dedicated to such tasks.

Conflict in cyberspace has become a reality. In 1991, after the Persian Gulf War, one of the conclusions was that information could be freely presented on the Internet; therefore, it was very important to control the messages being shared. This belief was further strengthened by research conducted among the American community in 1991, which revealed that as much as 89% of knowledge about the Persian Gulf War was obtained from television, and only a few citizens assessed the course of this war through the prism of experience.²⁶ This demonstrates the powerful tools of propaganda and disinformation, especially when used in cyberspace. Due to these tools, it is possible to create a societal perception of conflict in various countries and, thus, influence the policy of a given nation or the world.

3.2 Armed forces in cyberspace

Information protection is a basic task for every country's armed forces. In the activities of the armies of nations, it is important to maintain the confidentiality of military information, the effectiveness of its transmission, and its quality and credibility. This is made possible through information protection, during which the following actions are taken: counterintelligence, technical security of IT infrastructure, IT protection,

²⁶ The Conflict in Iraq and the media (media manipulation, or how beneficial it is selling your strategy), [Online]. Available at: mak00 (uw.edu.pl) (Accessed: 30 April 2024).

engineering development aimed at anticipating the enemy's actions, psychological protection, counter-disinformation, and reconnaissance (detering and incapacitating the enemy). Information protection involves securing information in such a way as to prevent undesirable disclosure, modification, or destruction. Defensive actions are being taken to protect the so-called sources of information or information environment shields. Information protection is thus strategically important for security systems, as any loss or disruption may weaken the information battlefield.

Defence potential focuses on the armed forces, which also carry out tasks related to security in cyberspace. Next to land, water, and air, cyberspace has become another area of warfare (for the armed forces) and is important from the perspective of the strategic, defence, and protective capabilities of the armed forces. In this space, cyberattacks are prevented, information is collected, and defence is implemented. It is also a place where the communication and coordination of operations, missions, and tasks are conducted. The main tasks of the armed forces in cyberspace are (a) protection of IT infrastructure (equipment and networks, as well as systems dedicated to specific tasks), sensitive data, and information contained therein; (b) data collection (e.g. monitoring the enemy's activities, its capabilities and intentions to act); (c) conducting intelligence activities (open and closed sources); (d) coordinating activities (possible at all levels of command); (e) counteracting cyberattacks and conducting offensive activities (implemented through a cyberattack on the enemy's infrastructure, information espionage, information warfare, propaganda, strategic communication, operational information, psychological operations, disinformation, sabotage of enemy systems, information manipulation); (f) communication (possible between team members, carried out using secure channels); (g) professional development (possibility of training soldiers and civilian staff in the field of cybersecurity, conducting exercises and simulations based on real scenarios); and (h) technological scientific development (conducting work on artificial intelligence, cryptology, cybersecurity technologies, big data).

Nowadays, thanks to modern technologies, the problem is not access to data, but access to too many differently formatted data. In this context, 'big data' are particularly noteworthy. Big data refers to four important Vs: (a) volume (processing large amounts of data); (b) velocity (data generated at high data transfer speeds); (c) variety (different types of data); and (d)

veracity.²⁷ Owing to big data analyses, it is possible to detect potential cyberattacks and cyber criminals, making real-time analysis, which is important for an effective and immediate response to incidents, preventing DDoS attacks, and protecting personal data and sensitive, official, and classified information.

Ensuring the safety of citizens and the nation requires the involvement of many forces and resources, as well as strategies and variants of action. Rapid technological development has become a fundamental factor in shaping the world and its functioning in all areas. This also applies to safety concerns. Achieving satisfactory security in a country depends on several factors. Therefore, various operational strategies and methods have often been combined. Multidirectional and diverse methods contribute to greater effectiveness than their individual uses. Anyone is responsible for safety, which is why the attitude of every person and citizen is important. This attitude depends on external factors such as the available information provided by various means of communication. On this basis, opinions and social attitudes are built and, consequently, actions are taken. Therefore, various, often very aggressive, actions shape public opinion not only in the country but also abroad. To achieve these assumptions, the following instruments can be used: propaganda, information warfare, disinformation, psychology, information, propaganda, and military disinformation operations.²⁸ These actions are intentional and allow the achievement of assumed political and military goals.

Psychological operations are carefully planned operations aimed at transmitting selected information to foreign recipients to induce specific emotions, motivations, and, ultimately, specific behaviours of foreign governments, institutions, or citizens. The assumption of the aforementioned operations is to obtain behaviour conducive to a nation's goals. This is part of not only diplomatic, informational, and economic activities but also military ones. They are used in times of crisis and armed conflict.

²⁷ Big Data Analytics, [Online]. Available at: https://www.cybertec-postgresql.com/pl/data-science/analitka-big-data/?gad_source=1&gclid=CjwKCAjwxLKxBhA7EiwAXO0R0AP4wteDaJk5guP13G2Q2b9aDMXLecz9C3UVW1Dj0y0w2GovF2HTyhoCaOcQAvD_BwE (Accessed: 15 February 2024).

²⁸ *Disinformation and Propaganda in the Context of Threats to State Security, Review of Constitutional Law*, [Online]. Available at: *Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa - Przegląd Prawa Konstytucyjnego - Issue 2(24) (2015) - CEJSH - Yadda (icm.edu.pl)* (Accessed: 11 February 2024).

Psychological operations are carried out at the strategic, operational, and tactical levels. They may negatively impact soldiers' morale, reduce the enemy's ability to conduct or sustain military operations and attract attention.²⁹

Information operations are the integrated implementation of projects aimed at influencing the attitudes of commanders and those in power, disrupting the functioning of IT systems and data carriers or destroying them, and corrupting decision makers while protecting one's own information and the systems processing it. Information operations are divided into offensive (OIO) and defensive (DIO) operations. OIA include intelligence-supported capabilities and activities. They influence the opponent's decisions and promote specific planned goals, that is, activities aimed at attacking information about the opponent and everything related to him. Defensive operations aim to protect information and IT systems.³⁰

Propaganda operations are defined as (a) planned and purposeful activities aimed at shaping specific views and behaviours of society based on directed images, slogans and symbols referring to human prejudices and emotions³¹; (b) planned and purposeful, skilful use of communicating a certain viewpoint, aimed at persuading the recipient to voluntarily recognise this point of view as their own, (c) activities aimed at 'intentional dissemination of information, opinions, views, theories explaining the surrounding reality and phenomena of social life'; (d) activities using the technique of influencing behaviour of citizens, managing and manipulating public opinion. These activities can be improved based on research results, among others, in the fields of social psychology, sociology, political science, and communication theory.

The assumption behind this type of activity is that government authorities lie to societies. A lie can be directed at an opponent, international

²⁹ Psychological Operation, [Online]. Available at: <https://www.globalsecurity.org/military/library/policy/usaf/afdd/2-5-3/afdd2-5-3.pdf>; (Accessed: 11 February 2024) and Department of Defense Dictionary of Military and Associated Terms, [Online]. Available at: https://irp.fas.org/doddir/dod/jp1_02.pdf (Accessed: 3 February 2024).

³⁰ Vademecum of Information Security. Information Operations, [Online]. Available at: <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/operacje-informacyjne/> (Accessed: 13 February 2024).

³¹ Vademecum of Information Security. Propaganda operations, [Online]. Available at: <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/operacje-propagandowe/> (Accessed: 12 February 2024).

opinion, or society. These activities focus on deliberate and planned intellectual and emotional manipulations carried out using false arguments, which should be considered disinformation. Propaganda aims to convince the recipient to accept content directed by the authorities in a country or countries or, based on it, to change awareness and beliefs about matters that are important in the country. Propaganda is also understood as persistent teaching. It is associated with terms such as lying, brainwashing, propagating slogans, speaking against someone or something, politicisation, and indoctrination. Propaganda uses many techniques to reach a recipient (e.g. image, sound, body language, written text, film, theatre, dance, radio, television, and social media). Broadly, propaganda refers to emotions rather than reason.³²

The literature provides various types of propaganda. When it comes to defining intentions and sources, the following are distinguished: (a) white propaganda (intentions and sources open), (b) grey propaganda (intentions and sources unclear and open), and (c) black propaganda (intentions, hostile, enemy-oriented sources).³³

There is also propaganda that is (a) political (influencing the opinion of society; used by governments, political parties, interest groups), (b) advertising (promoting products or services; used by entrepreneurs), (c) military (mobilising support for a specific side, demonising the enemy, increasing morale among soldiers and civilians; used by authorities, commanders), (d) religious (promoting faith, attracting followers; used by churches, religious organisations), (e) racial/ethnic (goal beliefs about the advantage of one group or race; used by governments, social groups), (f) health (goal belief in changing health behaviours; used by health services, government), (g) cultural (goal promoting cultural values; used by the government, specific organisations), (h) social media (goal spreading disinformation, manipulating public opinion, influencing elections; used by the government, specific social groups),³⁴ (i) state (goal promoting patriotism, justifying government policy; used by government, specific groups), and (j) corporate (goal promoting corporate interests; used by companies).

³² Dobek-Ostrowska, Fras and Ociepka, 1999.

³³ Vademecum of Information Security. Propaganda operations, [Online]. Available at: <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/operacje-propagandowe/> (Accessed: 15 February 2024).

³⁴ Batorowska, Klepka, and Wasiuta, 2019.

Military disinformation operations are defined as pre-planned activities that are part of military operation plans. Their goal is to mislead the opposing side regarding their own activities, namely, the number of forces at their disposal, their location, and combat readiness. This is intended to influence the opponent's decisions. The effects of this type of operation are as follows: chaos caused by the information received and favourable behaviour of the opponent in relation to his own side (inappropriate allocation of forces and resources to the task being carried out, unmasking the strengths and weaknesses of the opponent, revealing the intentions and intentions of action, and loss of combat capabilities).³⁵ Military disinformation operations are extremely difficult; therefore, they require a special focus on issues such as the purpose of the action (causing the enemy to take specific actions), security, timeliness (determining the most favourable time to carry out the operation), planning and control (implemented by the central command), and integration (coordination of activities with the operations that support them).³⁶

3.3. Organisation of cybersecurity in the Republic of Poland

The NIS Directive imposed the same solutions on all European Union countries in the field of information protection as part of cyberspace security. In relation to its provisions, the following have been established in Poland: (a) the National Computer Security Incident Response Team run by the Ministry of National Defense, operating as part of the Cyberspace Defense Component Command (CSIRT) of the Ministry of National Defense;³⁷ (b) the Computer Security Incident Response Team, national level, led by the Head of the Internal Security Agency (SIRT GOV);³⁸ and (c) the Computer Security Incident Response Team, national level, led by the Scientific and Academic Computer Network (CSIRT NASK).³⁹ Their

³⁵ Kacala, 2015.

³⁶ Vademecum of Information Security. Military Disinformation Operations, [Online]. Available at: <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/11/operacje-wojskowej-dezinformacji/> (Accessed: 10 February 2024).

³⁷ Cyberspace Defense Forces, [Online]. Accessed at: <https://www.wojsko-polskie.pl/woc/> (Accessed: 20 February 2024).

³⁸ Computer Security Incident Response Team, [Online]. Available at: <https://csirt.gov.pl> (Accessed: 10 February 2024).

³⁹ Day-To-Day Activities of the Computer Security Incident Response Team Under the Act on the National Cybersecurity System, [Online]. Available at:

tasks include (a) monitoring cyber incidents and cyber threats; (b) risk analysis in connection with disclosed cyber threats or cyber incidents; (c) exchanging information between authorised entities; (d) responding to cyber-attacks or cyber incidents; (e) issuing announcements about identified cyber threats or cyber incidents; (f) classifying incidents; and (g) conducting analyses, research, and development in the field of cybersecurity⁴⁰

In the Republic of Poland, the provision that responds to the implementation of the NIS directive is primarily the Act on the National Cybersecurity System, which was adopted on 5 July 2018. According to its provisions, the entities included in the above-mentioned system are (a) key service operators, (b) digital service providers, (c) CSIRT MON, (d) CSIRT NASK, (e) CSIRT GOV, (f) sector teams cybersecurity, (g) public finance sector entities, (h) research institutes, (i) National Bank of Poland, (j) Office of Technical Inspection, (k) Polish Air Navigation Services Agency, (l) Polish Center Accreditation, (m) National Fund for Environmental Protection and Water Management and provincial funds for environmental protection and water management, (n) commercial law companies performing public utility tasks, (o) entities providing cybersecurity services, (p) authorities competent for cybersecurity, (r) Single Contact Point for cybersecurity, (s) Government Plenipotentiary for Cybersecurity, and (t) Cybersecurity College.⁴¹

The Act also covers the Cybersecurity Strategy of the Republic of Poland, which was adopted in 2019 by the Council of Ministers for 2019–2024, which implements five specific objectives of the government's policy: (a) development of the national cybersecurity system; (b) increasing the level of resilience of public administration and sector information systems, and achieving the ability to effectively prevent and respond to incidents; (c) increase the national potential in the field of cybersecurity; (d) build awareness and social competencies in the field of cybersecurity; and (e) build a strong international position in the Republic of Poland in the area of

<https://www.nask.pl/pl/projekty-dofinansowane/projekty-realizowane-ze/3959,Dzialalnosc-biezaca-Zespolu-Reagowania-na-Incydenty-Bezpieczenstwa-Komputerowego.html> (Accessed: 10 February 2024).

⁴⁰ CSIRT of the Ministry of National Defence, [Online]. Available at: <https://csirt-mon.wp.mil.pl/pl/pages/zadania-2017-01-16-4/> (Accessed: 15 February 2024)

⁴¹ National cybersecurity system, [Online]. Available at: <https://sip.lex.pl/akty-prawne/dzuzdziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756> (Accessed: 15 February 2024)

cybersecurity.⁴² It is also worth mentioning the doctrinal document ratifying the doctrine of AJP 3.20, Operations in Cyberspace. Professor Piotr Dela is a recognised expert in the field of cybersecurity, with works on topics such as elements of the combat system in cyberspace,⁴³ the theory of combat in cyberspace,⁴⁴ and assumptions of operations in cyberspace,⁴⁵ as is Dr. Robert Janczewski.⁴⁶

3.4. Social potential of cybersecurity

According to the author and other experts, the social potential of cybersecurity is conditioned by the awareness of every citizen regarding threats to cyberspace and the related consequences. Educational, scientific, and technological developments have a significant impact on the development of cyberspace. Society plays a significant role in this respect if it is highly qualified and competent in the field of contemporary threats and security challenges, and constitutes invaluable social capital, thanks to which it is possible to ensure social development and, consequently, high quality of life and security of citizens.

The security of the state also depends on every citizen; therefore, awareness, knowledge, and skills in the field of cyber incidents that may occur or have already occurred are necessary. This can be achieved through an education system, awareness, application of security procedures, safe use of the Internet, activities in initiatives related to cybersecurity, reporting of cyber incidents, and civic initiatives (action within the community).

According to the author and experts, cybersecurity education should be implemented systematically to include several elements. The first are the curricula at the kindergarten, primary school, secondary school, and university levels, which should complement each other. The content should be age appropriate and cover issues such as online threats, basic rules for the safe use of the Internet, and rules for protecting private data. Along with the knowledge of these threats, it is necessary to focus on recognising them and applying an algorithm to deal with emerging cyber incidents.

⁴² Cybersecurity strategy of the Republic of Poland for 2019-2024, [Online]. Available at: <https://cyberpolicy.nask.pl/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024/> (Accessed: 22 February 2024).

⁴³ Dela, 2020b.

⁴⁴ Dela, 2020a.

⁴⁵ Dela, 2022.

⁴⁶ Janczewski, 2023.

At the student level, topics such as cryptography, information security, information society, IT security, detection of attacks on computer systems, security of computer systems, cyberdefence,⁴⁷ and cyber risk management should be included. In addition to exploring and improving their knowledge in the abovementioned areas, students should be able to conduct research in the field of cybersecurity and popularise their results on their own or together with their professors. Another element is the training and workshops in the military, non-military, and social sectors dedicated to working or serving society. The elements supporting the above measures are e-learning platforms containing training materials in the fields of cybersecurity, scientific research, technology development, and social incentives, although these should be classified as activities that signal the issue of cybersecurity.

An appropriate education system will contribute to increasing awareness of the consequences of threats in cyberspace, which will make citizens (a) capable of functioning in cyberspace using proven security practices such as setting strong passwords, updating software, ignoring suspicious links and attachments, and using anti-virus software; (b) use the Internet responsibly by not sharing personal data, private photos, and videos of themselves and their family members; material goods; checking their bank accounts; and monitoring transactions; (c) avoid participating in illegal activities on the Internet; (d) promote and popularise knowledge about safe functioning on the Internet; (e) report cyber incidents promptly; and (f) be careful when using public Wi-Fi networks.

Nowadays, in the face of many aggressive threats in cyberspace, citizens must have knowledge of them, as well as skills in using digital technologies and initiating security procedures. These factors will have a significant impact on ensuring the safety of individuals and the immediate environment, while also contributing to the broader goal of national security as part of a citizen's responsibility.

4. Conclusions

This analysis of the literature on the subject, reports, Internet sources, and interviews with experts allows us to conclude that cyberspace is a friendly environment in which various processes can take place. Therefore, this issue

⁴⁷ Cyber defence, [Online]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed: 23 April 2024).

should be considered comprehensively, in a systemic way, considering all the features associated with the term 'system'. It is vital to clearly indicate who is responsible for creating the cybersecurity policy, its strategy, and methods of implementation, as well as the entities responsible for employing the policy. With the dynamic technological developments, the security of cyberspace and society is changing. Currently, it is necessary to constantly recognise all current and potential threats and urgently and systematically introduce changes to legal provisions and procedures that will provide formal and practical opportunities to build cyber defence in individual countries and, consequently, in the structures of NATO and the EU.

In summary, the author of this article assumes that the cybersecurity system is a set of forces and resources understood as personal and material resources allocated by the state or states to implement tasks related to security in cyberspace. This system distinguishes between management and executive subsystems, consisting of the operational sector (security and defence) and the support sector (socioeconomic). It was also assumed that from the perspective of carrying out activities aimed at preventing or responding to cyberattacks or cyber incidents, the armed forces play a key role in the operational sector and society in the support sector.

Bibliography

- [1] Batorowska, H., Klepka, R., Wasiuta, O. (2019) *Media as an Instrument of Information Influence and Manipulation of Society*. Kraków: Libron.
- [2] Dela, P. (2020a) *Theory of combat in cyberspace*. Warsaw: Warsaw Academy of Art Publishing House.
- [3] Dela, P. (2020b) 'Elements of the combat system in cyberspace', *The Bellona Quarterly*, 2020/3, pp. 69-84; <https://doi.org/10.5604/01.3001.0014.6161>.
- [4] Dela, P. (2022) *Assumptions in cyberspace*. Warsaw: PWN Scientific Publishing House.
- [5] Dobek-Ostrowska, B., Fras, J., Ociepka, B. (1999) *Theory and Practice of Propaganda*. Wrocław: Publishing House of the University of Wrocław.
- [6] Janczewski, R. (2023) *Cyberfight. Military dimension of operations*. Warsaw: PWN Scientific Publishing House.
- [7] Kacała, T. (2015) 'Disinformation and Propaganda in the Context of Threats to National Security', *Przegląd Prawa Konstytucyjnego*, 24(2), pp. 49 - 65; <https://doi.org/10.15804/ppk.2015.02.03>.
- [8] Wiśniewski, B. (2013) *State security system. Theoretical and practical contexts*. Warsaw: PWN.

BÁLINT KOVÁCS*

Screening for Security: The Defence Sector as a Gateway to Broader Economic Control**

ABSTRACT: This paper explores certain aspects of defence industrial protectionism, and draws parallels with investment screening, as one of the major tools used to maintain economic security. Investment screening has been used quite often in the case of takeovers in the defence sector. Investments in this area, coming from either strategic partners or adversaries, have previously been blocked in several jurisdictions. While this was viewed as normal, the expansion of this treatment to other areas of the economy is a more recent development. Economic security, as a dimension of national security often takes precedence over liberal market principles. Several economic activities are now subject to screening, resulting in further state involvement in the economy, under the guise of the protection of economic security.

KEYWORDS: defence industry, national security, economic security, investment screening, broadening terms.

1. Introductory remarks

National security is a broad concept encompassing numerous dimensions and components. The international economic order, largely built upon neoliberal economic principles, in a period of low geopolitical competition, permits national security protection to prevail over free-market economics only in exceptional circumstances. While this rule remains in place, the number of exceptional circumstances triggering the national security exception appears to be increasing daily. Economic security, a dimension of

* Assistant Lecturer at the University of Szeged, and Senior Researcher at the Ferenc Mádl Institute of Comparative Law. The author would like to thank the attendees of the conference „Fortifying Europe: Selected Discussions on Common Security and Defence” organised by the Central European Academy in June 2024, for their valuable inputs, and the peer reviewers for their insightful suggestions. All errors remain the author’s own. balint1kovacs@gmail.com.

** The research and preparation of this study was supported by the Central European Academy.

national security that has been gaining greater attention, is increasingly used to justify state intervention in the economy on an unprecedented scale. This shift is driven, in part, by the expansion of economic areas considered *strategic*, as security is being addressed in a more complex and comprehensive manner. While military and defence-related economic activities have traditionally been clear-cut cases for national security protection, a growing number of economic sectors are now associated with this seemingly narrow domain. There has been a notable rise in defence-related technologies, an increase in technologies with *considerable dual-use potential*, and a broader recognition of sectors with strategic significance, ranging from high technology to academic research.

The heightened focus on security is relatively recent, as international agreements and domestic laws have historically prioritised economic benefits through market liberalisation and free trade. Even when certain countries introduced restrictions on or reviews of foreign investment in the 1970s, the primary objective appeared to be the enhancement of potential economic benefits. Such regulations were criticised at the time for granting governments ‘wide discretionary power’,¹ particularly because some states required foreign investment to align with the *national interest*, a term that was often defined with reference to economic considerations.² Nowadays, the situation is more explicit. From the expansion of the functions of the Committee on Foreign Investment in the United States (CFIUS),³ to the European Union’s (EU) introduction of national security reviews of foreign investment through regulation,⁴—which has prompted the adoption of various investment review mechanisms by its Member States—the *collective West* is strengthening its *geo-economic competition* toolkit. A key element of this strategy is the growing emphasis on economic security as a fundamental component of national security, including the imperative to safeguard certain *strategic interests*.

Focusing principally on the EU, this paper explores the intersection between defence industrial protectionism—often characterised by state intervention justified on national security grounds—and the extension of

¹ For example, in Canada, where it was also noted that wide discretion was actually needed for the system to be sufficiently flexible. See Cranston, 1973, p. 360.

² Ibid. pp. 361–362.

³ Via the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018.

⁴ Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, OJ L 79I, 21.3.2019, pp. 1–14.

such intervention to other areas of the economy. A case can be made for such an approach, as economic sectors beyond traditional defence are increasingly being incorporated into the broader concept of national security, effectively receiving similar treatment to that of the defence industry. The next section explores the expansion of the national security concept, which now includes *economic security*, as well as *food*, *data*, and *research security*. This broadening of scope is likely to extend the security exception to additional sectors of the economy, with potential implications for the existing framework of international economic law. Insights gained from the application of the security exception in the defence industry may provide valuable lessons in this regard.

The term *defence industry* should be interpreted broadly, as many companies, in pursuit of profitability, operate in both the military and civilian domains.⁵ Innovations emerging from the civilian sector now play an essential role in military equipment, and this interconnection has significant consequences for the further securitisation of other economic sectors. The third section of this paper explores these implications. The fourth section provides a brief analysis of investment screening—one of the most essential tools for ensuring economic security and preventing undesirable investments in the current geopolitical competition. The fifth section addresses the challenges of adapting to the economic security paradigm and presents two contrasting cases in which investment screening was applied to safeguard companies deemed strategic by the state. The final section offers the author's concluding remarks.

2. National security: Broadening

Although the national security exception has come under scrutiny in international dispute settlement, states continue to incorporate it into new mechanisms of economic control, often with limited judicial oversight.

The national security exception is not always compatible with the institutions of international economic law. In the rules-based system of international trade under the World Trade Organization (WTO), the *security exception*—embedded in Article XXI GATT, Article XIV GATS, and Article 73 TRIPS—was originally part of a *gentlemen's agreement*, intended for use only in truly exceptional circumstances.⁶ Controversy only

⁵ See also, Eisenhut, 2021, p. 278.

⁶ Nagy, 2021, p. 49.

recently arose in relation to tariff increases imposed by the first Trump administration on steel and aluminium products (Section 232 tariffs), which were challenged before a WTO dispute settlement panel. The panel found that the measures did not comply with the security exception in Article XXI(b)(iii) of the GATT⁷ invoked by the United States, as there was no evidence that they were ‘taken in time of war or other emergency in international relations.’ It may nevertheless be justified for a state to invoke Article XXI(b)(ii) of the GATT⁸ to implement a degree of protectionism aimed at preserving the production capacity of certain industries crucial for maintaining domestic defence capabilities.⁹ Such measures would be underpinned by the necessity of securing the supply chain for the production of certain defence materiel. Arguably, such measures would be upheld if taken in good faith, given that security exceptions are not entirely judicialized under the multilateral trading system.¹⁰ Much depends on whether protective measures are genuinely taken in good faith, as a vast array of goods can be linked to defence needs—‘from shoes to watches, radios to beef production’.¹¹ Consequently, if the national security exception is not appropriately curbed, its reach may be overly extended, potentially undermining the multilateral trading system. Similar concerns arise in the field of foreign direct investment (FDI) control.

Highlighting this crucial development, scholars have warned that the extensive use of economic security considerations in justifying national security exceptions could lead to their use as a protectionist tool ‘on everything from steel and aluminium to tents’.¹² Judicial intervention aimed at censoring actions of the executive branch underpinned by national security considerations is unlikely to be particularly assertive. In the context of investments, an *ex post* judicial review of a national security screening

⁷ Which reads as follows: „Nothing in this Agreement shall be construed to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests taken in time of war or other emergency in international relations”.

⁸ Which reads as follows: „Nothing in this Agreement shall be construed to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment”.

⁹ As suggested in Nagy, 2021, p. 56.

¹⁰ Ibid.

¹¹ Jackson, Davey, and Sykes, 2013, pp. 1199–1203 *apud* Nagy, 2021, p. 52.

¹² Roberts, Choer Moraes and Ferguson, 2019, p. 665.

decision may offer slightly more recourse than the WTO dispute settlement panel's decision. An investment arbitration case brought against an adverse screening decision—such as one resulting in the unwinding of an investment—may ultimately succeed. However, in the meantime, the investment remains obstructed. The immediate negative effects of investment screening are difficult to fully remedy. Strong regional economic integration organisations, such as the EU provide an additional layer of judicial scrutiny, which may override certain decisions made by national authorities and courts. However, such interventions may come too late for investors.¹³ Investment screening is not only a tool that can be applied swiftly, but is also one with quite a wide scope, allowing states a wide margin of appreciation for its application. In addition, there are other, more novel areas that are viewed through a *security lens*.

Data security has emerged as a particularly significant frontier of national security, with certain investors being required to divest from companies due to concerns about the nature of consumer data collected by their applications.¹⁴ Arguments related to data security have also been cited in policy moves against electric vehicles from China.¹⁵ Data security concerns were briefly referenced in the US Trade Representative's 2024 report to Congress.¹⁶ Meanwhile, Chinese electric vehicles have been subjected to high tariffs in the United States, the EU, and, more recently, Canada. Although data security was not a major focus of the report, its mention in the trade context raises the question of whether tariffs are truly an effective tool for protecting national security: in the mentioned context tariffs do not prevent the importation of the vehicles but merely make them more expensive. It is possible that high tariffs and data security concerns signal future regulatory measures aimed at a complete ban on Chinese electric vehicle (EV) imports.

Another emerging concern is food security, alongside the related concept of food sovereignty. These have been invoked as justifications for prohibiting foreign takeovers, even when the acquiring companies originate

¹³ Kovács, 2024, p. 224.

¹⁴ CFIUS forcing divestiture from *Grindr* and *PatientsLikeMe*, or more recently from *TikTok*.

¹⁵ In the US: Daly, 2024. Also in the UK: Churchill, 2024.

¹⁶ Executive Office of the President of the United States, 2024, p. II.

from allied countries.¹⁷ Similarly, academic research and collaborations between educational institutions are now regarded as integral to national security, with recent policy documents referencing *knowledge security* or *research security*.¹⁸ The potential security threats associated with knowledge security tend to centre on research and development projects with defence applications, particularly in engineering and material sciences. Innovation remains a cornerstone of military superiority. However, the role of the social sciences has not been entirely discounted. While no precise security threat has yet been identified in this field, collaborative research between European and Chinese academic institutions has been highlighted in reports on knowledge security.¹⁹

As the geopolitical competition intensifies, in the geopolitical turn, understanding the *security exception* in its various dimensions becomes increasingly pertinent. The defence industry, having consistently benefitted from protective measures, may offer insights into how this exception will be applied. This is particularly relevant for decision-makers seeking to ensure that the use of this exception is neither censured by domestic or international judicial bodies nor rendered prohibitively costly due to damages incurred.

3. The *special treatment* of the defence sector

The defence industry—including defence equipment procurement, investment, and trade—has long operated under a distinct regulatory framework that allows for both protection, by preventing the unwanted actors' involvement, and protectionism, through the application of industrial policy and preferential treatment. Even EU treaties have been drafted to accommodate such special treatment, requiring that subsequent rules and regulations align with these treaty provisions. As demonstrated herein, various controls may be imposed to prevent undesirable takeovers, mergers, and acquisitions, with investment screening being just one of them.

¹⁷ See the prohibition of takeover of French Carrefour by Canadian Couche-Tard, citing *food security* and *food sovereignty*, Barbaglia and Barzic, 2021. See also the prohibition by the Italian state of purchase of seed producer Verisem by Chinese-owned Syngenta.

¹⁸ Commission, 2024a. Executive Office of the President of the United States, 2024. Commission, 2022.

¹⁹ Navigating Challenges and Risks in Sino-European Academic Collaborations, Datenna, no date.

One of the broader exemptions from EU law is provided in Article 346(1)(b) TFEU, which states that ‘any Member State may take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material’. However, the application of this exemption is not without constraints. The European Commission has published an interpretative communication underscoring that Member States must ‘provide, at the Commission’s request, the necessary information and prove that exemption is necessary for the protection of their essential security interests.’²⁰ Furthermore, established CJEU case law mandates that any exemption must adhere to the principle of proportionality.

The *Schiebel* case before the CJEU,²¹ examined a particularly notable rule implemented by a Member State, which stipulated that any business engaged in the trade of military weapons and munitions, or in brokering such transactions, must have Austrian nationals as members of their statutory representation bodies or as their managing partner.²² In scrutinising these rules, the Court clarified that any derogation based on Article 346(1)(b) must be demonstrably necessary and proportionate to safeguarding a Member State’s essential security interests.²³

In the field of defence procurement, regulatory efforts to establish a European defence equipment market (EDEM), particularly through the Defence Procurement Directive,²⁴ have failed to significantly curtail preferential procurement practices or eliminate offset arrangements. A 2021 report commissioned by the European Parliament (EP) highlighted that Member States had introduced legislation making it ‘difficult to assess whether the Article 346 exception has been used for justified reasons of protection of national essential security interests, or just a way to limit the application of [the] Directive’.²⁵ By asserting control over defence

²⁰ Commission, 2006, p. 8.

²¹ Case C-474/12, *Schiebel Aircraft GmbH v Bundesminister für Wirtschaft, Familie und Jugend*, 4 September 2014.

²² *Id.*, para. 6.

²³ *Id.*, para. 37, 39.

²⁴ Consolidated text: Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC, OJ L 216 20 August 2009, p. 76.

²⁵ Schwab, 2021, p. 4/25.

acquisitions, Member States have leveraged procurement to strengthen their defence technological and industrial base, often by requiring offsets.

In the area of mergers and competition, Article 21(4) of the EU Merger Regulation²⁶ grants Member States jurisdiction over mergers that meet the Union dimension where the protection of legitimate interests—such as public security or specific public concerns—is warranted. This provision is frequently employed alongside Article 346 TFEU, with the latter typically analysed first.²⁷ Combining the two, and considering the opacity surrounding the use of the exemption under Article 346 TFEU, Member States may effectively thwart unwanted investments.

The Article 346 exemption may not suffice in certain circumstances, particularly as it is only triggered in ‘exceptional and clearly defined cases’.²⁸ With regard to dual-use goods, a category that continues to expand,²⁹ these are not even covered by the exemption under Article 346(1)(b). This is due to the explicit provision in the second part of this paragraph, which states that measures under it ‘shall not adversely affect the conditions of competition in the internal market regarding products not intended for *specifically* military purposes [emphasis added]’. Established case law holds that such derogations ‘do not lend themselves to a wide interpretation’.³⁰ This is further supported by jurisprudence³¹ as it pertains to dual-use goods. The rules governing dual-use goods seem clear in theory: in relation to civilian use, these goods are subject to general EU rules, while national security matters fall under Member States’ rules, in line with Article 346(1)(b) TFEU.³² However, discerning the *intended* use of dual-use goods is complex.

²⁶ Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings, OJ L 24, 29 January 2004, pp. 1–22.

²⁷ See Eisenhut, 2021, pp. 268–269, also for examples of cases, such as the takeover of Next AST by Altran Group, or the takeover of Atlas Elektronik by Thales Group, and others.

²⁸ C-414/97, *Commission of the European Communities v Kingdom of Spain*, 16 September 1999, para. 21.

²⁹ Commission Delegated Regulation (EU) 2023/2616 of 15 September 2023 amending Regulation (EU) 2021/821 of the European Parliament and of the Council as regards the list of dual-use items, published in OJ L 15 December 2023.

³⁰ C-414/97, *Commission of the European Communities v Kingdom of Spain*, 16 September 1999, para. 21.

³¹ Case T-26/01, *Fiocchi munizioni SpA v Commission of the European Communities*, 30 September 2003, para. 61, *apud* Trybus, 2014, pp. 94–95.

³² Craig and De Búrca, 2015, p. 347.

While it is easy to ascertain the use of semiconductors ordered by a company active in the defence industry, it is less straightforward when goods intended for civilian use are resold for military purposes.³³ Efforts are continually made to weed out economic actors involved in such practices and alert sellers to ensure compliance with export restrictions, thereby preventing unauthorised exports, reexports, or transfers.³⁴ Detecting investment activity in dual-use goods may be easier than tracking the final destination of a product. For example, identifying a company producing dual-use goods targeted for takeover by a civilian company with strong ties to an adversary nation's military may arguably be simpler than tracing a product sold to a foreign buyer. While dual-use goods are regulated at the EU level, the Regulation in question does not address investments, takeovers, mergers, or acquisitions.³⁵ To address this gap, the Commission strongly recommends that Member States adopt an investment screening mechanism focused on national security and public order to prevent unwanted capital flows into the dual-use sector and beyond.

The FDI Screening Regulation provides an exception to the free flow of capital for national security and public order reasons. Although this exception may seem wide and discretionary, it must be exercised under scrutiny. National security exceptions must be invoked within the limits of justifiability. Accordingly, EU Member States have both the right and the obligation to protect against investments that pose risks to themselves or the single market. The Regulation ensures EU-wide coordination and cooperation, as set out in Recital 7 and Article 1(2), while preserving Member States' responsibility for protecting their national security as per Article 4(2) TEU and their essential security interests under Article 346 TFEU.

The use of this national security exemption via investment screening must be justifiable in accordance with rule of law principles. As Recital 4 of

³³ An example is that of household appliances ending up as spare parts for military purposes, as suggested by the President of the European Commission Ursula von der Leyen at the Tallinn Digital Summit, and debunked by Tegler, 2023, *Is Russia really buying home appliances to harvest computer chips for Ukraine-bound weapons systems?* Forbes, 20 January 2023; and by Piedr, 2023.

³⁴ See Commission, 2023, Guidance for EU operators; or the Guidance issued by the Bureau of Industry & Security on 10 July 2024.

³⁵ See Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (recast), OJ L134, 29 May 2009.

the Regulation states, it ‘is without prejudice to the right of Member States to derogate from the free movement of capital as provided for in point (b) of Article 65(1) TFEU’. Under this, and in accordance with EU law, a restriction is permissible ‘only if there is a genuine and sufficiently serious threat to a fundamental interest of society’.³⁶ Recital 7 of the Regulation further stipulates that screening mechanisms must ensure legal certainty. Nevertheless, when evaluating national security decisions made by the executive branch, courts are likely to tread carefully. As stipulated by the Regulation, investors subject to screening obligations must be provided with an avenue for recourse against screening decisions.³⁷ The efficiency of such recourse will depend on numerous factors, with the political context playing an important role in the courts’ willingness to challenge such decisions. When reviewing measures concerning national security economic policy, courts generally exercise considerable deference.³⁸ This, coupled with the opacity of the screening procedure, is already highly likely to deter certain investors.

With respect to the key focal points of investment screening mechanisms, the defence industry is *primus inter pares*. Global competition is intensifying, and tools such as export controls and investment screening are increasingly deployed to prevent adversaries from acquiring Western technologies for purposes such as enhancing their military capabilities. The potential military threat is often cited as a principal reason for the introduction of (previously decoupling, nowadays) de-risking policies.³⁹ This positions defence industrial companies at the forefront, as primary targets of these tools. However, including defence-related industries within the scope of investment screening is somewhat perplexing, as many states view defence companies primarily ‘as part of their national security domain, closely linked to their defence and security policy, and only secondarily as an area of economic policy in a certain industry sector’.⁴⁰ Companies in this area have largely benefitted from state protection(ism).

³⁶ Case C-54/99, *Association Eglise de scientologie de Paris és Scientology International Reserves Trust kontra Premier minister*, 14 March 2000, para. 17, *apud* Hindelang, Moberg, 2020, pp. 1451–1452.

³⁷ Article 3(5) FDI Screening Regulation.

³⁸ Craig and De Búrca, 2015, p. 552.

³⁹ Josephs, 2024.

⁴⁰ Eisenhut, 2021, p. 266.

Criticism of EU defence industrial protectionism has come not only from NATO allies but also from major industry players within the EU.⁴¹ Nonetheless, the fate of defence industrial companies has rarely been left to the free-market principles applied to other sectors of the economy. Preserving a certain degree of armament autonomy through maintaining some defence industrial production capacity and the ability for autochthonous production to ensure security of supply is crucial to a country's security strategy. Considering the de-industrialisation that occurred in East-Central Europe after the fall of communism, affecting all areas of the economy, protectionism favouring local defence industrial players has been vital to preserve their capacity for autochthonous production. Even so, evidence suggests that the EU's eastward expansion has exacerbated the East-West imbalance in the defence industrial landscape.⁴²

In the context of the ongoing competition for technological supremacy, national security exceptions in international trade and investment may appear as mere tools of protectionism. However, this is only one interpretation. A closer examination of the structure of the defence industry reveals a more nuanced view, as currently large portions of the defence industry are commercially driven. This is a consequence of the fact that much technological innovation is commercially driven, from innovation in space technology, to the production of high technology components. Civilian technology and components produced in civilian industries have increasingly been used by defence companies. Conversely, to remain viable, defence companies have at times had to diversify their markets, thus producing for both civilian and defence sectors. The integration of civilian products into the defence supply chain introduces certain vulnerabilities, which regulators are now addressing. Security of supply is of paramount importance in the defence sector, and exposure to supply chain vulnerabilities can prove fatal. As a consequence of the integration of civilian technologies into military equipment production, further areas of the economy are now susceptible of being labelled as strategic and are now covered by new protective legal measures.

To ensure that other areas of the economy, especially companies in the expanding *dual-use* sector, receive adequate protection, investment screening has become a vital policy tool. The protection previously

⁴¹ Pfeifer and Foy, 2024; Mehta, 2018.

⁴² Briani et al., 2013, p. 34.

extended to undertakings in the defence industry may now be applied to undertakings in a broad range of adjacent economic sectors. As observed in a research note by the OECD, technological breakthroughs have expanded the scope of investment review mechanisms to encompass ‘non-traditional sectors’ in addition to traditional ones such as defence.⁴³ Additionally, as part of discussions on various dimensions of national security, states may also consider non-defence sectors as strategic and therefore subject to screening mechanisms. In the EU at least, the use of investment screening must also be justified, and the measures enacted must be proportional to the perceived threat.

4. Investment screening as a quintessential instrument of geoeconomic competition

Investment screening is a relatively novel tool through which the national security exception has been extended to new areas of the economy. In what could be called a rapid shift in attitude of the European Commission the EU adopted a more cautious approach to incoming FDI starting in 2017. At the request of the French, German, and Italian governments in February 2017, the Commission, after consulting with the EP, proposed a Regulation on the screening of FDI flowing into the EU. The proposal was adopted in March 2019, and the Regulation entered into force in October 2020.⁴⁴

The evolution of the EU’s approach to investment screening—amidst the repeated affirmation by then-Commission President Jean-Paul Juncker that ‘we are not naïve free traders’⁴⁵—has been well documented.⁴⁶ The FDI Screening Regulation, designed to encourage and coordinate the screening of FDI within the EU, is based on the Common Commercial Policy, Article 207(1) TFEU. Investment screening aims to block or unwind foreign investment in certain economic sectors based on national security and public order considerations. As a result of the screening process, an investment may be prohibited, allowed under certain conditions, or allowed unconditionally. However, the very existence of this mechanism, along with

⁴³ OECD, 2024, para. 8.

⁴⁴ Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, OJ L 79I, 21 March 2019, pp. 1–14.

⁴⁵ Commission, 2017.

⁴⁶ Hindelang and Moberg, 2020, pp. 1427–1435.

the obligation to undergo screening, may in itself discourage certain economic actors from proceeding with their investments.⁴⁷

As it moves towards becoming an established component of the EU's regulatory framework, the Commission is preparing to shift gears on FDI screening. In early 2024, the Commission published a package of five proposals aimed at strengthening the EU's economic security 'at a time of growing geopolitical tensions and profound technological shifts.'⁴⁸ These proposals target areas such as export controls, support for research and development involving technologies with dual-use potential, enhancing research security, as well as investment screening. Regarding the latter, two key dimensions must be noted: first, the strengthening of the existing system for investments coming into the EU, and second, the exploration of a regulatory framework for screening outbound investment.

The screening of investments into the EU has been part of the regulatory landscape for several years and is a factor that foreign investors must consider. The FDI Screening Regulation provides a blueprint for implementing national FDI screening mechanisms, offering guidance on key aspects such as time limits for the screening process, the possibility of judicial review, and the economic areas subject to scrutiny. It also establishes specific rules governing cooperation and information-sharing amongst Member States and with the Commission. While the Regulation does not impose an obligation to legislate, the document evaluating its impact presents arguments in favour of making screening mechanisms mandatory for all Member States.⁴⁹ Indeed, an investment established in any one Member State constitutes an investment within the EU, meaning some of its potential consequences are borne by all within the single market. This constitutes a robust argument for cooperation between Member States and the Commission regarding certain investments. However, such cooperation can easily be turned into a two-way avenue, as influence may also be exerted on Member States to adopt a particular stance on specific investments. This process is embedded within a screening procedure and cooperation framework that is, by default, subject to strict confidentiality. As a consequence, not only is judicial oversight limited, but broader mechanisms of public accountability—essential in a democratic society—may also be significantly curtailed or rendered opaque.

⁴⁷ As also noted in World Investment Report, 2021, p. 114.

⁴⁸ Commission, 2024a.

⁴⁹ Commission, 2024b, Section 3.2., p. 7.

The EU FDI Screening Regulation broadly identifies several areas of interest, including, *inter alia*, critical infrastructure in aerospace and defence, as well as critical technologies and dual-use items such as artificial intelligence, robotics, semiconductors, aerospace, defence, and nuclear technologies.⁵⁰ The proposal for a new FDI screening regulation⁵¹ expands the economic areas of interest in Annex II to include, *inter alia*, dual-use items, military technology and equipment, advanced semiconductors, quantum technologies, space and propulsion technologies, robotics, and autonomous systems. Annex II provides further guidance on these areas, while Annex I enumerates several EU funding programmes that require mandatory screening of investments in participating companies, including the European Defence Fund. Investments reviewed under Annex I must be notified to the cooperation mechanism between the Commission and Member States. Additionally, the proposed Regulation explicitly allows Member States to extend screening to economic sectors of particular importance to their national security and public order. Accordingly, Member States may include various economic activities within their screening mechanisms. Although screening decisions may be subject to judicial review—ultimately by the Court of Justice of the European Union (CJEU)—their immediate application may effectively thwart an investment.

Since its implementation, EU Member States have accumulated some experience with investment screening, and judicial practice has contributed to a clearer understanding of the Regulation's scope and application.⁵² Such judicial interpretation is valuable, as challenges in defining the Regulation's scope of application were revealed in the opposite conclusions reached in the judgment of the CJEU,⁵³ and the opinion of Advocate General Ćapeta⁵⁴ that preceded it.⁵⁵ Judicial proceedings have also revealed in part how the mechanism is used, especially in cases of misuse.

⁵⁰ Article 4(1)(a)–(b) of the Regulation.

⁵¹ Commission, 2024c.

⁵² Kovács, 2024; Kovács, 2023.

⁵³ C-106/22, *Xella Magyarország Építőanyagipari Kft. v Innovációs és Technológiai Miniszter*, 13 July 2023.

⁵⁴ Opinion of Advocate General Ćapeta delivered on 30 March 2023 in Case C-106/22 *Xella Magyarország Építőanyagipari Kft. v Innovációs és Technológiai Miniszter*.

⁵⁵ See also Di Benedetto, 2023. The proposed reform of the Regulation extends its applicability to *indirect* acquisition of control over an EU target, in line with many national screening regimes that already cover such cases.

In this new era of great power rivalry, investment screening serves as an essential, gap-filling instrument for mitigating security risks posed by unencumbered FDI. Its use may prevent systemic rivals from gaining control over sensitive emerging technologies or critical infrastructure. Asymmetries in national economic openness have exposed not only economic but also security vulnerabilities. European companies being ‘acquired as part of other countries’ strategic industrial policies’ is rightly perceived as a major threat.⁵⁶ The targeting of companies operating in strategically sensitive areas, including dual-use items, was among the key arguments for implementing FDI screening mechanisms.⁵⁷ However, what constitutes a *strategically sensitive* area is often a political decision, which also influences screening outcomes.⁵⁸ This fact may place certain screening decisions on a collision course with rule of law principles.

5. Adjustment to the economic security paradigm

As an increasing number of economic areas receive the special attention previously reserved for the defence industry, some of the principles and legal frameworks applied to the defence sector are now being transposed to other sectors. This shift reflects evolving perceptions of security risks. On one hand, there is a heightened awareness of security threats, exacerbated by Russia’s aggression against Ukraine, which has underscored hard defence risks. On the other hand, broader security considerations, such as economic security, are rising on national agendas. The principal objective of economic security measures is to mitigate dependencies—that is, to equip states with tools for intervention to prevent overreliance on particular supply chains and reduce economic vulnerabilities.

Notably, language traditionally associated with defence economic management is now being used to articulate other economic desiderata. Some of the rhetoric underpinning these newfound ambitions for *protection* has long justified *protectionism* in military procurement and the development of the domestic defence technological and industrial base. Terms such as militarily consequential goods, potential for dual-use, and security of supply are only some of the terms that more frequently appear in

⁵⁶ Proposals for ensuring an improved level playing field in trade and investment, Eckpunktepapier, 21 February 2017.

⁵⁷ Hindelang and Moberg, 2020, p. 1430.

⁵⁸ As also noted by Vig, 2020, p. 17.

discussions concerning economic activities and products previously outside the realm of the defence sector. Given that many civilian technologies are now assessed through the lens of their *potential for dual-use*, the adoption of defence-related terminology may be considered appropriate. Consequently, in an international economic paradigm, where non-discrimination was once paramount, there is now a discernible shift towards prioritising domestic or *like-minded economies* to preserve technological and strategic independence.⁵⁹

Navigating this evolving landscape presents significant challenges for legal practitioners—and even greater ones for businesses. As regulatory lists and designations expand, with more economic actors and products subject to sanctions and export controls, the prevailing trend is rather one of overcompliance. The regulatory complexity discourages companies from engaging with businesses closely linked to those affected by export controls and sanctions.⁶⁰ While these instruments may deter some investors, investment screening, by comparison, appears as an instrument which may be used with surgical precision.

Within the EU, Member States are solely responsible for their security needs, often excluding the defence industry from standard market regulations and free-market logic. Ensuring security of supply entails various controls that effectively normalise protectionism in this sector.⁶¹ These measures range from preferences in defence procurement and the use of offset requirements, to outright prohibitions on unwanted takeovers. As economic security is becoming part and parcel of foreign and economic affairs, similar protective measures will likely extend to other sectors deemed critical for maintaining economic security.

Legal instruments designed to uphold economic security must be effective in countering adversaries' attempts to impose economic coercion while remaining rooted in a rule of law system. Given this objective, it is understandable why such instruments must accord states a wider margin of discretion—particularly when the aim is as abstract as building resilience against economic disruptions. Their compatibility with rule of law principles remains an open question, as it may ultimately depend on the extent to which states feel compelled to invoke security exceptions in response to emerging threats.

⁵⁹ See also Eisenhut, 2021, p. 272.

⁶⁰ As was noted by Crosignani et al., 2024, pp. 20–23.

⁶¹ This has been the case for decades, as demonstrated by Commission, 2006.

The much-criticised *margin of discretion* is wide both in terms of states' discretion in determining their security interests and in relation to the economic activities that the screening mechanism may be applied to. Regarding trigger mechanisms for screening, the use of broadly defined criteria for review, such as *defence and security*, is noteworthy.⁶² Additionally, the expansion of the list of economic activities to which screening criteria apply must also be noted. Conversely, some have criticised investment screening mechanisms for having too narrowly defined a scope. One screening authority concluded that it did not have jurisdiction over a particular acquisition of a company owning technology that could also have military applications. In another case, the same authority chose not to scrutinise the acquisition of a company active in the development of 6G technology and semiconductors for radar systems.⁶³

Such criticism is commensurate with commentators' mention of *clean energy* as part of *dual-use*, alongside 5G, quantum computing, and artificial intelligence.⁶⁴ Defence-related industries are often referred to as *sensitive* or *critical*, and are subject to lower thresholds triggering screening.⁶⁵ Crucial factors triggering screening include the sensitivity of the economic activity targeted by the investment, the origin and economic activities of the investor, and the level of control or influence sought by the investor. Sensitivities may thus be triggered by the target company's products having defence potential, or by the investor's ties to a country's military. While it is quite clear that investment screening is a tool aimed principally at acquisitions made by companies linked to adversaries, the sensitive nature of the investment may result in the prohibition of investments made by companies from friendly countries.

The expansion of the list of sensitive sectors, especially in light of what is now considered dual-use or strategic, is striking. These factors together result in more investment control, and potentially more transactions

⁶² A policy brief observing trends on investment screening in G20 countries that have them, takes note of criteria such as: national security, public order, national interest, public security, national defence, essential interests of the state, defence interests, public safety, public health, smooth operation of the economy, essential security interests, etc. See Mildner and Schmucker, 2021, pp. 5–9.

⁶³ See the acquisition of Nowi by Nexperia, and the acquisition of Ampleon by „a Chinese investor”, as reported by Linklaters, 2024.

⁶⁴ Tyson and Zysman, 2024.

⁶⁵ See also Country Notes published by the CELIS Institute, [Online]. Available at <https://www.celis.institute/resources/#Countryreports> (Accessed: 12 July 2024).

being thwarted. A notable example in this regard is the acquisition of the German satellite and radar technology firm IMST by the Chinese defence company Addisino Co. Ltd. Several reasons led the state to oppose the acquisition, as reported in the press: the acquirer was a subsidiary of the Chinese state-owned entity China Aerospace and Industry Group (CASIC), the target company provided components to the German military, and the target company benefited from state funding. However, according to media reports, the company's owners were very dissatisfied with the decision of the competent authority to block the acquisition, arguing that their contribution was to a particular satellite of civilian use, which was only later used also by the Bundeswehr.⁶⁶

Despite the company owners' arguments that theirs was a strictly civilian technology firm, the competent ministry still considered the acquisition too sensitive to approve. While it may be argued that the research and development conducted with state funding should preclude such a sale, all such research was published and publicly accessible, as noted by ISMT owners, who also mentioned that the company was already part-owned by Chinese partners. The ministry's decision was contested in court, but the case was later withdrawn.⁶⁷ The fact that the acquisition was blocked even though the target company considered itself *civilian*, and noted that its technology was already freely available in research publications, reinforces in a sense that politics play a major role in screening decisions. More to this point: the owners were planning to sell their stake to a close business associate who was already a part-owner and presumably had access to all the technology developed by the target company.

In France, the state used investment screening measures to block the acquisition of Photonis, a high-technology company producing light intensification equipment, used in both nuclear and military technology. The bidder was Teledyne, a US-based company.⁶⁸ In this case, the French government chose to assert its strategic interests, even in relation to a company from a strategic partner.⁶⁹ Part of the rationale for the ban was to

⁶⁶ Neßhöver and Slodczyk, 2020.

⁶⁷ Von Rummel and Stein, 2024.

⁶⁸ Bernard, 2020. A similar case was the vetoing of the takeover of French companies Segault and Velan SAS by American group Flowserve, see: Leali and De Villepin, 2023.

⁶⁹ A similar situation occurred in the proposed acquisition of the Italian company Next AST by the French group Altran, which was blocked by the Italian government in view of the strategic activities of the company in the Italian defence sector. See Senato della Repubblica, 2018, p. 11.

‘prevent Photonis from ending up subject to the US International Traffic in Arms Regulations, thereby restricting its future export activity.’⁷⁰ This case highlights another important factor considered by states during investment screening: export controls, particularly in the expanding domain of defence-related and dual-use technologies.⁷¹ Screening in such cases appears increasingly complex, with more factors taken into account during the attempted takeover of a company in a strategic domain.

The above cases are excellent examples of the variation in state interest. The readiness of the state to block the takeover of a company partly owned by the acquirer is noteworthy. In this case, it is questionable how effective the protective measure actually was, considering that the acquirer, a Chinese company with a minority shareholding, had access to the company’s technologies. The state essentially insisted that the company’s technology was dual-use. By contrast, in two other cases where dual-use could have easily been argued, the state chose not to block the takeovers. Finally, there was the blocking of a takeover by a company from a partner country, justified by the need to protect state strategic interests, maintain control over a particular technology, and prevent it from becoming subject to an ally’s security measures, specifically export controls. These cases demonstrate the variation in state interest and buttress the view that investment screening is a tool to be applied with surgical precision.

6. Concluding remarks

The numerous dimensions of national security that have recently gained prominence, among which economic security stands out, also require new tools for their protection. The defence sector has been subject to special treatment within the EU, with carve-outs in its legal system allowing Member States to exercise a certain level of protectionism. The use of these carve-outs has also shown their limits. Investment screening is a tool that addresses some of these gaps, facilitating state intervention in economic activities that the state considers to be strategic. It thus helps to prevent dual-use or critical technologies from coming under the control of adversaries.

In the wider scheme of things, the introduction of these new instruments to protect economic security may restrict market efficiency and

⁷⁰ Bet-Mansour, 2023.

⁷¹ A point also highlighted in Viski, 2024, pp. 10–11.

foster a new economic paradigm inspired by the economic logic traditionally reserved for the defence sector, focusing on security of supply and the safeguarding of sensitive technologies. This begs further questions: what will happen to a target company, from which the owners wish to exit, but where the state does not agree with the proposed investor taking over? Should the state step in to take over such a company? Can anyone be forced to maintain ownership of a business? These are questions that merit further attention and suggest a likely conclusion: protection begets protectionism. Protecting national security may ultimately force states into actions that would come under the label of economic protectionism.

Bibliography

- [1] Barbaglia, P., Barzic, G. (2021) 'Exclusive: Canada's Couche-Tard drops \$20 billion Carrefour takeover plan after French government opposition, say sources', *Reuters*, 16 January 2021.
- [2] Bernard, J. (2020) 'French veto to the acquisition of Photonis par Teledyne', *Delcade*, 23 December 2020. [Online]. Available at: <https://www.delcade.com/2020/12/23/french-veto-to-the-acquisition-of-photonis-par-teledyne/> (Accessed: 11 July 2024).
- [3] Bet-Mansour, E. R., et al. (2023) 'French Foreign Investment Prohibition of U.S. Deal Highlights Regime's Importance for International M&A', *Debevoise*, 6 December 2023, [Online]. Available at: <https://www.debevoise.com/insights/publications/2023/12/french-foreign-investment-prohibition-of-us-deal> (Accessed: 11 July 2024).
- [4] Churchill, D. (2024) 'Spooks probe whether Chinese-made electric cars could be spying on Brits for Beijing', *Daily Mail*, 18 April 2024. [Online]. Available at: <https://www.dailymail.co.uk/news/article-13325527/Spooks-probe-Chinese-electric-cars-spying-Brits-Beijing.html> (Accessed: 11 July 2024).
- [5] Crosignani, M., Han, L., Macchiavelli, M., Silva, A. F. (2024) 'Geopolitical Risk and Decoupling: Evidence from U.S. Export Controls', *Federal Reserve Bank of New York Staff Reports*, no. 1096 April 2024; <https://doi.org/10.59576/sr.1096>.
- [6] Craig, P., De Búrca, G. (2015) *EU Law*, Sixth Edition. Oxford: OUP.
- [7] Cranston, R. (1973) 'Foreign investment restrictions: defending economic sovereignty in Canada and Australia', *Harvard International Law Journal*, 14(2), pp. 345–367.

-
- [8] Daly, M. (2024) 'Biden orders US investigation of national security risks posed by Chinese-made 'smart cars'', *Associated Press*, 29 February 2024.
- [9] Di Benedetto, F. (2023) 'Indirect FDI under EU FDI regulation in times of war: is the anti-circumvention clause enough? Columbia Center on Sustainable Investment', *Columbia FDI Perspectives*, No. 972.
- [10] Eisenhut, D. (2021) *The Defence, Military and Dual-Use Sector*, in Hindelang, S., Moberg, A., *YSEC Yearbook of Socio-Economic Constitutions 2020 – A Common European Law on Investment Screening (CELIS)*, Springer: Cham, pp. 265–282; https://doi.org/10.1007/16495_2020_19.
- [11] Hindelang, S., Moberg, A. (2020) 'The art of casting political dissent in law: The EU's framework for the screening of foreign direct investment', *Common Market Law Review* 57, pp. 1427–1460; <https://doi.org/10.54648/COLA2020743>.
- [12] Jackson, J. H., Davey, W. J., Sykes A. O. (2013) *Legal Problems of International Economic Relations*, St. Paul: West Academic Publishing.
- [13] Josephs, J., (2024) 'Protectionism eroding global business' – world trade chief, BBC News, 8 July 2024.
- [14] Kovács, B. (2023) National Interest and Freedom of Establishment: The CJEU's Judgment in Xella, CELIS Blog, 14 August 2023. [Online]. Available at: <https://www.celis.institute/celis-blog/national-interest-and-freedom-of-establishment-the-cjeus-judgment-in-xella/> (Accessed: 30 April 2024).
- [15] Kovács, B. (2024). *Facilitating and Scrutinizing National Security Measures: Analysis of an Investment Screening Case in the European Union*. In: Springer Studies in Law & Geoeconomics. Springer: Cham, (forthcoming); https://doi.org/10.1007/17280_2024_24.

-
- [16] Leali, G., De Villepin, P. (2023) France blocks American takeover of nuclear suppliers, *Politico*, 6 October 2023. [Online]. Available at: <https://www.politico.eu/article/france-vetoes-american-takeover-nuclear-supplier-segault-velan-flowserve/> (Accessed: 11 July 2024).
- [17] Mehta, A. (2018) US warns against ‘protectionism’ with new EU defense agreement, *DefenseNews*, 14 February 2018. [Online]. Available at: <https://www.defensenews.com/smr/munich-security-forum/2018/02/14/us-warns-against-protectionism-with-new-eu-defense-agreement/> (Accessed: 12 July 2024).
- [18] Mildner, S. A., Schmucker, C. (2021) *Investment Screening: Protectionism and Industrial Policy? Or Justified Policy Tool to Protect National Security?* September 2021, pp. 5-9. [Online]. Available at: https://www.t20italy.org/wp-content/uploads/2021/09/TF3_PB08_LM04.pdf (Accessed: 20 June 2024).
- [19] Nagy, Cs. I. (2021) ‘A Re-Conceptualization of WTO Law’s Security Exceptions: Squaring the Circle and Judicializing National Security’, *Journal of International Economic Law*, 24(2), pp. 49–59.
- [20] Neßhöver, C., Slodczyk, K. (2020) ‘Altmaier verbietet Verkauf von Kleinfirma nach China’, *Manager Magazin*, 3 December 2020. [Online]. Available at: <https://www.manager-magazin.de/unternehmen/industrie/peter-altmaier-wirtschaftsminister-bremst-chinesische-investoren-aus-a-1083ae9e-14cd-4eea-9fc4-29e18b7c388a> (Accessed: 11 July 2024).
- [21] Pfeifer, S., Foy, H. (2024) ‘Saab chief warns against EU defence protectionism’, *Financial Times*, 21 April 2024. [Online]. Available at: <https://www.ft.com/content/5db7c8a5-84c5-4400-a52a-67f4eb2039cc> (Accessed: 12 July 2024).
- [22] Piedra, J. M. (2023) ‘EU to sanction home appliance exports to Russia?’, *Asia Times*, 14 April 2023.

-
- [23] Roberts, A., Choer Moraes, H., Ferguson, V. (2019) 'Toward a Geoeconomic Order in International Trade and Investment', *Journal of International Economic Law*, 22(4), pp. 655–676; <https://doi.org/10.1093/jiel/jgz036>.
- [24] Schwab, A. (2021) 'Report on the implementation of Directive 2009/81/EC, concerning procurement in the fields of defence and security, and of Directive 2009/43/EC, concerning the transfer of defence-related products', *Committee on the Internal Market and Consumer Protection*, A9-0025/2021, 8 March. [Online]. Available at: https://www.europarl.europa.eu/doceo/document/A-9-2021-0025_EN.html (Accessed: 14 July 2024).
- [25] Tegler, E. (2023) 'Is Russia really buying home appliances to harvest computer chips for Ukraine-bound weapons systems?' *Forbes*, 20 January 2023.
- [26] Trybus, M. (2014) *Buying Defence and Security in Europe – The EU Defence and Security Procurement Directive in Context*. Cambridge: Cambridge University Press; <https://doi.org/10.1017/CBO9780511751462>.
- [27] Tyson, L., Zysman, J. (2024) *The New Industrial Policy and Its Critics*, *Project Syndicate*, 17 November 2023. [Online]. Available at: <https://www.project-syndicate.org/onpoint/the-case-for-new-industrial-policy-by-laura-tyson-and-john-zysman-2023-11> (Accessed: 20 June 2024).
- [28] Vig, Z. (2020) 'The Regulation of Screening of Foreign Direct Investment in the European Union', *Pro Futuro*, 2020/4; <https://doi.org/10.26521/profuturo/2020/4/9463>.
- [29] Viski, A. (2024) *Foreign Direct Investment (FDI) Screening: A Primer*, The Stimson Center, June 2024.

-
- [30] Von Rummel, L. F., Stein, R. M. (2024) *Snapshot: foreign investment law and policy in Germany*, Lexology, 16 January 2024. [Online]. Available at: <https://www.lexology.com/library/detail.aspx?g=7b44bbc8-3553-4396-8a9b-cd4ca5876f37> (Accessed: 11 July 2024).
- [31] Briani, V., Marrone, A., Mölling, C., Valasek, T. (2013) *The Development of a European Defence Technological and Industrial Base (EDTIB)*, European Parliament, Directorate-General for External Policies, Luxembourg: Publication Office; <https://doi.org/10.2861/15836>.
- [32] European Commission (2006) ‘Interpretative Communication on the application of Article 296 of the Treaty in the field of defence procurement’ COM (2006) 779 final, Brussels, 7 December.
- [33] European Commission (2017) Press Release: State of the Union 2017 – Trade Package: European Commission proposes framework for screening of foreign direct investments. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3183 (Accessed: 28 May 2024).
- [34] European Commission (2022) Tackling R&I Foreign Interference, Staff Working Document, January 2022.
- [35] European Commission (2023) Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention.
- [36] European Commission (2024a) Commission proposes new initiatives to strengthen economic security, Press Release, 24 January 2024.
- [37] European Commission (2024b) Commission Staff Working Document Evaluation of Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, SWD (2024) 23 final, Brussels, 24.01.2024, Section 3.2.

- [38] European Commission (2024c) Proposal for a Regulation of the European Parliament and of the Council on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452 of the European Parliament and of the Council, Brussels, 24.1.2024, COM (2024) 23 final.
- [39] Executive Office of the President of the United States (2022) Office of Science and Technology Policy, Memorandum for the Heads of Federal Research Agencies, Guidelines for Research Security Programs at Covered Institutions, 9 July 2024. European Commission, Tackling R&I Foreign Interference, Staff Working Document, January 2022.
- [40] Executive Office of the President of the United States (2024) Office of the United States Trade Representative, Report to Congress on the operation of the United States-Mexico-Canada Agreement with respect to trade in automotive goods, 1 July 2024.
- [41] Guidance issued by the Bureau of Industry & Security on 10 July 2024. [Online]. Available at: <https://www.bis.gov/press-release/bis-issues-guidance-addressing-export-diversion-risks> (Accessed: 11 July 2024).
- [42] Linklaters (2024) Foreign investment control in the Netherlands – Lessons learnt from one year of experience, 8 July 2024. [Online]. Available at: <https://www.linklaters.com/en/insights/blogs/foreigninvestmentlinks/2024/july/netherlands-one-year-on> (Accessed: 8 July 2024).
- [43] Navigating Challenges and Risks in Sino-European Academic Collaborations, Datenna (no date).
- [44] OECD (2024) Managing security implications of international investment: Policy developments in a changing world, Secretariat research note.

-
- [45] Proposals for ensuring an improved level playing field in trade and investment, Eckpunkt Papier, 21.02.2017. [Online]. Available at: <https://www.bmwk.de/Redaktion/DE/Downloads/E/eckpunkt Papier-proposals-for-ensuring-an-improved-level-playing-field-in-trade-and-investment.html> (Accessed: 30 April 2024).
- [46] Senato della Repubblica (2018) Relazione concernente l'attività svolta sulla base dei poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, Aggiornata al 31 dicembre 2018, p. 11. [Online]. Available at: https://www.governo.it/sites/governo.it/files/GP_RelazioneParlamento_2018.pdf (Accessed: 11 July 2024).
- [47] Speech President of the European Commission Ursula von der Leyen at the Tallinn Digital Summit. [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_6063 (Accessed: 11 July 2024).
- [48] World Investment Report 2021. New York: UNCTAD.

KAJA KOWALCZEWSKA*

Human oversight and risk-based approach to artificial intelligence: What does the Artificial Intelligence Act have in common with discussions about lethal autonomous weapon systems?*

ABSTRACT: The regulation of artificial intelligence (AI) is a pressing global concern, with various regulatory bodies aiming to foster innovation while safeguarding humanity's interests. This article synthesises perspectives on AI regulation in civilian and military domains, highlighting common ethical foundations and legal proposals. Emphasising the European Union's ethical community as delineated by fundamental rights, it explores the Artificial Intelligence Act and debates on lethal autonomous weapon systems within the Convention on Certain Conventional Weapons. By analysing the overlap between civilian and military ethics, the article argues for a shared objective: promoting innovation while upholding human dignity through robust regulations that ensure human oversight and a risk-based approach. The article contends that the consensus on substantive issues regarding military AI regulation is imminent, but its formalisation through legal means may lag behind.

KEYWORDS: Artificial Intelligence, Ethics, European Union, Lethal Autonomous Weapon Systems, Human Oversight, Risk-Based Approach.

1. Introduction

Various regulatory bodies worldwide are formulating regulations pertaining to the utilisation of artificial intelligence (AI), each drawing upon its specialised expertise. Amidst this diversity, a shared objective emerges: the regulation of AI to foster innovation for the betterment of humanity. This leads to the following question: what exactly does this objective mean, and how can it be guaranteed through legal regulations? This article summarises

* This article came about within the framework of Academic Excellence Hub – Digital Justice Center carried out under Initiative of Excellence – Research University at the University of Wrocław, Poland. kaja.kowalczevska@uwr.edu.pl.

** The research and preparation of this study was supported by the Central European Academy.

the main perspectives regarding the regulation of AI in civilian and military applications, focusing on identifying common ground, particularly concerning ethical foundations and the associated legal proposals.

One of the primary challenges associated with ethics is the fact that ethical concerns, which underpin and anticipate legal norms, vary significantly across states. However, within the European Union (EU), which is not only an economic entity but also a community founded on shared values, it can be argued that such an ethical community is delineated by values that are legally safeguarded and enshrined as fundamental rights.¹ Accordingly, this article examines the general-purpose AI regulation outlined in the Artificial Intelligence Act (AIA)² as well as the ongoing discourse surrounding lethal autonomous weapon systems (LAWS) within the Convention on Certain Conventional Weapons (CCW) forum. The discussion focuses on the positions advanced by EU member states in these discussions as exemplified in the two-tier approach and draft articles. The selection of these two overarching AI categories is predicated on the premise that legal norms governing peacetime and armed conflict, despite their apparent dichotomy and to a limited extent, share common ethical principles. I contend that the prohibition of certain use cases incompatible with the requirement of public conscience (unacceptable risk) and the insistence on human responsibility that cannot be delegated to AI-based machines (human oversight) represent such paramount considerations. In civilian AI applications, the requisites of public conscience are grounded in values such as democracy, the rule of law, and human rights.³ Conversely, in military contexts, they derive from the paradigm of international humanitarian law (IHL), which entails balancing the principles of humanity and military necessity. Thus, the overarching objective in both realms of AI applications is the promotion of technological innovation for the collective benefit of humankind, guided by ethical considerations rooted in principles aimed at protecting human dignity.

With the recent adoption of the AIA and the emergence of other global initiatives,⁴ the conversation surrounding AI regulation has shifted

¹ Wouters, 2020, pp. 11–38.

² European Parliament, 2024.

³ Załucki and Miraut, 2021.

⁴ Responsible Artificial Intelligence in the Military (REAIM), 2023; United Nations Secretary-General, 2023; United Nations Educational, Scientific and Cultural Organization, n.d.; Organisation for Economic Co-operation and Development, n.d.

from being taboo to becoming one of the most prominent subjects of discussion.⁵ While discussions within the CCW forum have persisted for over a decade, tangible outcomes remain elusive. The AIA, particularly on a regional level, has clearly delineated several unacceptable risks associated with potent AI models. This juncture may signify a crucial moment, especially concerning matters of warfare, with states still deliberating the acceptability of various autonomous weapons and the conditions under which they may be employed. This article proposes that consensus on substantive matters is imminent but that formalisation through legal regulation may remain distant.

Regulations, as exemplified by those articulated in the AIA, adopt a risk-based methodology to define the parameters of acceptable AI applications, demarcating the thresholds beyond which certain uses are considered unacceptable. Traditionally, regulations governing security and warfare have been distinct from those governing civilian affairs and peace. However, AI is unique in its capacity to gradually blur these boundaries, as in the need to address the bias issue.⁶ This phenomenon is particularly apparent in technologies with dual-use capabilities, serving both military and law enforcement purposes. Art. 2(3) of the AIA underscores this convergence, thereby blurring the distinction between security-related and civilian-focused regulatory concerns. Consequently, debates surrounding LAWS bear similarities to those concerning the deployment of social scoring or real-time biometric classification systems. In both cases, the central issue is how to delineate the ethical and moral boundaries of technological integration within societal and armed conflict contexts. Thus, the risk-based approach is increasingly permeating discussions on military applications of AI.

First, this article examines the AIA, emphasising its ethical foundation, risk-based methodology, and human oversight, including the exclusion of military applications. Second, the article explores debates on LAWS, highlighting concerns about unacceptable risks and the necessity of human oversight as emerging common points, followed by a conclusion.

⁵ Ramos et al., 2024, p. 34.

⁶ Bode, 2024.

2. Artificial Intelligence Act: The landmark law on general purpose artificial intelligence

The European Parliament adopted the AIA on 13 March 2024, marking a significant milestone in technology governance.⁷ Negotiated with the member states in December 2023, the regulation garnered widespread recognition as a landmark law, signalling a unified stance on advancing a new governance model rooted in technology. While the official version of the EU regulation remains pending, indications suggest that substantial amendments are unlikely, with the anticipated revisions being primarily cosmetic. Following three years of negotiations, the EU has emerged as a trailblazer in the legal regulation of civilian AI applications. The following section will offer an exposition of the AIA's ethical principles and a synthesis of the adopted risk-based approach, concluding with a discussion of why, in principle, the AIA does not extend to military AI applications.

The AIA represents a comprehensive legislative endeavour aimed at fostering technological innovation while safeguarding fundamental rights, particularly in contexts where highly impactful AI models pose risks. This alignment with fundamental rights protection is not unexpected, given the EU's adherence to the Charter of Fundamental Rights⁸ and the commitment of its member states to the European Convention for the Protection of Human Rights and Fundamental Freedoms.⁹ These states have pledged to uphold high standards of human rights protection amidst evolving technological and economic landscapes.

In the AIA, numerous references underscore the importance of values, such as health protection, safety, fundamental rights, democracy, the rule of law, and environmental sustainability. Moreover, the text of the AIA reflects a cohesive approach towards these emerging values, which have surfaced in discussions regarding broader AI applications.¹⁰ This is why the fundamental prerequisite outlined in the AIA is the establishment of trustworthiness in AI.¹¹ Central to this notion is the concept of “human-

⁷ Members of the European Parliament. overwhelmingly approved the Act, with 523 votes in favour, 46 against, and 49 abstentions.

⁸ Charter of Fundamental Rights of the European Union, 2000.

⁹ Convention for the Protection of Human Rights and Fundamental Freedoms, 1950.

¹⁰ Trustworthy AI, human agency and oversight, and traceability and explainability.

¹¹ Díaz-Rodríguez et al., 2023.

centricity”, wherein AI is envisioned as a tool serving the interests of people, with the overarching objective of enhancing human well-being.¹² In order to fulfil this mission, AIA draws from the meta-framework of ethical consideration that preceded the regulatory effort and should be presented as a normative prerequisite of the legal regulation.

2.1 Ethical underpinnings

The AIA builds upon the foundational work of the AI High-Level Expert Group, which established seven non-binding ethical principles for AI aimed at ensuring trustworthiness and ethical integrity in AI development and deployment.¹³ The preamble of the AIA declares that efforts should be made to integrate these principles into the design and utilisation of AI models wherever feasible. Furthermore, they are posited as fundamental components for the creation of codes of conduct consistent with AI regulations. The recommendation extends to all stakeholders, encompassing industry players, academic institutions, civil society organisations, and standards bodies, who are encouraged to adopt these ethical principles as they craft voluntary best practices and standards. Thus, these principles constitute essential pillars that should underpin any forthcoming regulatory framework governing AI within the EU.

Paramount consideration is accorded to the principles governing human agency and oversight. Within this framework, AI systems must be conceptualised and operationalised as instruments subservient to human interests while upholding fundamental tenets of human dignity and personal autonomy. Such systems must be engineered to operate within parameters amenable to human control and supervision, thereby ensuring alignment with ethical imperatives.¹⁴

Furthermore, the imperatives of technical robustness and safety require AI systems to be resilient against operational exigencies and impervious to external manipulations aimed at subverting their intended utility. This necessitates the development and deployment of AI technologies with robust mechanisms capable of withstanding adversities and thwarting illicit attempts to exploit or alter their functionalities for unlawful ends.

¹² Kowalczevska, 2021a, pp. 465–486.

¹³ Stix, 2021, p. 15.

¹⁴ Puscas, 2022.

Adherence to established regulatory frameworks governing data protection and privacy rights is of paramount importance in the realm of privacy and data governance. Therefore, AI systems must adhere rigorously to stipulated norms, ensuring data processing of impeccable quality and integrity, thereby safeguarding privacy rights and preserving data sanctity.¹⁵

Transparency, as a guiding principle, requires the elucidation of AI systems' inner workings, affording stakeholders insights into the dynamics of human–AI interactions. This entails furnishing users with comprehensive information regarding the operational modalities, capabilities, and limitations of AI systems, thereby fostering informed decision-making and engendering a culture of accountability.¹⁶

Additionally, the principles of diversity, non-discrimination, and fairness mandate the equitable treatment of individuals irrespective of their demographic attributes. Artificial intelligence systems are enjoined to promote inclusivity, gender equality, and cultural diversity while eschewing discriminatory practices or biases that contravene established legal standards.

Moreover, the ethical imperative of societal and environmental well-being necessitates the sustainable development and deployment of AI technologies. It is imperative that AI innovations not only serve to ameliorate human welfare but also mitigate adverse environmental impacts, thereby ensuring the perpetuation of societal equilibrium and ecological harmony.¹⁷

Finally, the principle of accountability mandates that AI systems be subject to stringent mechanisms of oversight and redress. This entails delineating clear lines of responsibility and establishing robust frameworks for recourse in the event of malfeasance or adverse outcomes attributable to AI operations.¹⁸

This ethical meta-framework largely aligns with other soft-law instruments developed in various AI-oriented forums. As demonstrated later, the framework was applied extensively in the AIA but also found significant resonance in discussions concerning LAWS.

¹⁵ Michel, 2021.

¹⁶ Michel, 2020.

¹⁷ United Nations Institute for Disarmament Research, 2015.

¹⁸ Anand and Deng, 2023.

2.2 Risk-based approach

An integral aspect of the AIA is the delineation of AI-based systems. As articulated in Art. 3(1) of AIA, these systems are characterised as:

...machine-based systems designed to operate with varying levels of autonomy, capable of exhibiting adaptability upon deployment, and with the capacity to infer from inputs received how to generate outputs such as predictions, content, recommendations, or decisions that may impact the physical or virtual environment.

Given the expansive scope of applications encompassed by the AIA, this definition involves a broad scope and has, consequently, been subject to criticism.¹⁹ However, it underscores a crucial attribute of AI systems (similar to the definition-related discussion regarding LAWS)—namely, their capacity for inference-making, along with varying degrees of autonomy from human intervention and the potential to execute actions without direct human involvement. Naturally, such autonomous action entails inherent risks, which are addressed in the provisions of the AIA.

In developing the AIA, a risk-based approach was adopted,²⁰ wherein AI systems were categorised into four distinct levels based on the risks they pose to fundamental rights: unacceptable, high, limited, and minimal (or no) risk. The AIA assigns specific obligations to providers and users based on the level of risk associated with the AI system. Of particular significance for this article are the first two categories, which delineate prohibited uses of AI and those necessitating human oversight.

2.2.1 Unacceptable risks and prohibitions of certain artificial intelligence systems

Art. 5 of the AIA prohibits placing AI systems on the market, putting them into service, or using them in several specific scenarios. These scenarios include the employment of manipulative or deceptive techniques, exploitation of vulnerabilities, implementation of social scoring systems for natural persons, deployment of biometric categorisation systems, and real-

¹⁹ Ruschemeier, 2023, pp. 361–376.

²⁰ Key Issue 3: Risk-Based Approach - EU AI Act, n.d.

time remote biometric identification of individuals in publicly accessible spaces for law enforcement purposes.

The AI systems categorised under this prohibition are considered harmful to individuals and are, therefore, completely barred from use within the EU space, with only limited exceptions for specific law enforcement purposes. The prohibited applications primarily involve scenarios in which continuous surveillance could lead to discrimination, substantial violations of privacy and freedom of movement, or other significant harms. Although why these specific systems are deemed contrary to democratic values is not elaborated, this decision is based on certain principles and falls within the realm of the political discretion vested in lawmakers. Similarly, the international community anticipates analogous decisions within discussions on LAWS, wherein states should interpret the fundamental principles of IHL and decide on the extent of the LAWS regulation.

2.2.2 High-risk and human oversight

The high-risk category of AI systems, as defined in Art. 6 of the AIA and further detailed in Annex III, requires AI systems to meet two conditions to qualify for classification within this group. First, the AI system must be subjected to the EU harmonisation legislation outlined in Annex I. Second, the system must undergo a third-party conformity assessment according to the same legislation.

The broad definition of high-risk AI applications encompasses a spectrum of schemes perceived as risky owing to their potential to cause significant harm across multiple domains, including health, safety, fundamental rights, the environment, democracy, and the rule of law. Examples of high-risk AI applications can be found in various sectors, such as critical infrastructure; education; employment; essential private and public services like healthcare and banking; certain law enforcement systems; migration and border management; and justice and democratic issues like election integrity. These examples highlight the diverse contexts in which high-risk AI implementations may pose substantial threats, thus warranting heightened scrutiny and regulation under the AIA.

Under this regulation, such systems are permitted on the market but are subject to a comprehensive set of conditions aimed at the provision of trustworthy AI. These include the implementation of a robust risk-management system (Art. 9), adherence to stringent data management and

governance practices (Art. 10), the maintenance of thorough technical documentation (Art. 11), and the establishment of comprehensive record-keeping protocols (Art. 12). Furthermore, transparency and informed instructions for use must be provided (Art. 13), and effective human oversight must be ensured throughout the system's lifecycle (Art. 14). Additionally, AI systems should maintain an appropriate level of accuracy, robustness, and cybersecurity (Art. 15). The affected individuals are entitled to obtain clear and meaningful explanations from the deployer regarding the AI system's role in decision-making processes and the key elements of the decisions made (Art. 86). This last provision also reflects a commitment to transparency and explainability for AI-based processes.

Within the high-risk category of AI systems, significant emphasis is placed on human oversight.²¹ The AIA mandates human oversight through three key pillars: the provision of appropriate human-machine interface tools; the objective of preventing or minimising risks; and the introduction of oversight measures tailored to the risks, autonomy level, and use context of the high-risk AI system. These measures can be integrated by the provider or implemented by the deployer. Through these pillars, the individual responsible for executing human oversight is expected to possess the capacity to understand the relevant capabilities of the AI system and effectively monitor its operation to detect and address any anomalies. They should maintain the awareness of automation bias and interpret outputs generated by the AI system appropriately. Additionally, they must be able to exercise the authority required to withdraw or override decisions made by the AI system and halt the operation of the AI system by pressing a stop button under safe conditions.

However, criticism has been raised regarding the AIA's approach to human oversight, suggesting that it focuses on procedural guidelines for AI system providers and lacks substantive guidance on the effectiveness of this oversight.²² Additionally, concerns have been voiced about the considerable freedom granted to AI system providers, particularly regarding the circumstances triggering oversight.²³ It is argued that a decision of such significance, embodying the essence of human oversight, should, at the very least, be accompanied by a set of guidelines formulated by lawmakers dedicated to safeguarding fundamental rights.

²¹ Key Issue 4: Human Oversight - EU AI Act, n.d.

²² Laux, 2023.

²³ Enqvist, 2023, p. 534–535.

Nevertheless, this human oversight framework serves as a solid starting point that can be enhanced by targeted regulation, best practices, and technical designs developed within the respective fields of AI system deployment. When examining the debate surrounding LAWS, a similar challenge arises in regulating human oversight in a qualitative manner without being overly restrictive or narrow. Moreover, the approaches differ slightly. In the military setting, there is a greater emphasis on user oversight, particularly by military commanders rather than providers. While awaiting more detailed guidance, it is important to acknowledge that the regulation of human oversight in the AIA represents a commendable yet preliminary step in establishing a legal framework for trustworthy AI.

2.3 *Exclusion of military purposes*

Any secondary law adopted in the EU, such as a regulation like the AIA, must be based on primary law. Primary law is where member states determine the allocation of competences among EU institutions and retain certain areas as sovereign competences. National security matters, including defence, are among those areas that member states have chosen to retain as their sole responsibility under Art. 4(2) and Chapter 2 of Title V of the Treaty on European Union

Given the primary objectives of the EU's existence, matters pertaining to world peace and security have traditionally fallen within the realm of public international law rather than EU law. This is underscored in the preamble to the AIA, which acknowledges that 'public international law is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities'. Consequently, the EU consistently excludes applications related to national security and warfare from the scope of its laws.²⁴ The provisions of the AIA are consistent with this approach.

According to Art. 2(3) of the AIA, the regulation explicitly excludes national security matters from its scope, irrespective of whether these tasks are carried out by public or private entities. Notably, it specifies that the AIA does not apply to AI systems when they are marketed, used, or exploited solely for military, defence, or national security purposes or when their outputs are utilised exclusively for such purposes within the EU, even if the systems themselves do not operate within its territory.

²⁴ Compare Recital 16 of the General Data Protection Regulation.

This somewhat cryptic formulation can be elucidated by considering the interpretation provided in the context of Recital 24 of the preamble. It clarifies that if the primary purpose of placing or using an AI system is for a military, defence, or national security application, then it falls outside the scope of the AIA. However, if such a system is subsequently used outside its military purpose temporarily or permanently, such as for civilian, humanitarian, or law enforcement purposes, it falls back within the scope of the AIA. The same rule applies to AI systems designed for mixed purposes (both military and civilian), wherein only the civilian-purpose use falls under the scope of the AIA.

Under this convoluted regulation, the AIA is not applicable when an AI system is intended for military purposes or is used by any entity for military purposes. It appears that the drafters of the AIA considered the dual-use nature of AI systems but also framed the exceptions in the use-case language (rather than technology-type language) that is used consistently throughout the AIA. They adopted this approach to exclude military actors engaged in military operations while including civilian uses of AI systems originally conceived for military purposes.

Nevertheless, I contend that the exclusion of AI systems developed for military purposes is not based primarily on the distinct ethical underpinnings of such military-oriented AI systems but is based on the formal issue of the competence division between EU institutions and member states. This is reflected in the normative referral of this issue from the realm of EU law to public international law. Indeed, discussions about military AI systems are ongoing in forums like the CCW, in which individual member states and the EU, with its competence as an observer, are actively participating. Furthermore, they present positions that are in line not only with IHL but also with the ethical principles expressed in the AIA.

3. Discussions about lethal autonomous weapon systems in the Convention on Certain Conventional Weapons forum

Discussions within the CCW, initiated by coalitions of non-governmental organisations such as Stop Killer Robots, have continued for over a decade. Despite the adoption of various formats, including informal expert meetings and gatherings of government experts, these deliberations have yet to progress towards a negotiation of a legally binding international instrument. While civil society holds expectations of such progress, particularly

concerning LAWS operating without meaningful human control and potentially creating an accountability gap,²⁵ the likelihood of achieving this goal has been minimal from the outset. Furthermore, the prevailing international security landscape further diminishes the possibility of such a solution in the foreseeable future.²⁶ However, these discussions have seen some progress, and I contend that officially embracing the positions outlined below would be perceived by Stop Killer Robots and the states supporting this position as a triumph and, fundamentally, a recognition of their demands.

While there is no universally accepted single definition of LAWS, states generally concur in principle that LAWS encompass weapon systems that, once activated, can identify, select, and engage targets with lethal force without further intervention by an operator.²⁷ By translating this definition into the language of the AIA, it can be inferred that LAWS are AI systems intended for military purposes that exhibit adaptability post-deployment. These systems are capable of inferring, from received inputs, how to generate outputs such as decisions regarding the identification and selection of military targets, which may influence the physical environment through engagement with military targets (including people or objects), potentially resulting in serious incidents. Although current discussions are considered to pertain to lethal AI applications, a detailed analysis reveals that some positions are broader, encompassing decision-support systems and other autonomous or remotely piloted means of warfare that do not pose risks similar to those posed by LAWS.²⁸ To narrow the scope of this discussion and focus on the most critical applications (i.e. those with lethal consequences), the discussion will concentrate on issues related to LAWS.

There is a widespread consensus that all developed and employed means of warfare must adhere to IHL.²⁹ This means that as a state's right to develop and deploy weapons is limited, the weapons must be utilised in compliance with the fundamental principles of IHL, including distinction, proportionality, precautions, and the prohibition against causing unnecessary suffering or superfluous injury.³⁰ However, I argue that this

²⁵ Human Rights Watch, 2012; Human Rights Watch, 2015.

²⁶ Puscas, 2023.

²⁷ CCW, 2023a.

²⁸ Bo and Dorsey, 2024.

²⁹ CCW, 2019.

³⁰ Kowalczevska, 2021b, pp. 88–103.

assertion may not be adequate to comprehensively regulate LAWS. I contend that the intrinsic nature of AI-based decision-making on matters of life and death, without clear human accountability, warrants examination by lawmakers to determine its acceptability, particularly in light of established customs, principles of humanity, and the mandates of public conscience (Martens clause).³¹ This requires states to declare their stance on the acceptable level of risk to fundamental rights, especially the right to life, within the context of armed conflict. Consequently, they should adopt a risk-based approach, akin to that outlined in the AIA, by explicitly prohibiting certain uses of LAWS and regulating high-risk LAWS more tightly with a set of mitigating measures. This perspective is increasingly evident in statements presented at the CCW. In the sections below, I will focus on two propositions recently put forth by several EU member states to highlight convergent points and demonstrate the gradual emergence of this approach in discussions.

3.1. The two-tier approach

The so-called “two-tier approach” was proposed in July 2022 by a group of European states, comprising Finland, France, Germany, the Netherlands, Norway, Spain, and Sweden.³² The states proposed a possible structure of recommendations for measures related to a normative and operational framework.

3.1.1. Unacceptable risks

The core concept underlying this approach posits that ‘autonomous weapons systems that cannot comply with IHL are effectively prohibited and should neither be developed nor used, necessitating further efforts to implement this commitment at the national level’. This seemingly straightforward and legally obvious assertion is elaborated upon in a more nuanced manner, providing insight into which types of AI systems, according to a two-tier approach, are deemed unacceptable and warrant regulation. The former category comprises LAWS that operate entirely beyond human control or a responsible chain of command; the latter pertains to all other types of LAWS. From the delineation of these LAWS categories, one can infer that, according to these states, LAWS lacking both a responsible chain of

³¹ Ibid., p. 228.

³² CCW, 2022.

command and appropriate human control inherently contravene IHL and should be de jure prohibited.

This statement can be contrasted with the AIA's classification of unacceptable risks, but there is a significant difference: LAWS, as AI systems under scrutiny, are normatively embedded within the IHL framework, which offers some direction on their acceptability. By contrast, civilian applications are governed according to human rights standards. Weapons law and IHL embody legal frameworks that are more robust than the civilian regulation of AI as they focus on specific military actions such as targeting. Thus, regulations are stricter for states deploying such systems in combat than in the broader and less-explored commercial settings. States can discern which systems pose unacceptable risks within established normative frameworks. In civilian AI, per the AIA, these systems generate risks incongruent with rights to privacy, human dignity, and protection from discriminatory practices. In the military sphere, attention is drawn to risks that would lead to an accountability gap. This disparity in approach reflects the distinct ethical foundations of both frameworks, which prioritise different values during peace and war.

3.1.2. Human oversight

Another aspect of the two-tier approach is its emphasis on human oversight, akin to the AIA. For LAWS other than those classified as unacceptable, this oversight entails appropriate human control and a responsible chain of command.³³ The author states define appropriate human control as encompassing human oversight over the entire lifecycle of LAWS, including the development, deployment, and utilisation phases. This oversight should ensure that LAWS operate predictably, enabling humans to ascertain their compliance with legal, political, and operational standards and ensuring the explainability of their operations. During the development stage, human control should involve the testing, certification, and legal review of LAWS to evaluate their reliability and predictability. During the deployment phase, human control should manifest in the establishment of rules of engagement and a delineation of the mission objectives, target types, and spatial and temporal constraints while monitoring the system's reliability and usability within this context. Finally, during utilisation, humans should retain decision-making authority over the use of force,

³³ For a critical approach to this framework, see Article 36, 2023.

which encompasses a scope broader than a mere attack. It includes the ability to approve any significant changes in mission objectives, maintain communication links, and deactivate the system, although the technical feasibility of the latter action is deemed optional by the author states.

The second condition entails maintaining human responsibility and state accountability throughout the lifecycle. This aligns with the ethical imperative wherein a human should always be held responsible for the actions of machines, thus heeding the call to address the accountability gap. This condition is considered satisfied through the implementation of several measures, including the development of LAWS-specific doctrines and procedures and the provision of adequate training on LAWS for human decision-makers and operators. It also entails ensuring that the responsible chain of human command encompasses human accountability for the creation and validation of rules of operation, use, and engagement as well as decision-making regarding deployment. This approach implies the introduction of after-action review measures. It also advocates for maintaining the accountability framework, which involves reporting, investigation, prosecution, and disciplinary procedures in cases of grave breaches of IHL due to the use of LAWS.

3.2. Draft articles

A more robust approach, known as the “Draft Articles on Autonomous Weapons”, was introduced in May 2023 by a coalition of states, including EU member state Poland, along with Australia, Canada, Japan, the Republic of Korea, the United Kingdom, and the United States.³⁴ This approach outlines autonomous systems in Art. 1 that should not be developed owing to their conflict with IHL principles. The subsequent articles focus on detailed regulatory measures to ensure the effective implementation of fundamental IHL principles: Art. 3 emphasises distinction, Art. 4 addresses proportionality, and Art. 5 highlights precautions. The final article, Art. 6, pertains to the accountability regime. To maintain consistency in the analysis, the presentation of the draft articles will follow the previous logic of a risk-based approach and human oversight indicators.

³⁴ CCW, 2023b.

3.2.1. Unacceptable risks

The proposing states assert that certain AI systems, by virtue of their design, pose unacceptable risks and are, therefore, incompatible with IHL. These systems include those that cause harm to civilians and civilian objects by targeting them, spreading terror, or consistently leading to disproportionate collateral damage. The articulation within the draft articles unequivocally establishes that only LAWS deliberately designed to contravene IHL principles are deemed unlawful. This assertion, while legally evident and akin to the two-tier approach, also reflects a pragmatic understanding of the nature of weapons and the regulatory framework governing armed conflict. It acknowledges the inherent purpose of weapons to cause harm while emphasising that only attacks on civilians and civilian objects that are intentional and disproportionate can be classified as war crimes. Consequently, states involved in deliberations regarding the acceptability of LAWS operate under the premise that AI-based weapon systems possess the capability to make critical life-and-death decisions. However, they converge with Stop Killer Robots on the second condition, concerning human responsibility.

The draft articles explicitly specify that LAWS operating outside the responsibility framework of commanders or their operators are considered unacceptable under this proposal. This stance aligns with the two-tier approach by prohibiting LAWS that would operate without human responsibility attached to their actions or those designed in contravention of IHL principles, as outlined in Annex I.

Therefore, it appears that states supporting the two-tier approach and draft articles generally align with the main argument of Stop Killer Robots. However, they differ in their willingness to be legally bound by this standard.

3.2.2. Human oversight

States supporting the draft articles contend that all other LAWS categories should be designed to foresee and manage their effects during attacks according to the principles of distinction and proportionality. In pursuit of this objective, they delineate various sets of risk-mitigating measures aimed at upholding fundamental IHL principles and establishing an effective accountability framework. During development, these measures should

include testing, evaluation, and legal review, along with limit-setting regarding target types, duration, geographical scope, and scale (e.g. self-destruct, self-deactivation, or self-neutralisation mechanisms), as well as addressing automation and unintended bias. Furthermore, the draft articles, offering a more detailed framework than the two-tier approach, underscore the significance of certain principles. These include the reliance on LAWS in good faith, taking into account the information available at the time of the use of force and exercising due diligence in adhering to IHL principles, as elucidated in Articles 3–5.

The draft articles establish an accountability framework within the broader context of implementing IHL and additional LAWS-specific measures. The former encompasses measures such as education and training on IHL, a responsible chain of human command and control, the development of domestic legislation, international reporting mechanisms, and appropriate investigations, which may entail accountability for personnel. The latter involves easily understandable human–machine interfaces and controls, guidance and training for personnel on the appropriate use of LAWS, and specific rules of engagement and other military documentation relevant to military operations.

Hence, the draft articles emphasise that LAWS should conform to the overarching IHL framework, encompassing all conventional rules. Moreover, they delineate specific measures targeted at ensuring the effective implementation of these norms, particularly in light of the unique characteristics of AI systems.

4. Conclusion

In this article, I aimed to demonstrate the emerging normative consensus on the need for human oversight and risk-based approaches for AI regulation. As examples, I used the AIA, covering a broad group of general-purpose AI systems, and discussions on military applications of AI in the form of LAWS. Although the examples involved different regimes of factual situations (i.e. peacetime and wartime), I attempted to show that a limited ethical anchorage could be commonly found across EU member states (as well as other states).

Utilising a risk-based methodology facilitates the identification of AI systems whose operations contravene core legal norms, such as those governing democracy, human rights, or IHL, thereby warranting their

prohibition. Conversely, for AI systems categorised under lower risk levels, tailored regulatory measures can be instituted to mitigate societal exposure to their potentially adverse ramifications. Within these deliberations, ethical principles such as human agency; technical robustness; and reliability, predictability, transparency, explainability, and human accountability have assumed central importance, resonating across discussions concerning the AIA and LAWS. These ethical precepts constitute integral components of a broader normative framework that remains indispensable in the AI discourse. The imperative now is to meticulously situate these principles within the specific operational context and milieu of the pertinent use case.

Furthermore, the discussion highlighted the imperative to ensure human oversight, particularly in instances where risks are deemed acceptable but are elevated. This underscores a reluctance to entrust decision-making to AI systems in contexts of ethical significance, such as in critical services, judicial proceedings, and the employment of force. The operationalisation of such oversight ought to be predicated upon a cohesive comprehension of procedural imperatives (what actions to undertake and when) and qualitative mandates (the rationale behind actions), which should be delineated not solely by ethical precepts but also be enshrined within legal regulatory frameworks.

Finally, the most notable disparity between the two cases concerns regulation. While the AIA serves as a directive targeting economic entities, mandating compliance for profit generation within the EU, its adoption is relatively straightforward compared with the negotiation and implementation of a multilateral arms treaty. Nonetheless, I posit that, if EU member states are committed to upholding the normative values that are fundamental to the EU, they should actively articulate, in a legally binding manner, the unacceptable risks posed by AI in armed conflict, thereby affirming their adherence to fundamental ethical principles such as human dignity. However, the current geopolitical landscape, underscored by Russia's aggression against Ukraine in 2022, has engendered reluctance among states to embrace new arms control commitments, and some have even contemplated withdrawing from existing commitments. Consequently, while the calls from Stop Killer Robots for a ban on such weapons may be unavailing at present, it is hoped that the positions articulated in the two-tier approach and draft articles will suffice to prevent the development, deployment, or utilisation of the most hazardous AI systems—those endowed with full unsupervised autonomy and lethal capabilities.

Bibliography

- [1] Anand, A., Deng H. (2023) *Towards Responsible AI in Defence: A Mapping and Comparative Analysis of AI Principles Adopted by States*. [Online]. Available at <https://unidir.org/publication/towards-responsible-ai-in-defence-a-mapping-and-comparative-analysis-of-ai-principles-adopted-by-states/> (Accessed: 1 July 2024).
- [2] Bo, M., Dorsey, J. (2024) *Symposium on Military AI and the Law of Armed Conflict: The 'Need' for Speed – The Cost of Unregulated AI-Decision Support Systems to Civilians*. *Opinio Juris*. [Online]. Available at: <https://opiniojuris.org/2024/04/04/symposium-on-military-ai-and-the-law-of-armed-conflict-the-need-for-speed-the-cost-of-unregulated-ai-decision-support-systems-to-civilians/> (Accessed: 10 April 2024).
- [3] Bode, I. (2024) The problem of algorithmic bias and military applications of AI. *Humanitarian Law & Policy Blog*. [Online]. Available at: <https://blogs.icrc.org/law-and-policy/2024/03/14/falling-under-the-radar-the-problem-of-algorithmic-bias-and-military-applications-of-ai/> (Accessed: 29 March 2024).
- [4] Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, H., Herrera, F. (2023) 'Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation' *Information Fusion* 99, p. 101896; <https://doi.org/10.1016/j.inffus.2023.101896>.
- [5] Enqvist, L. (2023) 'Human oversight' in the EU artificial intelligence act: what, when and by whom?' *Law, Innovation and Technology* 15(2), pp. 508–535; <https://doi.org/10.1080/17579961.2023.2245683>.

-
- [6] Kowalczevska, K. (2021a) *Unia Europejska wobec autonomicznych systemów śmiertelnych broni (LAWS) – znacząca ludzka kontrola jako fundament wiarygodnej sztucznej inteligencji* in Fischer, B., Pązik, A., Świerczyński, M. (eds.) *Prawo sztucznej inteligencji i nowych technologii*, Wolters Kluwer Polska, pp. 465–486.
- [7] Kowalczevska, K. (2021b) *Sztuczna inteligencja na wojnie. Perspektywa MPHKS. Przypadek autonomicznych systemów śmiertelnych broni*. Wydawnictwo Naukowe Scholar.
- [8] Laux, J. (2023) ‘Institutionalised distrust and human oversight of artificial intelligence: towards a democratic design of AI governance under the European Union AI Act’, *AI & SOCIETY*; <https://doi.org/10.2139/ssrn.4377481>.
- [9] Michel, A. (2020) *The Black Box, Unlocked: Predictability and Understandability in Military AI*. [Online]. Available at: <https://unidir.org/publication/the-black-box-unlocked/> (Accessed: 1 July 2024).
- [10] Michel, A. (2021) *Known Unknowns: Data Issues and Military Autonomous Systems*. United Nations Institute for Disarmament Research. [Online]. Available at: <https://unidir.org/publication/known-unknowns> (Accessed: 1 July 2024).
- [11] Puscas, I. (2022) *Human-Machine Interfaces in Autonomous Weapon Systems*. [Online]. Available at: <https://unidir.org/publication/human-machine-interfaces-in-autonomous-weapon-systems/> (Accessed: 1 July 2024).
- [12] Puscas, I. (2023) *AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures*. [Online]. Available at: <https://unidir.org/publication/ai-and-international-security-understanding-the-risks-and-paving-the-path-for-confidence-building-measures/> (Accessed: 1 July 2024).

-
- [13] Ramos, G., Squicciarini, M., Lamm, E. (2024) ‘Making AI Ethical by Design: The UNESCO Perspective’, *Computer*, 57(2), pp. 33–43; <https://doi.org/10.1109/MC.2023.3325949>.
- [14] Ruschemeier, H. (2023) ‘AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal’, *ERA Forum*, 23(3), pp. 361–376; <https://doi.org/10.1007/s12027-022-00725-6>.
- [15] Stix, Ch. (2021) ‘Actionable Principles for Artificial Intelligence Policy: Three Pathways’, *Science and Engineering Ethics* 27(1), p. 15; <https://doi.org/10.1007/s11948-020-00277-3>.
- [16] Wouters, J. (2020) *From an economic community to a union of values: The emergence of the EU’s commitment to human rights*. in Wouters, J. et al. *The European Union and Human Rights*. Oxford University Press. pp. 11–38. <https://doi.org/10.1093/oso/9780198814191.003.0002>.
- [17] Załucki, M., Miraut, M. (2021). *Artificial intelligence and human rights*. Dykinson.
- [18] Article 36. (2023) *Completely outside human control?* [Online]. Available at: <https://article36.org/wp-content/uploads/2023/03/Completely-outside-human-control.pdf> (Accessed: 29 March 2024).
- [19] CCW (2022) *Working paper submitted by Finland, France, Germany, the Netherlands, Norway, Spain, and Sweden to the 2022 Chair of the Group of Governmental Experts (GGE) on emerging technologies in the area of lethal autonomous weapons systems (LAWS)*. [Online]. Available at: https://documents.unoda.org/wp-content/uploads/2022/07/WP-LAWS_DE-ES-FI-FR-NL-NO-SE.pdf (Accessed: 1 July 2024).

- [20] CCW (2023a) *Draft articles on autonomous weapon systems – prohibitions and other regulatory measures on the basis of international humanitarian law (“IHL”)*. [Online]. Available at: [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2023\)/CCW_GGE1_2023_WP.4_US_Rev2.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_WP.4_US_Rev2.pdf) (Accessed: 1 July 2024).
- [21] CCW (2023b) *Non-exhaustive compilation of definitions and characterizations*. [Online]. Available at: [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2023\)/CCW_GGE1_2023_CRP.1_0.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf) (Accessed: 1 July 2024).
- [22] Convention for the Protection of Human Rights and Fundamental Freedoms (1950).
- [23] Charter of Fundamental Rights of the European Union (2000).
- [24] European Parliament (2024) *Artificial Intelligence Act. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts*. [Online]. Available at: [https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2024/03-13/0138/P9_TA\(2024\)0138_EN.pdf](https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2024/03-13/0138/P9_TA(2024)0138_EN.pdf) (Accessed: 29 March 2024).
- [25] Human Rights Watch. (2012) *Losing humanity: the case against killer robots*. Amsterdam Berlin: Human Rights Watch. [Online]. Available at: https://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf (Accessed: 29 March 2024).

-
- [26] Human Rights Watch. (2015) *Mind the Gap: The Lack of Accountability for Killer Robots*. [Online]. Available at: https://www.hrw.org/sites/default/files/reports/arms0415_ForUpload_0.pdf (Accessed: 1 July 2024).
- [27] OECD (n.d.) *AI-Principles Overview*. [Online]. Available at: <https://oecd.ai/en/ai-principles> (Accessed: 1 July 2024).
- [28] REAIM (2023) *REAIM 2023 Call to Action*. [Online]. Available at: <https://www.government.nl/documents/publications/2023/02/16/ream-2023-call-to-action> (Accessed: 1 July 2024).
- [29] UNESCO (n.d.) *Ethics of Artificial Intelligence*. [Online]. Available at: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics> (Accessed: 28 August 2023).
- [30] UNIDIR (2015) *The Weaponization of Increasingly Autonomous Technologies: Considering Ethics and Social Values*. [Online]. Available at: <https://unidir.org/publication/the-weaponization-of-increasingly-autonomous-technologies-considering-ethics-and-social-values/> (Accessed: 1 July 2024).
- [31] UNSG. (2023) *Secretary-General's remarks to the Security Council on Artificial Intelligence*. [Online]. Available at: <https://www.un.org/sg/en/content/sg/speeches/2023-07-18/secretary-generals-remarks-the-security-council-artificial-intelligence>. (Accessed 1 July 2024).
- [32] (n.d.) *Key Issue 3: Risk-Based Approach - EU AI Act*. [Online]. Available at: <https://www.euaiact.com/key-issue/3> (Accessed: 29 March 2024).
- [33] (n.d.) *Key Issue 4: Human Oversight - EU AI Act*. [Online]. Available at: <https://www.euaiact.com/key-issue/4> (Accessed: 29 March 2024).

KATARZYNA MALINOWSKA**

Space defence legal regime in the service of sustainable development**

ABSTRACT This article examines the challenges and opportunities of military space activities in the context of the sustainable development of space exploration. It investigates the legal frameworks governing military use, focusing on the need for regulations to address risks such as space debris caused by anti-satellite testing, as well as space governance issues. It analyses the role of international, regional (EU), and national laws and policies in achieving a sustainable and responsible exploration of outer space. The role of international and regional bodies such as the UN and EU in achieving sustainability goals is analysed in terms of the synergy between civil and military uses of space.

KEYWORDS: space militarisation, space law, sustainability, responsible behaviour, EU space law, space defence strategy.

1. Introduction

An increasing number of nations are incorporating space into their defence strategies, as evidenced by the intensifying deployment of military satellites. By the term “military use of space”, the author means its use for purposes permitted by international law (i.e. security and defence purposes), excluding the offensive use of space. However, among space’s military purposes, this study analyses aspects of space use that, although not explicitly prohibited by international law, raise numerous ethical and legal questions, such as those concerning anti-satellite (ASAT) tests.

As military space operations escalate, so do the accompanying challenges. Chief among these is navigating the application of space laws to

** University Professor, Director of the Centre for Space Studies, Leon Kozminski University, Poland. katarynamalinowska@kozminski.edu.pl.

This article came about within the framework of Academic Excellence Hub – Digital Justice Center carried out under Initiative of Excellence – Research University at the University of Wrocław.

** The research and preparation of this study was supported by the Central European Academy.

governmental military activities and, by extension, adhering to sustainability principles outlined in international agreements and domestic space regulations. Key concerns include conducting ASAT tests and properly registering military space assets.¹ The intersection of military operations in outer space with sustainability concerns presents a multifaceted dynamic that merits careful examination. While initially appearing akin to civilian applications, the military's involvement introduces unique considerations. Depending on the perspective adopted, the escalating military utilisation of outer space may be construed as either a formidable challenge or an opportunity to bolster sustainability within the space domain.

The challenges concern the application of space regulations and standards. Although commercial operators are subject to routine adherence to established rules, the regulatory landscape governing military space activities is more obscure. Interpretations of regulations often hinge on the specific requirements and priorities of spacefaring nations, leading to ambiguity in their application.² Thus, the goal of sustainability may face mounting obstacles. Specifically, a growing challenge is presented by regulatory frameworks, prompting questions regarding the integration of military elements into space law and their alignment with established principles. Furthermore, rapid advances in military and defence applications for space exploration raise governance concerns at the international, national, and (for Europe) regional levels, including within the EU framework.

Sustainability has recently emerged as a pivotal principle guiding space strategies, laws, and legal endeavours. This principle finds expression at various levels, including in the UN, the EU, and national space strategies and legislation enacted in recent years. The concept of sustainable development in outer space extends to both civilian and military applications, although current legal frameworks emphasise requirements for commercial operators. Whereas this alignment with civilian laws seems intuitive, uncertainties arise concerning the military utilisation of outer space, which is often excluded from conventional licensing regimes, leading to questionable adherence to technical standards aimed at mitigating space debris and ensuring overall sustainability in space exploration. Consequently, international space law exhibits significant gaps concerning

¹ Jakhu et al., 2018.

² For example, the notion of the peaceful exploration of outer space and military purposes. See Lyall and Larsen, 2018.

military activities in space, particularly from the sustainability perspective. One such gap pertains to the application of sustainability principles to both civil and military space exploration. To address that gap, sustainability has been introduced into soft law measures, such as the UN Guidelines for long-term sustainability, indicating the need for a careful consideration of its application to military space activities.

The proliferation of space activities in the context of defence and security entails the institutionalisation of activities and the separation of responsibilities between bodies that govern military and commercial space matters. This proliferation, especially at the national level, may affect how norms of responsible behaviour are applied.

The doubts and gaps described above raise several fundamental questions. What is the roadmap for applying sustainability postulates to the military use of space, and how can these postulates be made enforceable? How can the challenges of making military activities sustainable be turned into an opportunity leading to enhanced peace and security?

This issue has several important dimensions. This article focuses on three. First, it discusses ASAT tests, their permissibility, and the efforts made to stop them at the international and European levels. Second, it discusses the regime for space activity licensing and its inclusion of military space activities, focusing on the international and national levels of space law. Finally, the article discusses the governance of military space activities and the role of space agencies. The analysis investigates international and national “hard laws”, as well as acts of political will in areas not covered by binding laws. International initiatives are also considered, with their potential to shape international standards, good practices, and binding custom (as a source of international law).³

2. Sustainability defined and why it concerns military space activities

It is essential to examine the concept of sustainability within the current legal framework to determine its potential applicability to military space endeavours. If it is deemed applicable, the next step is to ascertain how this objective can be enforced effectively.

Sustainability is a mature concept, though not yet embedded in all sectors of industry. It was used initially in relation to environmental issues, but its scope has always been much broader. It was popularised by the 1987

³ Art. 138 of the statute of the ICJ.

Brundtland Report, “Our Common Future”, and the 1992 UN Conference on Environment and Development (the “Earth Summit”). The Brundtland Report asserted the need for the integration of economic development, environmental protection, and social justice and inclusion.⁴

The report described sustainable development as the pursuit of development that fulfils the requirements of the current generation while safeguarding the capacity of future generations to satisfy their own needs. It encompassed two fundamental concepts: the notion of “needs”, prioritising the basic needs of the impoverished global population; and a recognition of the constraints imposed by technological advancements and societal structures on the environment’s capacity to meet both current and future needs. A comparable concept has been embraced by the EU, as outlined in the Strategy for Sustainable Development: Sustainable development means that the needs of the present generation should be met without compromising the ability of future generations to meet their own needs. [...] It is about safeguarding the earth’s capacity to support life in all its diversity and is based on the principles of democracy, gender equality, solidarity, the rule of law and respect for fundamental rights, including freedom and equal opportunities for all. It aims at the continuous improvement of the quality of life and well-being on Earth for present and future generations.⁵

The common principles of sustainable development have been recognised as inherently related to environmental limits and comprised of integrated decision making (policy and legislation working complementarily); good governance that is democratic, transparent, inclusive, participatory, and accountable; and the responsible use of robust and credible scientific evidence in decision-making. Of particular interest is the concept of boundaries, which represent global Earth systems and processes within which there is a safe living space for humans and wildlife. It is argued that overstepping one or more of these boundaries could create a tipping point by which the global Earth system would shift to a permanently less-hospitable state. There are nine recognised thresholds, but none relates

⁴ The Earth Summit was followed by such revolutionary documents as the Rio Declaration. It contained 27 principles of sustainable development, including the precautionary and polluter pays principles, Forest Principles, the Convention on Biological Diversity, and the Framework Convention on Climate Change, as well as Agenda 21, which was a voluntary SD plan of action for implementation by national, regional, and local governments; Pisani, 2006; Bohlmann and Petrovici, 2019.

⁵ The Renewed EU Sustainable Development Strategy as adopted by the European Council on 15/16 June 2006, Brussels, 26 June 2006, 10917/06.

directly to space.⁶ It was therefore considered necessary to design an architecture of sustainability that would respond to the specificities of space exploration.

The notion of sustainable development for the space domain aims to provide a response to the burgeoning growth of the space sector. Consequently, it should encompass both the civilian and military utilisation of outer space. The primary assertion made during the Stockholm Conference in 1972, albeit focusing on Earth's environment, is relevant for the repercussions of the human exploitation of Earth's orbits:

A point has been reached in history when we must shape our actions throughout the World with a more prudent care for their environmental consequences. Through ignorance or indifference, we can do massive and irreversible harm to the earthly environment on which our life and well-being depend. Conversely, through fuller knowledge and wiser action, we can achieve for ourselves and our posterity a better life in an environment more in keeping with human needs and hopes. To defend and improve the human environment for present and future generations has become an imperative goal for mankind.⁷

The first works on the sustainability concept applied the outer space exploration were undertaken a few years ago, along with active debris removal initiatives.⁸ Though their ideas are unstructured, space stakeholders have started considering how to stop and reverse the exploitation of outer space without due regard to future generations. An analysis of the attempts to regulate this issue in the space sector reveals numerous documents that focus on space debris. The concept of the sustainable use of outer space can be found in the Outer Space Treaty⁹: art. I establishes outer space as a province of mankind; art. III imposes an obligation to act in accordance with

⁶ These are as follows: climate change, change in biosphere integrity (biodiversity loss and species extinction), stratospheric ozone depletion, ocean acidification, biogeochemical flows, land-system change (e.g. deforestation), freshwater use, atmospheric aerosol loading (microscopic particles in the atmosphere that affect climate and living organisms), and the introduction of novel entities (e.g. organic pollutants, radioactive materials, nanomaterials, micro-plastics); Sustainability Guide, *Planetary Boundaries*, [Online]. Available at: <https://sustainabilityguide.eu/sustainability/planetary-boundaries/> (Accessed: 30 April 2024).

⁷ United Nations, as quoted in Pisani, 2006, p. 91.

⁸ Toussaint and Dumez, 2022.

⁹ Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies (1967) [referred to as "Outer Space Treaty"].

international law, including the Charter of the United Nations, in order to maintain international peace and security and promote international cooperation and understanding; and art. IX makes the environmental protection of outer space integral to the implementation of all space activities:¹⁰

State Parties shall pursue studies of outer space, including the moon and other celestial bodies, and conduct exploration of them so as to avoid their harmful contamination and also adverse changes in the environment of the Earth resulting from the introduction of extraterrestrial matter.

Art. III appears pertinent to the concept of sustainability, though it is not mentioned. The earliest document that explicitly addresses sustainable development as an imperative seems to be the European Code of Conduct, proposed in 2004. It sought to foster an understanding among the public of the gravity of the threat and the need to ensure sustainable development in near-Earth space. Although unsuccessful, it marked the inception of discussions regarding the necessity for cohesive measures in this regard. No definition of “sustainability” was provided by the draft Code of Conduct, the Space Debris Mitigation Policy for Agency Projects adopted by the European Space Agency (ESA) on March 28, 2014,¹¹ the Space Debris Mitigation Guidelines issued by the Inter-Agency Space Debris Coordination Committee (IADC),¹² the COPUOS 2010 Space Debris Mitigation Guidelines,¹³ or Recommendation ITU-R S.1003.2 on the environmental protection of the geostationary-satellite orbit S series.¹⁴ Nevertheless, the direction set in those documents gradually led to a more comprehensive approach (i.e. beyond just space debris) taken by the UN and European and national legislators.

The first international-level document that directly addressed the concept of sustainability seems to be the proposal of the Committee on the Peaceful Uses of Outer Space, adopted at the 59th session (June 8–17, 2016),

¹⁰ Yang, 2023, p. 4.

¹¹ ESA/ADMIN/IPOL(2014)2, [Online]. Available at: https://www.iadc-home.org/documents_public/file_down/id/4150 (Accessed: 30 April 2024).

¹² IADC, Available at: <https://orbitaldebris.jsc.nasa.gov/library/iadc-space-debris-guidelines-revision-2.pdf> (Accessed: 30 April 2024).

¹³ UNOOSA, [Online]. Available at: https://www.unoosa.org/pdf/publications/st_space_49E.pdf (Accessed: 30 April 2024).

¹⁴ Recommendation ITU-R S.1003.2 (ITU), [Online]. Available at: https://www.itu.int/dms_pubrec/itu-r/rec/s/R-REC-S.1003-2-201012-I!!PDF-E.pdf (Accessed: 30 April 2024).

which provided the first set of guidelines and a renewed work plan for the Working Group on the Long-term Sustainability of Outer Space Activities of the Scientific and Technical Subcommittee.¹⁵ This was followed by the Guidelines for the Long-term Sustainability of Outer Space Activities, which define sustainability as the ability to maintain the conduct of space activities indefinitely into the future in a manner that realizes the objectives of equitable access to the benefits of the exploration and use of outer space for peaceful purposes, in order to meet the needs of the present generations while preserving the outer space environment for future generations.¹⁶

The guidelines are based on the idea that the interests and activities of states and international intergovernmental organisations in outer space, insofar as they have or may have implications for defence or national security, should be consistent with the preservation of outer space for peaceful exploration and use, as well as with its status under the Outer Space Treaty and relevant principles and norms of international law.¹⁷ That idea became the main concept governing the modern regulation of space activity. Although none of these documents mentioned military space activities explicitly, neither did they exclude them or limit their application to civil space exploration. They may and should exert considerable influence in those domains. It is imperative to ascertain their applicability to military activities and determine whether there is any reason to exempt such activities from these regulations, should they acquire the force of customary law.

¹⁵ These guidelines were followed by Resolution No. 75/36 of 7 December 2020, A/RES/75/36, where the UN COPUOS expressed a ‘desire that all Member States reach a common understanding of how best to act to reduce threats to space systems in order to maintain outer space as a peaceful, safe, stable and sustainable environment, free from an arms race and conflict, for the benefit of all, and consider establishing channels of direct communication for the management of perceptions of threat’.

¹⁶ COPUOS, Guidelines for the Long-term Sustainability of Outer Space Activities, 27 June 2018, 5A/AC.105/2018/CRP.20. It must be noted that the guidelines are voluntary and not legally binding under international law, but any action taken towards their implementation should be consistent with the applicable principles and norms of international law. [Online]. Available at:

https://www.unoosa.org/documents/pdf/PromotingSpaceSustainability/Publication-Final_English_version.pdf (Accessed: 30 April 2024).

¹⁷ See the Report and Annex II thereto on LTS. [Online]. Available at: https://www.unoosa.org/res/oosadoc/data/documents/2019/a/a7420_0_html/V1906077.pdf (Accessed: 30 April 2024).

The Guidelines cover several of the most important aspects of space exploration that impact sustainability. Those relevant to military space operations include the guidelines enumerated in Table 1.

Table 1 *Extract from the Guidelines of long-term sustainability of Outer Space (LTS) (by author, on the basis of LTS Guidelines)*

Guideline A.1	Adopt, revise, and amend, as necessary, national regulatory frameworks for outer space activities: “States should adopt, revise or amend regulatory frameworks to ensure the effective application of relevant, generally accepted international norms, standards and practices for the safe conduct of outer space activities”
Guideline A.2	Consider a number of elements when developing, revising, or amending, as necessary, national regulatory frameworks for outer space activities
Guideline A.5	Enhance the practice of registering space objects
Guideline B.8	Design and operate space objects regardless of their physical and operational characteristics
Guideline B.9	Take measures to address risks associated with the uncontrolled re-entry of space objects
Guideline B.10	Observe measures of precaution when using sources of laser beams passing through outer space

One of the most recent document worth citing with respect to sustainability is the Opinion of the European Economic and Social Committee.¹⁸ It asserts that the management of space traffic, including debris, is the highest priority and calls for the implementation of a space

¹⁸ Opinion of the European Economic and Social Committee on the Proposal for a Regulation of the European Parliament and of the Council establishing the Union Secure Connectivity Programme for the period 2023–2027 (COM(2022) 57 final–2022/0039 (COD)) and Joint Communication to the European Parliament and the Council: An EU Approach for Space Traffic Management—An EU contribution addressing a global challenge; (JOIN(2022) 4 final), *OJ C* 486, 21.12.2022, pp. 172–184.

situational awareness system to ensure the long-term sustainability of space for all Member States. Finally, the plans of the EU Space Law (EUSL) are based on preserving the security, resilience, and sustainability of space activities and operations. The sustainability pillar of the EUSL aims to ensure the long-term sustainability of space operations and thus the EU's ability to rely on space as a key enabler of services and economic growth. This goes hand-in-hand with the Joint Communication of 10 March 2023, on an EU Space Strategy for Security and Defence to increase the security and resilience of space operations and services in the EU, as well as their safety and sustainability. An EU Space Act is being prepared with a view to promoting the development of resilience measures in the EU, information exchange for significant incidents, and cross-border coordination and cooperation.¹⁹

As the preceding analysis shows, the concept of sustainability is not tied to a specific category of space activities, but applies equally to both civilian and military utilisation. However, certain activities pose greater threats to sustainability goals than others. A prime example is the ASAT testing conducted by governments of spacefaring nations, which are inherently linked to military operations in outer space. Military space missions have followed a distinct trajectory for a long time, existing outside established regulatory frameworks. This trajectory is encapsulated in the remarks of a US Secretary of Defense, who said “for decades, the U.S. military conducted space activities with little regards for how they polluted orbits with debris that posed threats to existing and future space-based assets”, and in the past, the focus was primarily on achieving military objectives, with not much consideration given to the long-term sustainability of the space environment.²⁰

Based on what it had learned, the United States became the first country to adopt a moratorium on the destructive testing of direct-ascent anti-satellite missile systems in April 2022. In July 2021, the US Department of Defense adopted the “Tenets of responsible behaviour in space” in a Memorandum for Secretaries (of 7.07.2021), which include limiting the creation of long-lasting debris. The Tenets include the following: operating in, from, to, and through space with due regard to

¹⁹ Cesari, Developing an EU Space Law: the process of harmonising national regulations, [Online]. Available at: <https://www.mcgill.ca/iasl/article/developing-eu-space-law-process-harmonising-national-regulations> (Accessed: 30 April 2024).

²⁰ Erwin, 2023.

others and in a professional manner; limiting the generation of long-lived debris; avoiding harmful interference; maintaining a safe separation and trajectory; and communicating and providing notifications to enhance the safety and stability of the domain.²¹

3. ASAT tests and sustainability

One of the most pertinent issues related to the sustainability of outer space activities are ASAT tests.²² ASATs are space weapons designed to target, destroy, disable, or impair satellites. These systems can be directed towards both military and civilian satellite networks, serving both offensive and defensive purposes.²³ The technology can also be employed for ballistic missile defence purposes.²⁴ There are two main types of ASATs: kinetic and non-kinetic. Kinetic systems utilise direct ascent methods, employing ballistic missiles to propel an interceptor onto a trajectory to destroy the target through sheer kinetic force. By contrast, space-to-space co-orbital systems (i.e. the non-kinetic type) require a space launch vehicle to position an interceptor in orbit, which then collides with or passes by the target, utilising explosives to destroy the target. Another category of anti-satellite weapon employing “directed energy” in the form of laser beams, sub-atomic particles, radio frequencies, or microwave generators may emerge in the future and play a significant role.²⁵

²¹ Memorandum for Secretaries of the military departments Chairman of the Joint Chiefs of Staff under Secretaries of Defense Chiefs of the military services, Commanders of the Combatant Commands, General Counsel of the Department of Defense, Directors of Defense Agencies of 7th July 2021. Although the Tenets seem to be in line with the postulates of sustainability, some differences in approach should be noted. They concern the notion of “responsible behaviour” and its content in relation to space debris mitigation (i.e. the Memorandum’s focus on limiting the generation of long-lived debris, rather than all debris).

²² Bittencourt, 2013; Cassotta, 2019; Williams, 2008; Cuddihy, 2000.

²³ Towards ASAT Test Guideline, [Online]. Available at: <https://unidir.org/wp-content/uploads/2023/05/en-703.pdf> (Accessed: 30 April 2024).

²⁴ U.S. Congress, Office of Technology Assessment, Chapter 5: ASAT Arms Control: History in: “Anti-satellite Weapons, Countermeasures and Arms Control: Summary”, U.S. Government Printing Office, Washington 1984, p. 94, [Online]. Available at: <https://www.princeton.edu/~ota/disk2/1985/8502/850207.PDF> (Accessed: 30 April 2024).

²⁵ Kinetic ASATs must physically strike an object in order to destroy it. Examples of kinetic ASATs include ballistic missiles, drones that drag an object out of orbit or detonate explosives in proximity to the object, and any item launched to coincide with the passage of a target satellite. Thus, any space asset, even a communications satellite, could become an

ASAT tests have been conducted by four countries (the Russian Federation, the United States, China, and India), who have conducted approximately 80 tests in total. Comprehensive studies mapping the proliferation of various types of ASAT weapons show that numerous states possess kinetic ASAT weapons designed to physically impact a target.²⁶ The United States, Russia, China, and India have conducted tests involving such weapons on their own satellites, resulting in the generation of significant space debris orbiting the Earth. Spacefaring countries have also developed other counter-space capabilities apart from the ASAT with potential military utility. These can be divided into five categories: direct-ascent, co-orbital, electronic warfare, directed energy, and cyber.²⁷ Among them, ASAT as a destructive counter-space capability seems to be the most important to assess from the sustainability point of view.

The primary outcome of ASAT tests is the generation of space debris. This exacerbates the risk of the Kessler syndrome, in which a high density of objects encircling the Earth increases the likelihood of collisions, with each collision generating additional debris, amplifying the risk of further collisions. Since the inaugural ASAT test in 1968, destructive tests have produced over 6,300 fragments of debris, as reported by the Secure World Foundation, which monitors developments in space security.²⁸

However, the prevailing view of scholars is that the Outer Space Treaty and other binding space legislation do not prohibit ASAT tests. For

ASAT if it were used to physically destroy another space object. A non-kinetic ASAT can use a variety of non-physical means to disable or destroy a space object, such as frequency jamming, blinding lasers, or cyberattacks. These methods can also render an object useless without causing the target to break up and fragment, absent additional forces intervening. Strobeyko, 2019; Koplow, 2009, p. 1201.

²⁶ Peperkamp, *An Arms Race in Outer Space?* *Atlantisch Perspectief*, 44(4), [Online]. Available at: <https://www.jstor.org/stable/48600572> (Accessed: 30 April 2024); Weeden and Samson (eds), 2020, *Global Counterspace Capabilities Report*, Secure World Foundation. Available at: https://swfound.org/media/206955/swf_global_counterspace_april2020.pdf (Accessed: 30 April 2024); Harrison, *Space Threat Assessment*, Center for Strategic & International Studies. [Online]. Available at: <https://www.csis.org/analysis/space-threat-assessment-2020/> (Accessed: 30 April 2024).

²⁷ Secure World Foundation 2024, *Global Counter Space Capabilities – Report* [Online]. Available at: https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf (Accessed: 30 April 2024).

²⁸ *Op. cit.*

example, Art. IV of the OST prohibits only the placement of nuclear weapons in space. There is also no prohibition against testing, developing, or deploying (nuclear) weapon systems for use in space or against space objects. However, in view of the destructive effects of ASATs, work has begun to stop their deployment. In this context, the UN General Assembly Resolution and the moratorium announced by the United States should be mentioned in particular.²⁹

In April 2022, the United States announced a unilateral moratorium and pledged not to test any more destructive direct ascent anti-satellite missiles. Vice President Kamala Harris announced that the United States commits:

...not to conduct destructive, direct-ascent anti-satellite (ASAT) missile testing, and that the United States seeks to establish this as a new international norm for responsible behaviour in space.

This commitment was followed by a call for other nations to make similar commitments and work together to establish this as the norm, arguing that such efforts benefit all nations. Since then, several countries have made pledges, beginning with Canada in May 2022 and most recently Costa Rica and Norway in October 2023, bringing the total number of participating countries to 37.

Soon after the Moratorium, on 7 December 2022, the UN General Assembly adopted Resolution A/RES/77/41 in support of a moratorium on destructive DA-ASAT testing.³⁰ The Resolution does the following:

1. Calls upon all States to commit not to conduct destructive direct-ascent anti-satellite missile tests.
2. Considers such a commitment to be an urgent, initial measure aimed at preventing damage to the outer space environment, while also contributing to the development of further measures for the prevention of an arms race in outer space.
3. Calls upon all States to continue discussions in the relevant bodies and to establish and develop further practical steps that could be taken, in order to

²⁹ Wei Sooi, WSF, *Direct-Ascent Anti-Satellite Missile Tests: State Positions on the Moratorium, UNGA Resolution, and Lessons for the Future*, [Online]. Available at: https://swfound.org/media/207711/direct-ascent-antisatellite-missile-tests_state-positions-on-the-moratorium-unga-resolution-and-lessons-for-the-future.pdf (Accessed: 30 April 2024).

³⁰ In total, 155 states voted in favour, with 9 voting against and 9 abstentions. Notably, the United States, India, China, and Russia are the only states that have demonstrated a destructive direct-ascent anti-satellite missile capability.

enable risk reduction, prevent conflict from occurring in outer space and prevent an arms race in outer space; such steps could include, inter alia, transparency and confidence-building measures and additional moratoriums, which could contribute to legally binding instruments on the prevention of an arms race in outer space in all its aspects.

Both these documents, although not legally binding and adopted voluntarily, represent significant developments, particularly given the broader context of stalemate in space security negotiations, such as those concerning the prevention of an arms race in outer space (PAROS).³¹

4. Role of national laws in promoting sustainable military space operations

ASAT testing, although one of the most important issues, is only a symptom of the broader problem, which concerns the overall regulatory framework for military space operations. In this respect, the words of Kamala Harris regarding the ASAT ban seem symptomatic:

Without clear norms we face unnecessary risk in space... The United States will work with commercial industry and allies to lead in the development of new measures that contribute to the safety, stability, security, and long-term sustainability of space activities. Through this new commitment and other actions, the United States will demonstrate how space activities can be conducted in a responsible, peaceful, and sustainable manner. It's an attempt to lead by example and demonstrate we're willing to make this commitment ourselves and then encourage others to follow.

These words should be applied not only to civil space activities but also to military ones. Although this seems obvious, it is not clear from the practices of States. Under Art. VI of the Outer Space Treaty, supervision and control through authorisation for space activities apply only to non-governmental activities: The activities of non-governmental entities in outer space, including the Moon and other celestial bodies, shall require authorization and continuing supervision by the appropriate State Party to the Treaty.

Thus, the treaty does not oblige states to introduce norms for the authorisation and ongoing supervision of military (usually governmental) space operations. This gap may seem insignificant from a political and legal point of view, as States are liable and responsible for any damage caused by

³¹ Sooi, 2023.

either governmental or non-governmental space missions. However, most space laws enacted by spacefaring nations are vague regarding the rules for conducting military space operations.

An example can be seen in the French approach to military space activities. France's Space Defence Strategy, announced in 2019, develops mainly through the competence of the respective authorities. Though well-established, French space law is focused on commercial applications and sets no requirements for governmental military space activities. Consequently, according to Article 26 of the French space law,³² the law does not apply to the launch and control of space objects required for national defence, the trajectories of which pass through outer space, such as ballistic missiles. Moreover, the activities of the Ministry of Defence, acting as primary space-based data operator, are not subject to the provisions of Title VII (which means that they are not obliged to report their activities to the public administration).

Another example is US space law. The US Commercial Space Act adopted in November 2023 is aimed at regulating non-governmental space activities. Thus, military activities, such as efforts at preserving sustainability in space, are not subject to transparent regulations. The bill designates the Department of Commerce Office of Space Commerce (DOC/OSC) as the sole authority responsible for the authorisation and supervision certification process. It also grants the OSC sole authority and responsibility for making determinations and placing conditions on certifications to ensure compliance with international obligations. The military component of space activities is excluded from the application of the regulatory measures in the Act.

Circumstances are similar regarding space legislation in the United Kingdom, where significant strides have been made at the regulatory level. This progress began in 1986 with the adoption of the Outer Space Act 1986, which has since been amended by the Space Industry Act 2018 and complemented by the Space Industry Regulations of 2021.³³ The legal

³² Law No. 2008-518 of June 3, 2008, regarding Space Operations (as amended by Law No. 2013-431 of May 28, 2013).

³³ The Spaceflight Activities (Investigation of Spaceflight Accidents) Regulations 2021 establish a spaceflight accident investigation body and provide for the conduct of accident investigations, [Online]. Available at: <https://www.legislation.gov.uk/ukxi/2021/793/contents/made> (Accessed: 30 April 2024); the Space Industry (Appeals) Regulations 2021 outline the decisions made by the CAA that

framework established in the United Kingdom focuses on civilian and industrial space missions. Military space affairs fall under the jurisdiction of the Ministry of Defence, which operates a Space Directorate. This directorate collaborates closely with the UK Space Agency and is responsible for the MoD's space policy and international coordination. The United Kingdom's military space program is overseen by UK Space Command, which was established in April 2021 and given overall command and control functions.

Conversely, the distinctiveness of Russian space legislation lies in its explicit regulation of space activities conducted for defence and security purposes within the Russian Federation, as outlined in Article 7. Russia's Ministry of Defence is responsible for overseeing these activities, as well as coordinating with other ministries and departments to implement long-term programmes and annual plans for the development and utilisation of both military and civilian space technologies.

The examples discussed above show that it is crucial to recognise the disparity between the political commitments made by states on the international stage and their governance of military space missions at the national level. Although international declarations hold significant importance, they lack binding authority, whereas national laws enact regulations that increasingly impose sustainability obligations, primarily targeting civilian missions. This is achieved by confining space laws to non-governmental missions or by distributing responsibilities among various authorities at the governance level. A potential remedy for this gap could involve partially integrating military government space operations into the framework of technical safety regulations, thereby enhancing the sustainability of outer space exploration efforts.³⁴ This goal could be tackled through the forthcoming EU Space legislation, which constitutes one of the initiatives aimed at realising the objectives outlined in the EU Space and Defence Strategy. The concept of the EU space regulatory framework was introduced in late 2022 through a communication from the Social Economic Committee,³⁵ which stated that one of the main goals of establishing

may be appealed and set procedures and timescales for making and deciding appeals; <https://www.legislation.gov.uk/ukxi/2021/816/contents/made> (Accessed: 30 April 2024).

³⁴ An example of such an approach may be seen in the Polish draft of the space law. Though it excludes governmental missions from authorisation and insurance obligations, it ensures that they are conducted in accordance with technical regulations.

³⁵ Opinion of the European Economic and Social Committee on the Proposal for a Regulation of the European Parliament and of the Council establishing the Union Secure

consistent space law for the whole EU is to enhance the level of security and resilience of space operations and services in the EU, as well as their safety and sustainability, the Commission will consider proposing an EU Space Law. It will encourage the development of resilience measures in the EU, foster information-exchange on incidents as well as cross-border coordination and cooperation.

Thus, safety and sustainability are directly related and should be extended to military space activities. With space recognised as a strategic domain, additional measures are required to fortify the EU's strategic posture and autonomy in space through regulatory interventions. Consequently, ongoing analysis and consultations aim to delineate the necessary scope of European space law. Preliminary considerations indicate a focus on safety, security, and sustainability. It is crucial to strike a balance between the civilian and commercial dimensions of space and the defence aspects of space activities, without encroaching upon the internal laws of Member States.³⁶

Regarding regulatory approaches to military space operations at the international, regional, and national levels, it is important to recognise the significance of academic initiatives. For example, two manuals on warfare in the space domain are being developed by expert groups: the Woomera Manual on the International Law of Military Space Operations, led by the University of Adelaide and Exeter University;³⁷ and the Manual on International Law Applicable to Military Activities in Space (MILAMOS) by McGill University (Canada). Although these manuals lack strict enforceability, their influence is widely acknowledged, and they are relied upon by governments and armed forces. They have the potential to shape space policy and military doctrines and help prevent the hostile use of space weapons.

Connectivity Programme for the period 2023–2027 (COM(2022) 57 final — 2022/0039 (COD)) and Joint Communication to the European Parliament and the Council: An EU Approach for Space Traffic Management — An EU contribution addressing a global challenge; (JOIN(2022) 4 final), *OJ C 486*, 21.12.2022, pp. 172–184.

³⁶ See The Strategic Compass for Security and Defence and called for an EU Strategy for security and defence. [Online]. Available at: <https://consilium-europa.libguides.com/strategic-compass/EUpublications> (Accessed: 30 April 2024).

³⁷ The Woomera Manual On The International Law Of Military Space Operations, [Online]. Available at: <https://law.adelaide.edu.au/woomera/system/files/docs/Woomera%20Manual.pdf> (Accessed: 30 April 2024).

The MILAMOS, launched in May 2016, aims to develop widely accepted fundamental rules for the military use of outer space.³⁸ The authors state as follows:

The MILAMOS Project was initiated with a vision of contributing to a future where all space activities are conducted in accordance with the international rules-based order, without disrupting, and preferably contributing to, the sustainable use of outer space for the benefit of present and future generations of humanity.³⁹

The Manual clarifies the application of international and national space laws to military space operations. Its provisions include the following:

Rule 109: All space activities, including military space activities, shall be carried on in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding.

Rules 110: A State may not rely on its national law as justification for failure to comply with its international obligations related to its space activities, including military space activities

Rule 111: An international organisation that carries on space activities, including military space activities, shall comply with general international law, constituent instruments and other rules of that organisation, and international treaties in respect of which it has expressed its consent to be bound

Rule 124: When a space object, including a space object used in military space activities, is launched into Earth orbit or beyond, a launching State shall register the space object by means of entry in its appropriate national registry.

Rule 129: International law does not contain explicit rights and obligations regarding the creation of space debris. However, to the extent necessary to comply with other rules of international law, States and

³⁸ The Milamos Group of Experts Arrived at a Consensus on Key Issues Reflected In 52 Rules, Which Are Set Out in This Manual. Volume I Covers a Variety of International Law Issues Particularly Relevant to Current and Potential Military Uses of Outer Space, [Online]. Available at: https://www.mcgill.ca/milamos/files/milamos/mcgill_manual_volume_i_-_rules_final_0.pdf (Accessed 30 April 2024).

³⁹ McGill Manual On International Law Applicable To Military Uses Of Outer Space. [Online]. Available at: https://www.mcgill.ca/milamos/files/milamos/mcgill_manual_volume_i_-_rules_final_0.pdf (Accessed: 30 April 2024).

international organisations shall limit the creation of space debris when carrying on space activities, including military space activities.

5. Governance of military space activities: A remedy for responsible behaviour

Outer space activities remain anarchic in terms of governance, primarily in their lack of an overarching authority.⁴⁰ The deficiencies in this regard extend beyond the regulatory framework and include the governance structure. At the global, regional (e.g. EU), and national levels, there is a complex matrix of authorities vested with competencies concerning space defence. This section conducts a vertical analysis of the roles and regulations related to the governance of military operations. At the national level, the analysis considers France and the United Kingdom because their advanced space legislation and policy can serve as an example of the way forward.

At the global level, the role of the UN is constrained, limiting its ability to preserve the foundational principles governing outer space exploration, particularly in light of the diminishing scope for the peaceful use of space endeavours. Given prevailing geopolitical tensions, there is a pervasive scepticism regarding the UN's efficacy as a policymaker and rule-setter. Consequently, coordination of defence and military matters on the international stage is more appropriately conducted within military and political alliances, such as NATO.

Although the efforts of the international community to introduce sustainability goals and responsible behaviour should not be ignored, they are not of great importance from a governance perspective. Many voices are calling for the establishment of an intergovernmental organisation (similar to the IADC) with responsibilities for coordinating sustainability measures for both civil and military space applications.⁴¹

Conversely, within the EU at the regional level, implementing a space defence strategy necessitates a restructuring of space governance. From an

⁴⁰ Tepper, 2022, p. 490.

⁴¹ See, for example, the Montreal Recommendations on Aviation Safety and Uncontrolled Space Object Reentries by the Outer Space Institute. Its Recommendation no. 1 proposes that 'states should establish a new international body or build upon an existing one to provide a focus on the safety implications of uncontrolled reentries'; [Online]. Available at: <https://outerspaceinstitute.ca/osisite/wp-content/uploads/Montreal-Recommendations-on-Aviation-Safety-and-Uncontrolled-Space-Object-Reentries.pdf> (Accessed: 30 April 2024).

institutional point of view, EU-level space administration is very diverse and relies on several institutions due to the integration of both supranational and national elements.⁴² The European space sector is governed by three main actors: the ESA, the EU (through the European Commission), and the European Union Agency for the Space Programme (EUSPA), the operational agency in charge of the Space Programme. The ESA is excluded from this analysis because of its independence from the EU and its technological nature. The publication of the EU Space Strategy for Security and Defence was a milestone in the process of unifying space activities at the EU level.⁴³ The Strategy emphasises the role of the European Commission in synchronising and coordinating activities in critical space technologies together with the European Defence Agency (EDA) and ESA, as well as the EUSPA.⁴⁴ The Directorate-General for Defence Industry and Space leads the European Commission's activities in the defence and space sectors.

Although the EUSPA oversees civilian programs, in recognition of their dual-use potential, the EDA assumes a central role. The EDA's activities span various facets of the space domain, including prioritisation and planning to bolster space capability development, engaging in research and technology (R&T) activities pertaining to space, and identifying common military requirements and defence user needs for space-based systems. This encompasses collaborative capability development and alignment with broader EU space policy objectives. The newly established Defence in Space Forum, under the purview of the EDA, plays a pivotal role

⁴² The European space ecosystem consists of 22 members of the ESA: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, and the United Kingdom. Latvia, Lithuania, and Slovenia are Associate Members. The ESA signed European Cooperating States Agreements with Bulgaria, Cyprus, and Slovakia and cooperation agreements with Croatia and Malta, as well as 27 other members of the EU, often with separate national space agencies and space strategies.

⁴³ EU Space Strategy for Security and Defence for a stronger and more resilient European Union. [Online]. Available at: https://defence-industry-space.ec.europa.eu/eu-space-policy/eu-space-strategy-security-and-defence_en (Accessed: 30 April 2024).

⁴⁴ The EU Council on approved the Council Conclusions on the EU Space Strategy for Security and Defence on 13 November 2023; EU Space Strategy for Security and Defence, p. 5; Joint communication to the European Parliament and the Council on the EU Space Strategy for Security and Defence, March 10, 2023, p. 5.

in identifying military requirements, delineating capability priorities, and fostering cooperation in space among EU Member States.

Owing to the circumstances and threats that have emerged over the past few years,⁴⁵ the EDA has become increasingly important in the context of space activities. Security and defence would be at risk without the provision of a resilient space infrastructure. Therefore programmes coordinated by the EDA are coming up against several challenges as they fill the gaps of European defence capabilities. The EDA also focuses on broader areas. Its role includes the development of R&T⁴⁶ capabilities and engaging in other activities in the space sector; the planning and prioritisation of space development and capabilities;⁴⁷ and the identification of the needs of Member States in the space domain, including the mapping of training and education activities to assist public administration in the field of space security and defence, as well as the exchange of best practices in developing space-related skills.

The Defence and Security Strategy underscores collaboration between the European Commission, supported by the EUSPA, and the EDA and ESA.⁴⁸ Additionally, the governance of the EU Space Programme is defined by a clear allocation of tasks and responsibilities among the entities involved in implementing each of its components and measures. This includes the Member States, the Commission, the EUSPA, the ESA, and EUMETSAT. These allocations are based on their respective competences, to prevent any overlap in tasks and responsibilities.⁴⁹

It appears that the sphere of military space operations is typically beyond the purview of national agencies. The authority of military administration tends to prevail when defence and security issues arise in the context of civilian space missions. Furthermore, military space operations typically fall under the exclusive control of the armed forces, often

⁴⁵ For example, Russia's aggression against Ukraine and the increased development of counterspace capabilities and threats in the form of DA-ASAT tests and cyberattacks on space infrastructure.

⁴⁶ The Capability Technology Group Space (CapTech Space) was established in 2022 by the EDA Research and Technology Steering Board, which is focused on strengthening and coordinating R&T for space defence in Europe.

⁴⁷ EDA, Defence in Space, [Online]. Available at: <https://eda.europa.eu/news-and-events/spotlight/spotlight-of-the-month/defence-in-space-how-is-eda-providing-support-to-the-eu-s-wider-strategy> (Accessed: 30 April 2024).

⁴⁸; See Council Conclusions, 2023.

⁴⁹ Article 26 of Regulation (EU) 2021/696.

involving the establishment of specialised divisions for space command, as exemplified in the cases of the United States and United Kingdom. It is crucial to emphasise, however, that most national space laws lack clarity regarding the delineation of administrative tasks and powers within this domain. It would be worthwhile considering those among the many spacefaring countries that have well-established approaches. It would also be interesting to examine how space governance, especially space agencies, operate in EU and non-EU countries, particularly in the context of possible relations with the EU space administration.

France is an interesting example. Space administration in France traces its origins to 1958, when several space research committees were established. This was followed by the creation of the Comité d'études spatiales in 1959 and the Centre national d'études spatiales (CNES) in 1961.⁵⁰ The CNES is France's national space agency, operating under the supervision of the Ministry of Economy, Ministry of Higher Education and Research, and Ministry of Defence. This cross-sectoral approach to space management in France can also be seen in the use of satellite frequencies, for which the competent body is the French National Frequency Agency created in 1997 and operating under the supervision of the Minister responsible for telecommunications, although its powers do not extend to government programmes.⁵¹

The role of the CNES is defined in the Research Code (L-331-1 - L 331-6), according to which the CNES is responsible for defining and implementing French space policy in five main areas: launchers, science, Earth observation, telecommunications, and defence.⁵² Regarding the latter, close cooperation between the CNES and the Ministry of Defence is envisaged on the basis of the French Space Defence Strategy (SDS) announced in 2019.⁵³ In particular, the SDS foresees new forms of interaction between the Ministry, through the Space Command, and the CNES. The position of the CNES is more specific than that of other

⁵⁰ Act no 61-1382 of 19 December 1961 establishing the National Center for Space Studies (French Official Journal, 20.12.1961).

⁵¹ Achilleas, 2010, p. 113.

⁵² Achilleas, 2010, p. 110.

⁵³ French Space Defence Strategy (2023), [Online]. Available at: <https://www.frstrategie.org/en/publications/notes/implementing-french-space-defence-strategy-towards-space-control-2023>; French Ministry for the Armed Forces (2019). *Stratégie spatiale de défense, rapport du groupe de travail "espace"*. (Accessed: 30 April 2024).

European space agencies, because of the role of France in European space activities. Thus, the CNES has been entrusted with certain powers relating to the safety management of the spaceport in French Guyana, as delegated by the French government following the signing of two agreements between France and the ESA on 11 April 2002. This responsibility was also confirmed in the Research Code.⁵⁴

Concerning civil programmes, in addition to the Research Code, the powers of the CNES derive from the provisions of the French Space Act. The basic powers (e.g. the authorisation of space activities) are vested in the Ministry of the Economy; in practice, however, the supervision of licences and authorisations is largely delegated to the CNES and its legal and technical experts.⁵⁵ Within the Ministry, some related tasks are carried out by the General Directorate for Research and Innovation, which assists the Ministry in examining applications and exercising its responsibilities under the space law. As has been noted in sec. 4, French space law does not apply to the launch and control of space objects for the purposes of national defence with trajectories that pass-through space, such as ballistic missiles. The activities of the Ministry of Defence, as the primary operator of space data, are not subject to the provisions of Title VII, which means that France's civil and military space administrations operate in parallel.

The United Kingdom presents another interesting example. The UK National Space Strategy 2021 outlines the country's approach to space governance, characterised by a cross-governmental framework; various bodies operate at different levels to ensure its execution. In 2019, the government introduced the National Space Council, a cabinet committee chaired by the prime minister, tasked with providing strategic direction for the cross-governmental approach to space and formulating a strategy. Additional entities include the Department for Business, Energy and Industrial Strategy, which serves as the central department responsible for coordinating civil space policy and sponsors both the UK Space Agency and UK Space Command, alongside the Ministry of Defence. At the implementation level, key bodies include the UK Space Agency (UKSA), the Civil Aviation Authority (CAA), and Space Command.

⁵⁴ Achilleas, 2010, p. 110.

⁵⁵ Couston, 2014, p. 129.

A parallel line of space governance covers the defence aspects of space.⁵⁶ For this purpose, the UK Space Command has been established as the defence lead for space operations, the space workforce, and space capabilities, based on the Defence Space Strategy. It is co-ordinated by the Ministry of Defence and also works with the UKSA to deliver a common national space capability in line with the National Space Strategy. This includes the establishment of a combined military and civilian National Space Operations Centre.

As far as the Central Eastern Europe (CEE) space governance model is concerned, most countries rely on joint coordination between several ministries and various related public agencies. Considering the concept of space governance in Western European countries, the new space countries of the CEE seem to be following the same path. The question that deserves more attention is whether the increasing dependence on space technologies and applications in the civil and military fields may require a rethinking of the role of space agencies. Should they not be given more independence and coordination powers, rather than being subordinated to various ministries? An examination of existing approaches suggests that national space agencies could play a coordinating role in both the civil and defence spheres, in cooperation with rather than subordination to ministries, while also ensuring a consistent implementation of space programmes, strategy, and regulations. Such an approach could be beneficial by fostering a consistent approach to different types of space missions, while increasing the potential for the sustainable development of space exploration.

An examination of the strategies used by the EU and individual Member States as well as space legislation at the international, regional, and national levels reveals a current trend for the development of strategic documents that are specifically tailored to the space domain. This trend involves formalising activities and delineating competencies among bodies responsible for space, particularly in the context of military applications versus commercial space activities. The role of space agencies, typically operating under civilian government administration, lacks clarity concerning the application of space legal provisions. Although legal regulations for space use are being developed, primarily at the national level and for civilian applications, the role of space agencies is well-defined in these

⁵⁶ Defence Space Strategy: Operationalising the Space Domain. [Online]. Available at: https://assets.publishing.service.gov.uk/media/61f8fae7d3bf7f78e0ff669b/20220120-UK_Defence_Space_Strategy_Feb_22.pdf (Accessed: 30 April 2024).

contexts. However, the situation becomes more ambiguous when military missions are involved. Regulations pertaining to space law that could apply to military matters often exist in a regulatory grey area, where licensing is not required, and are consequently lacking clear adherence to technical standards, including those aimed at preventing space debris and ensuring the sustainability of space exploration. The authority of space agencies in certifying space activities is therefore uncertain.

6. Conclusion

An analysis of space strategies and legislation across international, regional, and national levels reveals an ongoing development of strategic documents tailored specifically to the space defence domain. This process involves institutionalising activities and delineating competencies between bodies responsible for space military issues and commercial space activities. Although legal regulations for space use are also being developed, primarily at the national level and for civilian applications, regulations pertaining to space law that could apply to military matters often remain in a regulatory grey area. They are not subject to licensing and consequently lack clear adherence to technical standards, particularly concerning space debris prevention and sustainability, as observed in civilian missions.

International legal acts that are binding on states, regardless of mission purpose, contain either very general regulations subject to inconsistent interpretations or are non-binding, such as UNGA resolutions. This lack of a comprehensive regulatory framework for military applications poses a significant threat to the future of human activities in space, in terms of both the security of space assets and ground security as a last resort.

Among the many regulatory grey zones that require attention, one of the most important is the need to provide a coherent application of regulatory measures for ensuring responsible behaviour in outer space, thus fostering sustainable development. Achieving this will require such fundamental objectives as imposing a universal ban on ASAT testing and preventing the generation of space debris. Neither of these issues, which are so crucial for sustainable development, has any chance of being regulated by mandatory standards at the international level. However, progress can be made in small steps through unilateral commitments by states, such as the Moratorium initiated by the United States in 2022, as well as the comprehensive approach to the space sector proposed by the EU. This also

means that the United States and the EU could eventually play a leading role as promoters of legal arrangements governing sustainability in all types of space activities, even if only by promoting binding documents on the basis of national adherence. Legal frameworks in this realm could be established through decisive, coordinated, and harmonised technical standards, as well as clear requirements for both governmental and private entities.

Bibliography

- [1] Achilleas, P. (2010) Regulation of Space Activities in France. in Jakhu, R. S. (ed.), *National Regulation of Space Activities*. Springer, pp. 109-122.
- [2] Bittencourt, O. (2013) Defining the Limits of Outer Space for Regulatory Purposes. Springer.
- [3] Bohlmann, U., Petrovici, A. (2019) Space sustainability, long-term sustainability of space activities. in Froehlich A (ed.), *Sustainability of Outer Space Activities*, Springer, pp. 13-28.
- [4] Cassotta, S. (2019) The Paris Agreement vis-à-vis climate change in outer space law. In A. Froehlich (Ed.), *Sustainability of Outer Space Activities*, Springer, pp. 211-226.
- [5] Couston, M. (2014) *Droit spatial* [Space Law]. Ellipses.
- [6] Cuddihy, R. (2000) 'Law of anti-satellite weapons', *Air & Space Power Journal*, 14(4), pp. 100-121.
- [7] Erwin, S. (2023) 'Pentagon to adopt tenets of responsible behavior in space'. *SpaceNews*, [Online]. Available at: <https://spacenews.com/pentagon-to-adopt-tenets-of-responsible-behavior-in-space/> (Accessed 30 April 2024).
- [8] Harrison, T. (2020) Space threat assessment 2020. Center for Strategic & International Studies. [Online]. Available at: <https://www.csis.org/analysis/space-threat-assessment-2020/> (Accessed: 30 April 2024).
- [9] Jakhu, R. S., Pelton, J. N., Nyampong, Y. O. M. (2018) *Space mining and its regulation*. Springer. <https://doi.org/10.1007/978-3-319-39246-2>.

-
- [10] Koplow, D. A. (2009) 'ASAT-isfaction: Customary international law and the regulation of anti-satellite weapons', *Michigan Journal of International Law*, 30(4), pp. 1187-1272.
- [11] Lyall, F., Larsen, P. B. (2018). *Space law: A treatise* (2nd ed.). Routledge. <https://doi.org/10.4324/9781315610139>.
- [12] Peperkamp, J. (2020) 'An arms race in outer space?' *Atlantisch Perspectief*, 44(4), pp. 7-12.
- [13] Pisani, J. A. D. (2006) 'Sustainable development – historical roots of the concept' *Environmental Sciences*, 3(2), pp. 83-96. <https://doi.org/10.1080/15693430600688831>.
- [14] Strobeyko, P. (2019) 'Theoretical approaches to modern international conflicts: How to define and study 'hybrid warfare'', *Yearbook of the Institute of East-Central Europe*, 17(4), pp. 101-118.
- [15] Tepper, E. (2022) 'Space governance in the 21st century', *Journal of Space Law*, 46(2), pp. 487-521.
- [16] Toussaint, M., Dumez, J. (2022) 'The case for the development of a comprehensive legal regime for active debris removal', *Journal of Space Law*, 46(2), pp. 257-289.
- [17] Weeden, B., Samson, V. (Eds.) (2020) Global counterspace capabilities report. Secure World Foundation. [Online]. Available at: https://swfound.org/media/206955/swf_global_counterspace_april2020.pdf (Accessed 30 April 2024).
- [18] Williams, M. (2008) 'Anti-satellite missile test by China', *Strategic Comments*, 14(2), pp. 1-2.
- [19] Yang, H. (2023) 'Sustainability in outer space: A practical approach to the implementation of the long-term sustainability guidelines', *Air and Space Law*, 48(1), pp. 1-30; <https://doi.org/10.54648/AILA2023030>.

-
- [20] Defence Space Strategy: Operationalising the Space Domain. [Online]. Available at: https://assets.publishing.service.gov.uk/media/61f8fae7d3bf7f78e0ff669b/20220120-UK_Defence_Space_Strategy_Feb_22.pdf (Accessed: 30 April 2024).
- [21] European Council (2006) The renewed EU sustainable development strategy as adopted by the European Council on 15/16 June 2006 (10917/06). Brussels.
- [22] Secure World Foundation. (2024) Global counter space capabilities report. [Online]. Available at: https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf (Accessed: 30 April 2024).
- [23] Sooi, W. (2023) Direct-ascent anti-satellite missile tests: State positions on the moratorium, UNGA resolution, and lessons for the future. Secure World Foundation. [Online]. Available at: https://swfound.org/media/207711/direct-ascent-antisatellite-missile-tests_state-positions-on-the-moratorium-unga-resolution-and-lessons-for-the-future.pdf (Accessed 30 April 2024).
- [24] The Milamos Group of Experts Arrived at a Consensus on Key Issues Reflected In 52 Rules, Which Are Set Out in This Manual. Volume I Covers a Variety of International Law Issues Particularly Relevant to Current and Potential Military Uses of Outer Space, [Online]. Available at: https://www.mcgill.ca/milamos/files/milamos/mcgill_manual_volume_i_-_rules_final_0.pdf (Accessed: 30 April 2024).
- [25] The Woomera Manual On The International Law Of Military Space Operations, [Online]. Available at: <https://law.adelaide.edu.au/woomera/system/files/docs/Woomera%20Manual.pdf> (Accessed: 30 April 2024).

KRZYSZTOF MASŁO*

Accession of the European Union to the European Convention on Human Rights from the perspective of the Common Foreign and Security Policy**

ABSTRACT: According to Article 6 of the Treaty on the Functioning of the European Union, the European Union (EU) is obliged to access the European Convention on Human Rights (ECHR). Accession to the ECHR is particularly important in the context of Common Foreign and Security Policy (CFSP). The work carried out on the basis of which the EU will accede to the ECHR should aim to shape the future accession agreement so that it not only resolves the problem of judicial control over the CFSP and the compatibility of the law created with the standards developed by the European Court of Human Rights (ECtHR) but also, above all, addresses the relationship between the CJEU and the ECtHR in the context of the deficit of judicial control of the Court of Justice of the European Union (CJEU) over the law created under the CFSP and the practice of the functioning of this policy. This article thus focuses on previous works concerning EU accession to the ECHR, possible solutions to problematic questions, and the importance of the ECHR to the CFSP. The process of accession to the ECHR has shown that the introduction of an explicit legal basis in the treaties authorising the EU to do so has proven insufficient and created new problems which have in turn proved difficult to solve in practice.

Keywords: accession, Common Foreign and Security Policy (CFSP), Court of Justice of EU, European Convention on Human Rights (ECHR), Opinion 2/13, Protocol no. 8.

1. Introduction

The European Union (EU) is a community of states with respect for and observance of human rights. Among the many mechanisms for realising this

* Assistant professor, Cardinal Stefan Wyszyński University in Warsaw, Poland.
<https://orcid.org/0000-0002-9085-3589>, k.maslo@uksw.edu.pl.

** The research and preparation of this study was supported by the Central European Academy.

value, the Treaties mention accession to the European Convention of 4 November 1950 for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, ECHR). EU's accession to the ECHR will entail a fundamental change in EU's legal order, as the Union will become part of a distinct international institutional system and its legal order will be integrated not only with the provisions of the ECHR but also with the entire body of the case law of the European Court of Human Rights (ECtHR). Accession to the ECHR will thus have constitutional significance for the legal order created by the EU.

Accession to the ECHR is of particular importance in the context of the Common Foreign and Security Policy (CFSP), which, despite the Lisbon reform and its integration as one of the EU's policies and activities, is still intergovernmental rather than supranational in nature. Legislative acts adopted under the CFSP are drafted by bypassing the supranational bodies of the EU and, in addition, much of this legislation has been excluded from the jurisdiction of the Court of Justice of the European Union (CJEU). Therefore, the question arises as to how to ensure that the law created under the CFSP and the actions of the Member States and the EU in military and civilian missions are compatible with the fundamental rights and rich jurisprudence of the ECtHR. The work on the basis of which the EU will accede to the ECHR should aim to shape the future accession agreement so that it not only resolves the problem of judicial control over the CFSP and the compatibility of the created law with the standards developed by the ECtHR but also, above all, addresses the problem of the relationship between the CJEU and the ECtHR given the deficit of judicial control of the CJEU over the law created under the CFSP and the practice of the functioning of this policy.

This article does not address all aspects that the EU accession to the ECHR will bring about for the CFSP, as its primary purpose is to present a possible solution to the problem of the judicial control deficit of the CJEU over the CFSP. Until this problem is resolved, EU's accession to the ECHR is impossible. However, the solutions must comply with EU law, which has placed several conditions for accession to the ECHR. These considerations are preceded by a brief historical outline and characterisation of the current legal basis for accession. Opinion 2/13 requires a separate discussion in the context of the conditions under which the CJEU placed the accession agreement in the context of the CFSP.

2. Historical background to the process of EU accession to the ECHR with particular reference to the CFSP

The idea for the EU accession to the ECHR emerged in the 1970s. In 1979, the Commission presented a ‘Memorandum on the Accession of the European Communities to the ECHR’, with considerations for and against accession.¹ The Commission stressed that the formal accession of the Community to the ECHR was the best way to strengthen the protection of fundamental rights at the Community level and proposed to the Council to start the accession procedure. However, this document was not followed by any actual action to bind the three Communities to the ECHR.

The proposal to accede to the ECHR was reiterated in the Communication of the European Commission (EC) concerning the accession of the Community to the ECHR on 19 November 1990.² Then, the question of accession to the ECHR was not revisited until the 1990s, when the creation of the EU provided the impetus. On 26 October 1993, the EC published a working document titled ‘The Accession of the Community to the European Convention on Human Rights and the Community Legal Order’, in which it examined, *inter alia*, the question of the legal basis for accession and the exclusive jurisdiction of the Court of Justice (CJ) for judicial review.³ In 1993 as well, on the initiative of the Belgian Presidency, an *ad hoc* group was created within the Committee of Permanent Representatives (COREPER) to analyse the initiative for EU accession to the ECHR. As the working group did not reach a consensus on the existence of the European Community’s competence to accede to the ECHR and the compatibility of the accession with the EC legal autonomy and the exclusive jurisdiction of the CJ over Community law, the Council requested the CJ to deliver an opinion based on Article 228(6) TEC (now Article 218(11) Treaty on the Functioning of the European Union [TFEU]). Opinion 2/94 was issued on 28 March 1996.⁴ The CJ first emphasised that nothing in the Treaty conferred general power (express or implied) to the EC to issue human rights standards or conclude international agreements in this field.⁵

¹ Memorandum on the Accession of the European Communities to the Convention for the Protection of Human Rights and Fundamental Freedoms, COM/1979/0210 final.

² Communication of 19.11.1990, SEC (90), I 087 final.

³ Krzysztofik, 2022, p. 126.

⁴ Opinion of the Court, 2/94, Admissibility of the request for an Opinion, ECLI:EU:C:1996:140.

⁵ Point 27.

The legal basis for accession to the ECHR is Article 235 of the EC Treaty (now Article 352 TFEU), which allows the EC to legislate under its so-called complementary competence. According to the CJ, the modification of the rules for the protection of human rights in the Community resulting from accession to the ECHR would have a systemic character for the Community and for the Member States and, by its nature, would go beyond the scope of Article 235.⁶ In the legal state of affairs at the time, the CJ found no legal basis for EC's accession to the ECHR. It is worth noting that the Treaties of Amsterdam and Nice, drafted shortly after this opinion, did not change the competence of the EU or EC to accede to the ECHR.

EU's accession to the ECHR was discussed by the European Convention working on the draft Treaty establishing a Constitution for Europe.⁷ Within the framework of the Convention, the Working Party on Fundamental Rights worked on the issue of the EU accession to the ECHR, recommending accession but drawing attention to several related problems.⁸ One was the issue of individuals' access to the CJ in the context of ensuring effective legal aid. Ultimately, the issue of EU's accession to the ECHR was dealt with in Article I-9(2) of the Constitutional Treaty (Treaty establishing a Constitution for Europe), which stated that the Union should accede to the convention.⁹ In doing so, it was emphasised that 'accession to the Convention shall not affect the Union's competences as defined in the Constitution'. The European Convention further elaborated Protocol No. 32 under the conditions of accession and Declaration No. 2, incorporated into the Final Act. However, the failure of the Constitutional Treaty did not lead to the demise of the idea of introducing into Union law a treaty basis enabling EU's accession to the ECHR. The obligation indicated in Article I-9(2) of the Treaty establishing a Constitution for Europe was fully incorporated into the Lisbon Treaty and, as Article 6(2) TEU, came into effect on 1 December 2009.¹⁰

⁶ Paragraph 35.

⁷ Treaty establishing a Constitution for Europe, OJ of the European Union, C 310, 16 December 2004.

⁸ Wyrozumska, 2007, pp. 51–52.

⁹ Treaty establishing a Constitution for Europe, OJ EU C 310, 16.12.2004.

¹⁰ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13.12.2007 (OJ C 306, 17.12.2007, pp. 1–271).

Shortly after the entry into force of the Lisbon Treaty on 11 December 2009, the European Council adopted the Stockholm Programme, envisaging early accession to the ECHR as essential for the EU.¹¹

It is worth noting that the Council of Europe also recognised the need for legal changes to enable the EU to accede to the ECHR since 2002. The Steering Committee on Human Rights (CDDH) submitted a check to the Committee of Ministers of the Council of Europe with suggestions for modifications to the ECHR, thus enabling EU accession. The CDDH believed that these modifications could be made either through a protocol amending the ECHR or through an accession treaty to be concluded between the Union on the one hand and State Parties to the ECHR on the other.¹² However, the CDDH favoured the second option in 2002. The EU still did not have a legal basis for accession to the ECHR; hence, the Council of Europe decided to amend only Article 59(2) and create a formal legal basis for the EU to be bound by it. This amendment was carried out under Protocol No. 14 of the ECHR.¹³ Therefore, from the perspective of the Council of Europe, the formal legal prerequisite for EU accession to the ECHR was guaranteed.

The entry into force of Protocol 14 to the ECHR coincided with the entry into force of the Lisbon Treaty and, in July 2010, the CDDH *Ad Hoc* Negotiating Group on EU accession to the ECHR began negotiating a draft agreement. In 2013, the CDDH has reached a preliminary agreement with the draft accession agreement.¹⁴ However, negotiations on agreements with the EU were prolonged. In December 2014, at the request of the EC, the CJEU issued Opinion 2/13 on the compatibility of the draft accession agreement with the treaties,¹⁵ and concluded that the draft was not compatible with EU law. Given the wording of Article 218(11) TFEU, according to which ‘In the event of a negative opinion of the Court, the

¹¹ European Council Conclusions, 10–11 December 2009.

¹² Explanatory Report to Protocol No. 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, amending the control system of the Convention, Strasbourg, 13.5.2004.

¹³ Protocol No. 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, amending the control system of the Convention (CETS No. 194), Strasbourg, 13.05.2004; Protocol entered into force in 1.06.2010.

¹⁴ Fifth Negotiation Meeting Between the CDDH *Ad Hoc* Negotiation Group and the European Commission on the Accession of the European Union to the European Convention on Human Rights, Final report to the CDDH, 10.06.2013, 47+1(2013)008rev2.

¹⁵ Opinion 2/13 CJEU (full), 18.12.2014, ECLI:EU:C:2014:2454.

agreement envisaged may not enter into force unless it is amended or the Treaties are revised', Opinion 2/13 blocked the accession process for several years. Only in October 2019. The Council expressed its commitment to the early resumption of negotiations and adopted additional negotiating directives to address the concerns expressed by the CJEU in Opinion 2/13. Since then, negotiations have focused mainly on aligning the 2013 draft accession agreement with the requirements indicated by the CJEU in Opinion 2/13.

During the intra-EU discussion on Opinion 2/13, the problems listed by the CJEU were divided into four baskets. Basket 1 comprises an EU-specific mechanism for proceedings before the ECtHR. Basket 2 covers interstate complaints and requests for advisory opinions against EU Member States. Basket 3 deals with the principle of mutual trust between EU Member States and the guarantee that EU accession to the Convention will not be affected. Basket 4 covers EU actions in the CFSP areas that are excluded from CJEU jurisdiction.

In practice, the issues in the CFSP sphere have triggered the most heated discussions within the EU. By 2022, EU Member States reached a provisional agreement on all issues raised by the CJEU in Opinion 2/13, with the exception of those concerning Basket 4 and ensuring the judicial review of EU acts in the CFSP. Meanwhile, the accession to the ECHR has also taken a political dimension. At the 4th Council of Europe Summit of Heads of State and Government in Reykjavik on 16–17 May 2023. The Council of Europe welcomed the unanimous provisional agreement on revised draft accession instruments as an important achievement in EU accession to the ECHR. The Council of Europe Heads of State and Government also stressed that accession would enhance the coherence of human rights protection in Europe and encourage the timely adoption of the agreement.

3. Treaty legal bases for EU accession to the ECHR

The legal basis for EU's accession to the ECHR should be sought in both the ECHR itself and EU law.

The ECHR is an international agreement addressed primarily to states, so accession to it by the EU, which is an international organisation, requires a separate legal basis. Within the framework of the Council of Europe, the legal basis was provided by Protocol No. 14 to the ECHR, which amended

the ECHR provisions by defining entities entitled to be bound by the Convention. According to the new wording of Article 59(2), the European Union may accede to this Convention. This provision establishes only a formal legal basis for the EU to bind itself to the ECHR but does not specify either the conditions for accession or the required institutional and procedural changes in the functioning of the human rights protection mechanisms established by the Convention. Therefore, the ECHR leaves it to the Council of Europe and EU member states to determine all conditions for accession and future EU membership in the Convention.¹⁶

From the EU side, the legal basis for accession to the ECHR is Article 6(2) TEU, according to which ‘The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms’. This provision also notes that ‘Accession to the Convention shall not affect the Union's competences as defined in the Treaties’. Article 6(2) TEU is supplemented by Protocol No. 8 of the Treaties and Declaration No. 2 relating to Article 6(2) TEU, which formulates certain conditions upon which the EU will accede to the ECHR. While Protocol No. 8 is an integral part of the Treaties (Article 51, TEU) and has the rank of primary law, Declaration No. 2 does not enjoy this status.¹⁷ It is evident from the content of this declaration that it was agreed upon by the Intergovernmental Conference and, thus, by all the signatory states of the Lisbon Treaty. It has no binding force, although it may have international legal significance in the interpretation of Article 6(2) TEU and Protocol No. 8. The Declaration may be regarded as an agreement concerning the treaty reached between all parties in connection with the conclusion of the treaty, which provides the context. Considering Article 31(2)(a) of the Vienna Convention of 23.05.1959 on the Law of Treaties, context is of vital importance for the interpretation of any treaty.

According to Article 1 of the Protocol, the accession agreement must reflect the need to preserve the specific features of the Union and Union law, particularly regarding:

- a) specific conditions for EU participation in ECHR monitoring bodies;

¹⁶ Explanatory Report to Protocol No. 14 to the Convention for the Protection of Human Rights and Fundamental Freedoms, amending the control system of the Convention, Strasbourg, 13.5.2004.

¹⁷ Kornobis-Romanowska, 2023.

- b) the mechanisms necessary to ensure that complaints by non-member states and individual complaints are correctly addressed against the EU or its member states, as the case may be.

Protocol No. 8 emphasises that accession would not affect the competences of the EU or the powers of its institutions. The accession agreement should also contain guarantees that nothing in it will affect the particular situation of Member States in relation to the ECHR, in particular the protocols to that Convention, measures taken by Member States by way of derogation from the ECHR in accordance with Article 15 and reservations to the ECHR made by the Member States in accordance with Article 57.

Furthermore, Protocol No. 8 expressly emphasised that the accession agreement would not affect the obligation not to submit disputes arising from the interpretation and application of EU law to procedures other than those regulated by the Treaties.

Declaration No. 2 emphasises that EU's accession to the ECHR should take place in such a way that the specific nature of the Union's legal order can be preserved. The Intergovernmental Conference stressed the existence of a regular dialogue between the CJEU and the ECtHR and indicated that this dialogue could be strengthened upon EU's accession to the convention.

When analysing the legal basis for EU's accession to the ECHR contained in EU law, the accession framework needs to be shaped in such a way that it does not lead to changes in the EU's competences or affect the powers of its institutions.¹⁸ This is required to comply with the principle of conferral, which is a fundamental structural principle of the EU. On the one hand, EU accession must not lead to a diminution in the competencies of the union. On the other hand, this should not be extended, particularly to human rights. Indeed, the Union still lacks general competence in the field of fundamental rights and cannot acquire such competence through accession to the ECHR.

EU's accession to the ECHR will be implemented through an international agreement concluded between the EU and the Council of Europe¹⁹. According to Article 218(8) TFEU, the decision on the conclusion of the agreement on the EU's accession to the ECHR will be taken by the Council, acting unanimously. The Council's decision in this regard will enter into force only after it has been approved by all Member States in

¹⁸ Bear, 2015, p. 10.

¹⁹ Grądzka, 2022, p. 184.

accordance with their respective constitutional requirements. The procedure for EU's accession to the ECHR involves the European Parliament, which provides consent for the agreement.

The parties to the future accession agreement will not be EU Member States, although the Treaty provisions validate the Council's decision to conclude the accession agreement, subject to its approval by all Member States in accordance with their respective constitutional requirements. Nevertheless, in accordance with Article 216(2), the accession agreement binds both EU institutions and their member states. In doing so, Protocol No. 8 strongly emphasises the obligation to structure the accession agreement in such a way that its provisions preserve the specific features of the EU and the law it creates. The specific features are, first and foremost, the autonomy of the Union's legal order and the multilevel nature of the EU system, understood as the division of competences and responsibilities between national authorities and bodies that exist within the Union and are regulated by its law.²⁰ Within the EU law system, the exclusive competence of the CJEU under Article 344 TFEU to settle disputes arising from the interpretation and application of primary and derived EU law assumes particular importance. The obligation to preserve the specific characteristics of the EU and EU law is quite well characterised in the jurisprudence of the CJEU, particularly in the *Kadi* judgment.²¹ This obligation means that an international agreement must not violate the competence structure set out in the Treaties, the exclusive competence of EU courts to decide disputes concerning the interpretation and application of EU law (including inter-state disputes) and the competence of national courts to rule on the interpretation and application of EU Law.²²

4. Determinants of accession to the ECHR in the context of the CFSP as formulated in Opinion 2/13

Opinion 2/13 was issued on 18.12.2014 at the request of the EC. The EC asked, 'Is the draft agreement on the accession of the European Union to the ECHR compatible with the Treaties?' The CJEU formulated in Opinion

²⁰ Opinion of Advocate General Juliane Kokott, 13.06.2014, Opinion Proceedings 2/13, paras. 157–159.

²¹ Joint cases C-402/05. P. and C-415/05. P., *Yassin Abdullah Kadi v Council of the European Union and Commission of the European Communities*, 16 January 2008.

²² Soltys, 2015, p. 40.

2/13 the key condition for EU's accession to the ECHR and the future regulation of relations between the EU, the ECtHR, and the Council of Europe. The proceedings before the CJEU were also of great interest to the EU institutions and Member States, which submitted their comments on, *inter alia*, the principles of the CFSP.

Advocate General Juliane Kokott presented her opinion on this matter.²³ It dealt with a number of issues emerging from EU's accession to the ECHR, but the Advocate General drew attention to two fundamental issues concerning the impact of accession to the ECHR on the functioning of the CFSP.

The fundamental question posed by the Advocate General was whether the Union's competence, particularly that of the CJEU, was sufficient to provide, in the field of CFSP, a level of legal protection that satisfied the requirements of Articles 6 and 13.²⁴ On the one hand, accession to the ECHR will have the effect that the EU will be obliged to comply with the fundamental rights guarantees of the ECHR and thus also the imperative of effective legal protection under Articles 6 and 13 of the ECHR in all areas of its activity, including the CFSP, from which the EU cannot derogate in any way. On the other hand, the CJEU has neither jurisdiction over the provisions of primary law relating to the CFSP nor over acts adopted on the basis thereof, with the exception of Article 275, paragraph 2, TFEU. This jurisdiction covers, first, the review of compliance with the so-called 'inviolability clause' (Article 40 TEU) and, second, actions for annulment brought by individuals (Article 263, fourth paragraph, TFEU) against restrictive measures adopted by the Council under the CFSP against natural or legal persons.²⁵

However, the Advocate General concluded that EU's accession to the ECHR can be achieved without the need to create new competencies for the CJEU. According to Article 19(1) TEU, the legal protection system of the Treaties is supported by two pillars: the courts of the Union and national courts. In the field of CFSP, there is no possibility of direct action before the Union courts (with the exception of Article 275(2) TEU), while national courts retain their competence to assess the actions of the Member States.²⁶

²³ Opinion of Advocate General Juliane Kokott, 13.06.2014, Opinion procedure 2/13, ECLI:EU:C:2014:2475.

²⁴ Para. 82.

²⁵ Paras. 83–84.

²⁶ Para. 96.

Indeed, Article 19(1) TEU obliges Member States to establish the necessary means of judicial review to ensure effective legal protection in the areas covered by union law and thus also in the field of CFSP. This avenue should be used by individuals who wish to submit judicial review acts, measures, or omissions falling within the scope of the CFSP and that affect them in any (and not only direct and individual) way.²⁷ Moreover, even when the CFSP is implemented by the institutions, bodies, or other organisational units of the Union in a manner which affects the individual directly and individually, any individual's avenue of recourse to the national courts is not foreclosed unless, exceptionally, he or she can find legal protection directly before the courts of the Union based on Article 275(2) TFEU.²⁸ In the view of the Advocate General, effective legal protection of the individual, as required by Articles 6 and 13 ECHR, can thus be ensured without the preliminary ruling competence and the monopoly of jurisdiction of the CJEU, as in matters relating to the CFSP, effective legal protection of the individual is provided partly by the Union courts (Article 275, paragraph 2, TFEU) and partly by national courts (Article 19(1), paragraph 2, TEU, and Article 274 TFEU).²⁹

The Advocate General also noted a difference in competence between the CJEU and the ECtHR. Following EU's accession to the ECHR, it will be incumbent on the ECtHR to examine all areas of Union law, as well as complaints brought by individuals and states on CFSP, and to determine possible violations of the ECHR for which the EU may be liable. By contrast, the Courts of the Union have limited powers in the field of CFSP, and it is, in principle, incumbent on the courts of EU Member States to provide effective legal protection in that field.³⁰ According to the Advocate General, the principle of autonomy of Union law does not prevent the EU from recognising the jurisdiction of an international court whose competence in a particular field is broader than that of the CJEU.³¹ First, conflicts of jurisprudence and threats to the supranational structure of the Union arising from the deliberate exclusion of the CFSP from that structure must be ruled out.³² In addition, the authors of the Lisbon Treaty

²⁷ Para. 98.

²⁸ Para. 99.

²⁹ Paras. 102–104.

³⁰ Para. 187–188.

³¹ Para. 191.

³² Para. 192.

consciously entrust the EU with the competence to accede to the ECHR without at the same time equipping the EU courts with the competence to decide on all issues arising from the functioning of the CFSP. Therefore, the authors of the Lisbon Treaty saw no contradiction between the severely limited jurisdiction of the Union's courts in CFSP and recognition of the jurisdiction of the ECHR as a result of EU's accession to it.³³ Moreover, the authors of the Lisbon Treaty relied on national courts as the second pillar of the EU's legal protection system, and it is incumbent on national courts to punish possible violations of the ECHR that could occur under the CFSP unless, exceptionally, the Union courts have jurisdiction pursuant to the second paragraph of Article 275 TFEU.³⁴

The EC presented a different argument during the proceedings before the CJEU. It proposed a broad interpretation of the terms used in Article 275, paragraph 2, TFEU of the term 'decision providing for restrictive measures against natural or legal persons adopted by the Council on the basis of Chapter 2 of Title V of the Treaty on European Union'. According to the EC, this provision encompasses not only CJEU's competence to rule on actions for annulment (Article 263 TFEU) brought by individuals against restrictive measures but also on actions for damages (Article 265 TFEU) and preliminary rulings by national courts in the field of CFSP.³⁵ Furthermore, it advocated the application of the possibility of legal protection of individuals in the field of the CFSP so that it covers not only acts within the meaning of Article 263, paragraph 1, TFEU, which has binding legal effects but also mere acts of fact, that is, acts without legal effects.³⁶

The EC also submitted that, when an act is attributed to the Union or to a Member State for the purpose of establishing responsibility under the ECHR, the same criteria should be applied within the Union. The Commission argues that the first sentence of Article 1(4) of the draft Accession Agreement fulfils this requirement by providing that a measure of a Member State is imputed to that state even if it implements Union law, including decisions taken under the TEU and TFEU.³⁷ Military operations

³³ Para. 194.

³⁴ Para. 195.

³⁵ The position of the European Commission is discussed in the Opinion of Advocate General Juliane Kokott, 13.06.2014, Opinion Procedure 2/13, ECLI:EU:C:2014:2475, paras. 86–91.

³⁶ Para. 86.

³⁷ Opinion 2/13 CJEU (full), 18.12.2014, ECLI:EU:C:2014:2454, para. 93.

under the CFSP are carried out by Member States and the acts of Member States are attributed to the concerned Member State, not the Union. In this way, the draft Accession Agreement ruled out the application to relations between the Union and its Member States of the case law of the ECtHR on the responsibility of an international organisation with regard to actions taken by a state to implement decisions of that organisation.³⁸

The CJEU did not share the views of the Advocate General or the EC in Opinion 2/13.³⁹ Regarding the CFSP, the CJEU noted that it only has jurisdiction to review compliance with Article 40 TEU and to review the legality of certain decisions provided for in Article 275, paragraph 2, TFEU. Therefore, it does not have general jurisdiction to review compliance with the law created in the CFSP, and some of the acts issued under the CFSP are not subject to the Court's judicial review.⁴⁰

Pursuant to Article 275 TFEU, the Court has jurisdiction to rule on actions brought under the terms of the fourth paragraph of Article 263 TFEU concerning the review of the legality of decisions providing for restrictive measures against natural or legal persons adopted by the Council based on Chapter 2 of Title V TEU. The CJEU rejected the broad interpretation of Article 275 proposed by the EC. Indeed, the Commission's position distinguished between acts that produce binding legal effects and those devoid of such effects. Acts producing binding legal effects constitute, to the extent that they may infringe fundamental rights, 'restrictive measures' within the meaning of Article 275, paragraph 2, TFEU and may therefore be the subject of an action for annulment before the EU courts. By contrast, acts that do not have such effects cannot be the subject of an action for annulment or a reference for a preliminary ruling. The only remedy available within the Union against such acts is an action for damages under Article 340 TFEU, as such an action is not, in the Commission's view, precluded by the first paragraph of Article 275 TFEU.⁴¹ EC's position broadly defined the scope of the CJEU's CFSP judicial review as covering all situations that could be the subject of action before the ECtHR. The CJEU commented on the EC's position by stating that it had not yet had the opportunity to define the exact scope of the limits of its CFSP competence.⁴²

³⁸ Para. 95.

³⁹ Opinion 2/13 CJEU (full), 18.12.2014, ECLI:EU:C:2014:2454.

⁴⁰ Para. 252.

⁴¹ Para. 99.

⁴² Para. 251.

Nevertheless, the position of the EC seems inappropriate for several reasons. First, Article 275 TFEU is an exception to the general rule that the CJEU does not have CFSP competence with the exceptions described in this provision. As exceptions are subject to restrictive interpretation, Article 275 TFEU should not be interpreted in an expansive manner. Second, Article 275 TFEU does not specify that the division of CFSP acts into acts that produce and do not produce binding legal effects. The provision only mentions acts providing 'restrictive measures'. Third, accepting the European Commission's argument would *de facto* lead to an extension of CJEU's adjudicatory powers and would, therefore, directly contravene the prohibition formulated in Article 6(2) and Protocol No. 8.

The CJEU ultimately refrained from interpreting Article 275 TFEU and contented itself by stating that it was sufficient to conclude that, in the current state of Union law, certain acts issued under the CFSP are not subject to judicial review by the Court.

The CJEU further noted that, in light of the draft agreement under assessment, the ECtHR would have the power to rule on the compatibility with the ECHR of certain acts, acts, or omissions taking place under the CFSP, including those with respect to which the CJEU has no jurisdiction to review their legality in light of fundamental rights.⁴³ Such a situation would entail entrusting the judicial review of those acts or omissions of the EU exclusively to a body external to the Union, even if that review was limited to compliance with the rights guaranteed by the ECHR.⁴⁴ Meanwhile, in Opinion 1/09, the CJEU noted that the jurisdiction to exercise judicial review of the acts, acts, or omissions of the EU, including in light of fundamental rights, cannot be entrusted exclusively to an international judicial body not embedded in the institutional and judicial framework of the EU.⁴⁵ This gave the CJEU reason to conclude that the envisaged accession agreement does not consider the specific characteristics of Union law with regard to the judicial review of the acts, actions, or omissions of the EU in the field of CFSP.⁴⁶

⁴³ Para. 254.

⁴⁴ Para. 255.

⁴⁵ Para. 256.

⁴⁶ Para. 257.

5. Possible solutions to the CFSP judicial review deficit following the EU's accession to the ECHR

The most significant problem emerging from Opinion 2/13 was the regulation of CJEU's competence on judicial review in the CFSP area. This problem was perceived in the doctrine of European law even before the Opinion.⁴⁷ CJEU's competence in this area of European integration is, in principle, excluded, and it may exercise it in the two cases indicated in Article 24(1) TEU and Article 275 TFEU:

- a. to monitor compliance with Article 40 TEU;
- b. control the legality of decisions by providing restrictive measures against natural or legal persons, adopted by the Council (Article 275, paragraph 2, TFEU).

The acts and activities of the EU that do not fall within the aforementioned provisions are not subject to judicial review by the CJEU. This primarily concerns the creation of EU military and civilian missions and their activities, which may indirectly lead to violations of fundamental rights. At the same time (according to the wording of Article 340 TFEU), the legal admissibility of submitting a dispute concerning these acts and activities to the judgment of another international court is questionable.⁴⁸ The CJEU made it clear in Opinion 2/13 that the EU could not accede to the ECHR or grant the ECtHR the ability to hear cases without prior involvement. A situation in which the CJEU is not the first to hear cases of fundamental rights violations arising from the actions of the EU and/or its Member States under the CFSP (analogous to the national system) would be unacceptable to the CJEU. Discussions within the EU on how to provide the CJEU with the jurisdiction to exercise judicial review of CFSP acts and actions have been ongoing since 2019. During this time, there have been several proposals to address this issue.

The first proposal was presented by the EC during the proceedings for Opinion 2/13 and implied an expansive interpretation of Article 275(2) TFEU. While the CJEU and Advocate General did not accept EC's position, the Court itself did not explicitly reject the Commission's argument, merely stating that it had no jurisdiction to review certain acts. In this way, the Court left room for an extensive interpretation of Article 275, paragraph 2, TFEU in the future, in the absence of treaty changes to its CFSP

⁴⁷ Baere, 2008, p. 183.

⁴⁸ Hillon and Wessel, 2022, p. 78.

jurisdiction. The lack of a clear position of the CJEU on an expansive interpretation of this provision has been noted by some EU Member States who, in the course of the discussions on providing the CJEU with the competence to exercise judicial review in the area of the CFSP, have proposed the adoption of an intergovernmental declaration by all EU Member States. This declaration aims to extend CJEU's CFSP jurisdiction to cases of violation of fundamental rights caused by acts, actions, or omissions of the European Union, which will be subject to judicial review by the ECtHR after EU's accession to the ECHR. This would enable the legal impasse following Opinion 2/13 to be overcome without amending the EU Treaties. Based on such an intergovernmental declaration, the CJEU would acquire, in the field of CFSP, the competence to hear complaints brought by those who claim to be victims of fundamental rights violations caused by acts or omissions of the European Union, which would be subject to judicial review by the ECtHR after the Union's accession to the ECHR. According to the declaration, the Treaties would allow complainants who have standing to bring an action before the ECtHR to bring an action before the CJEU based on Article 263 TFEU (action for annulment) or Article 268 TFEU (action for damages).

When assessing a proposal to make an intergovernmental declaration, attention should first be paid to the legal form and procedures for the adoption of such a declaration. The declaration would be intergovernmental and would have to be agreed upon by the representatives of the Member States' governments. The EU practice is familiar with the format of the so-called Conference of Representatives of Member States, whereby, for example, in the margins of a COREPER meeting, CJEU judges are elected (under the Treaties, CJEU judges are appointed by common agreement by the governments of Member States). By means of a declaration accepted in the margins of COREPER, a rotating system for the election of CJEU Advocates General was adopted. Each of these declarations is of technical nature and serves to implement the treaty provisions (election of CJEU judges) or clarify their application in practice (rotation system for the positions of Advocates General). However, none of these declarations led to a *de facto* modification of the treaty provisions or an extension of the competences of EU institutions. Further, none of the abovementioned declarations adopted by the Conference of Representatives of Member States dealt with such an important issue as the extension of the jurisdiction of the CJEU to areas which, until now, according to the unanimous will of

Member States, were excluded from its jurisdiction. Articles 344 and 275 TFEU reveal the preference to exclude CFSP cooperation from any judicial proceedings, rather than a wish to ensure a uniform interpretation of the CFSP by the CJEU. Such a state of affairs should potentially be considered a specific feature of the Union's legal order. Article 1 of Protocol No. 8 of the Lisbon Treaty on Article 6(2) TEU on the accession of the EU to the ECHR dictates that the agreement applicable in this regard must reflect the need to preserve the specific features of the Union and Union law.

It is not clear whether an intergovernmental declaration takes the form of a reservation, an interpretative declaration, or another type of declaration. International practice is generally familiar with two types of declarations made by States or international organisations which have the effect of modifying treaty obligations. These are reservations and interpretative declarations.⁴⁹ Reservations may be made upon signature, ratification, acceptance, approval, or accession to a treaty, and have the effect of excluding or modifying the legal effect of certain provisions of a treaty in their application to that state or international organisation.⁵⁰ The time limitation for reservations precludes an intergovernmental declaration from taking this form. As the Declaration is intended to modify the jurisdiction of the CJEU, it should be attached to the TEU and TFEU, not to the Accession Agreement.

An interpretative declaration is a unilateral declaration, however phrased or named, made by a state or by an international organisation, whereby that state or organisation purports to clarify the meaning or scope attributed by the declarant to the treaty or to certain of its provisions.⁵¹ The character of a unilateral statement as a reservation or interpretative declaration is determined by the legal effect that its author purports to produce, and an interpretative declaration does not purport to exclude or modify the legal effects of any provision of the treaty in its application to the reserving state.⁵² The interpretative declaration can be made jointly by

⁴⁹ Sozański, 2005, p. 74.

⁵⁰ See Article 2(1)(d) Vienna Convention on the Law of Treaties of 23.05.1969 and Article 2(1)(d) Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations, 21.03.1986, United Nations publication, Sales No. E.94.V.5.

⁵¹ Guide to Practice on Reservations to Treaties, Yearbook of the International Law Commission, 2011, vol. II, Part Two.

⁵² *Idem*.

several states or international organisations and may be formulated at any time.⁵³

An intergovernmental declaration extending CJEU's CFSP jurisdiction can take the form of an interpretative declaration. However, it does not have binding force. Therefore, it could not effectively extend the jurisdiction of the CJEU into the areas of cooperation covered by the CFSP and would not fulfil the conditions indicated by the CJEU in Opinion 2/13.

The 1969 Vienna Convention on the Law of Treaties provides another solution to the nature of an intergovernmental declaration, which extends the jurisdiction of the CJEU. Article 31(3)(a) allows for subsequent agreements between parties concerning the interpretation of the treaty or the application of its provisions. Such agreements should be considered when interpreting treaties. Ultimately, however, given the specific and unique features of the EU legal order, it will be the CJEU to determine whether such a statement should be considered and to determine the meaning to be given to it, given that it was agreed upon by the signatories to the treaties. In this regard, the CJEU has already agreed to consider statements as instruments of interpretation of EU Treaties,⁵⁴ although it has confirmed that it has no jurisdiction to review the legality of such statements.⁵⁵ The CJEU has also emphasised the political nature of such declarations and stressed that recourse to them can only be made under very specific circumstances.

The amendment of the treaties forming the basis of the EU by means of an intergovernmental declaration must be assessed critically, as it is not mentioned in Article 48 TEU, which introduces mechanisms for amending the founding treaties. While such a procedure is not impermissible under the provisions of the 1969 Vienna Convention on the Law of Treaties, in practice, it will mean that the treaties forming the basis of the EU would be modified by a declaration attached to the 'ordinary' international agreement under which the EU accedes to the ECHR. This creates a precedent that could be used in the future to amend the treaties constituting the basis of the EU in a non-treaty mode unknown to Article 48 TEU. Since the treaties explicitly exclude the jurisdiction of the CJEU in the CFSP and introduce only two exceptions, the jurisdiction of the CJEU should be extended to new areas of the CFSP through the procedure indicated in Article 48 TEU.

⁵³ *Idem.*

⁵⁴ C-135/08, *Janko Rottman v Freistaat Bayern*, 02 March 2010, § 40.

⁵⁵ C-684/20 P, *Eleanor Sharpston v Council of the European Union*, 16 June 2021, § 45.

An extension of the concept of an intergovernmental declaration extending the competence of the CJEU is the call for the development of an administrative procedure whereby the Council can hear complaints arising from the acts and actions of states under the CFSP, which violate the fundamental rights granted by the ECHR. A unilateral EU declaration attached to the accession agreement clarified that this procedure should be used to exhaust internal EU remedies. The concept is that a provision would be added to each decision establishing a military or civilian mission to regulate the administrative procedure in which the Council would be empowered to hear the complaints arising from CFSP actions. Once a complaint is received, it is addressed by a Council decision; a Council decision to accept or reject the complaint is subject to appeal before the CJEU. Failure by the Council to make a decision within the set time limit would be tantamount to the Council rejecting the complaint, thus opening the way for legal proceedings before the CJEU.

The main reason for this idea is that an administrative procedure would allow for the control of Council acts and actions on CFSP matters. Such a procedure would also occur without prejudice to subsequent judicial review. The argument against it is that the Council would acquire *quasi-judicial* competence, whereby it would be given the competence to receive complaints from individuals and to adjudicate violations of fundamental rights. However, these competencies are not available to the council under the functions currently conferred on them. Under Article 16 TEU, the Council has legislative and budgetary functions, as well as policymaking and coordination functions. The transfer of new competencies will lead to a change in the existing competencies of this body, which is prohibited by Article 6(2) TEU and Protocol No. 8.

A third proposal discussed within the EU to address CJEU's lack of jurisdiction in the CFSP was the concept of so-called 'reattribution of responsibility'. This implies the attribution of responsibility to a given EU Member State for a specific CFSP act based on legal fiction. However, this concept did not gain the support of EU Member States, inter alia, because of the high complexity of the possible procedure in practice and the difficulty in foreseeing its material and political consequences. It also did not gain support among the non-EU Member States of the Council of Europe.

The lack of consensus preventing EU's accession to the ECHR on resolving the deficit of judicial review of CFSP acts and actions should prompt Member States to return to the simplest way of resolving this issue.

As there is no consensus among EU Member States to amend the Treaties and extend the jurisdiction of the CJEU to acts and actions carried out under the CFSP, it would be appropriate to revert to the already existing treaty-based mechanisms for the control of respect for human rights, as described in Article 19(1) and (2) TEU, and to entrust the national courts of Member States with jurisdiction over CFSP matters that do not fall within the jurisdiction of the CJEU. This solution is supported by the doctrine of European law.⁵⁶ Ultimately, what remains is the procedure for amending the Treaties in Article 48 TEU, which would either give the CJEU new competence in the field of CFSP or repeal the provision obliging the EU to accede to the ECHR. The latter idea does not seem unreasonable, given that the EU has given binding force to the Charter of Fundamental Rights and obliged not only its institutions and bodies but also (albeit only to a limited extent) Member States to comply with it. The Charter has also established a link between the fundamental rights derived from it and the human rights guaranteed by the ECHR. After 2009, CJEU has developed a rich case law on the understanding and scope of individual fundamental rights.

6. Completion

The process of accession to the ECHR has shown that the introduction of an explicit legal basis in the treaties authorising the EU to do so has proven insufficient and created new problems which have in turn proved difficult to solve in practice. The idea of a non-binding intergovernmental declaration that has the strongest support among member states may not be sufficient. As the CJEU wants to remain the primary court to adjudicate on issues of respect for human rights arising from acts and actions implemented under the CFSP, it may not be content to grant it legally dubious competence or attempt to block accession to the ECHR until the Treaties are amended and it is granted jurisdictional competence covering the entire CFSP. In this respect, it is puzzling why the CJEU rejected the idea of entrusting national courts with the adjudication of cases of fundamental rights violations during military and civilian missions.

The current legal impasse does not serve any individual, that is, neither Member States who are unable to fulfil their obligation of EU accession to the ECHR nor individuals who may be deprived of judicial legal protection.

⁵⁶ Soltys, 2015, pp. 41–42; Hillon, Wessel, 2022, p. 77.

Bibliography

- [1] de Baere, G. (2008) *Constitutional Principles of EU External Relations*. Oxford: Oxford University Press.
- [2] Grądzka, I. (2022) 'Perspektywy przystąpienia Unii Europejskiej do Europejskiej Konwencji Praw Człowieka i Podstawowych wolności' in Krzysztofik, E., Maksymiuk, M., Tarczyński, D. (eds.) *Unijny system ochrony praw człowieka wobec współczesnych wyzwań*. Lublin: Episteme, pp. 179-195.
- [3] Hillon, C., Wessel, R. A. (2018) 'The Good, the Bad and the Ugly': three levels of judicial control over the CFSP', in Blockmans, S., Koutrakos, P. (eds.) *Research Handbook on the EU's Common Foreign and Security Policy*. Edward Elgar Publishing, pp. 65-87.
- [4] Kornobis-Romanowska, D. (2023) 'Commentary on art. 6 TEU' in Grzeszczak, R., Kornobis-Romanowska, D. (eds.) *Treaty on the European Union. Commentary*. Warsaw: Wolters Kluwer, 2023.
- [5] Krzysztofik, E. (2022) 'Ewolucja i struktura unijnego systemu ochrony praw człowieka' in Krzysztofik, E., Maksymiuk, M., Tarczyński, D. (eds.) *Unijny system ochrony praw człowieka wobec współczesnych wyzwań*. Lublin: Episteme, pp. 119-139.
- [6] Niedźwiedź, M. (2015) 'Ochrona prawna w obszarze Wspólnej Polityki Zagranicznej i Bezpieczeństwa UE: rozważania w świetle opinii Trybunału Sprawiedliwości 2/13 z 18 grudnia 2014 r. (cz. I)', *Europejski Przegląd Sądowy*, 8, pp. 4-11.
- [7] Niedźwiedź, M. (2015) 'Ochrona prawna w obszarze Wspólnej Polityki Zagranicznej i Bezpieczeństwa UE: rozważania w świetle opinii Trybunału Sprawiedliwości 2/13 z 18 grudnia 2014 r. (cz. II)', *Europejski Przegląd Sądowy*, 9, pp. 14-19.

-
- [8] Soltys, A. (2015) 'Kontrola sądowa w zakresie Wspólnej Polityki Zagranicznej I Bezpieczeństwa w świetle opinii Trybunału Sprawiedliwości 2/13', *Europejski Przegląd Sądowy*, 12/2015, pp. 40-44.
- [9] Sozanski, J. (2005) *Współczesne prawo traktatów*. Warszawa-Poznań: Polskie Wydawnictwo Prawnicze Juris.
- [10] Wyrozumska, A. (2007) 'Traktat Reformujący UE – umocnienie ochrony praw podstawowych (status Karty Praw Podstawowych i przystąpienie UE do EKPCz)' in Barcz, J. (ed.) *Traktat reformujący Unię Europejską. Mandat Konferencji Międzyrządowej – analiza prawno-polityczna. Wnioski dla Polski*. Warszawa.
- [11] Guide to Practice on Reservations to Treaties (2011) *Yearbook of the International Law Commission*, vol. II, Part 2.
- [12] Vienna Convention on the Law of Treaties of 23.05.1969, United Nations, *Treaty Series*, vol. 1155, p. 331.
- [13] Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations, 21.03.1986, United Nations Publication, Sales No. E.94.V.5.

JAN MAZAL*

Defence capability development optimisation**

Abstract: This article outlines comprehensive research methodologies and practical outcomes aimed at enhancing strategic decision-making processes in defense capability development. It introduces a structured and applicable methodological framework that integrates theoretical principles, advanced technological approaches, and practical experiences. Central to this framework are advanced modeling and simulation techniques, specifically constructive wargaming and operations research methods. These techniques systematically integrate a set of capability optimization tasks exploiting detailed mathematical modeling and simulation, supported by specialized software tools. The article outlines thirteen conceptual steps for optimizing military force structures and capability configurations by evaluating a vast array of combat scenarios by operational effectiveness criteria within established financial and strategic constraints. The proposed framework is the subject of serious research activities and a defense project development aimed at enhancing the practical applicability of the described methods and approaches to computer-aided capability development processes, effectively supporting strategic planning and substantially improving overall military preparedness.

Keywords: Capability planning, operational optimization, constructive wargaming, military capabilities, armed forces development.

1. Introduction

In the wake of rapid scientific and technological advancements, new opportunities and abilities have emerged. Strategic management staff can implement advanced methods and components in real time over large datasets, such as advanced analyses, modelling and simulation (M&S) tools,

* COL, GS, Doc, Dipl. Eng., PhD., Chief of the Military Robotics Department, University of Defence, Brno, Czech Republic. <https://orcid.org/0000-0001-5741-558X>, jan.mazal@unob.cz.

** The research and preparation of this study was supported by the Central European Academy.

operations research optimisation approaches, machine learning technologies, and artificial intelligence (AI) tools, to support optimal decision-making and maintain business competitiveness, public administration, research and technology domains or other areas, particularly in the military.

Armed forces' optimal strategic management and development planning processes are typically complex, driven by various factors, primarily uncertainty surrounding the future security environment and evolution of military technology. Traditionally, strategic decisions in the military domain are influenced by human experience; nevertheless, scientific progress now offers advanced opportunities for strategic decision-making activities that optimise features such as configurations, operational efficiency, available time, minimising material/human resources, cost, etc.

Planning and developing armed forces' capabilities⁵⁰⁷ has a decisive impact on the state's defence and formation of regional, i.e. global security environment⁵⁰⁸. Generally, all defence resorts ask the same fundamental question: 'How should armed forces maintain operational effectiveness at the highest possible level annually and in the long term'?

The need for a prompt response (to that question) is amplified by the growing complexity and dynamics of the future battlefield, as well as the need to choose an appropriate focus for (modern/future) technological development. Considering that this decisive technology could take decades to evolve, any mistake in that field could have dramatic outcomes.

The contemporary planning process faces several pitfalls, which can be characterised as follows:

- the planning process at the strategic level primarily uses an empirical–intuitive approach, which expeditiously reaches hypothetical boundaries: even with increased efforts, it is not possible to achieve an outcome close to the 'theoretical optimum', which is attributable to the so-called 'shallow' state space investigation of possible configurations;
- another complication in problem-solving related to 'military capabilities' is the inconsistent level of perception, because variations in identifying significant areas across different countries⁵⁰⁹ create hurdles in their development;

⁵⁰⁷ MO CR 2002, MO CR 2018, MO CR 2019.

⁵⁰⁸ MO CR 2015, MO CR 2019, MO CR 2017.

⁵⁰⁹ Procházka, 2018, p. 106, 112.

- ‘capability’ according to the order of the Czech Ministry of Defence No. 66/2012 Bulletin⁵¹⁰, is defined as ‘a set of necessary characteristics of an individual, organisational unit, task force or system characteristics (e.g. weapons) to create the desired effect (e.g. completing a combat mission, achieving a goal). Abilities can acquire quantitative and qualitative attributes and can be characterised as ‘hierarchised’ (divided into orders or levels, progressively choosing the degree of aggregation). Therefore, the description provided is general and has vast scope for interpretation.

This implies an increased need for further elaboration (solution) of the given issue and eventual implementation of innovative or standardised approaches covering the given area. From the perspective of effective skill implementation or force planning, it is generally accepted that seeking rationalised approaches in all military areas is necessary. In practice, ‘optimisation’ efforts encounter several challenges, such as:

- high complexity and uncertainty surrounding the environment affected by the solution;
- insufficient knowledge among strategic (defence) personnel regarding modern technology and advanced methodologies;
- high administrative congestion of responsible staff hindering the investigation and development of alternative solutions;
- inclination to establish and adhere to ‘old-fashioned’ bureaucratic procedures;
- capability planning process is part of a complex procedural legislative framework, making adjustments innately challenging;
- lack of specialised SW solutions adapted to the specific problem;
- possibly others.

These factors contribute to the high degree of conservatism and sluggish and ‘alibi’ procedures that are usually used, which limits the implementation of advanced techniques in military capability evolution and armed forces development. A similar challenge was identified within the NATO STO SAS-164 working group, which deals with 21st-century Force Development (2020–2022).

This paper presents an algorithm-based methodological framework for strategic decision-making processes, presented several times (by the author) within the North Atlantic Treaty Organization (NATO) CA²X² Forum. It

⁵¹⁰ RMO 66 – Czech Ministry of Defence. Prague, 2012, p. 3.

drew the attention of governmental institutions, particularly in Germany, Italy and France, because such solutions have yet to be applied. The philosophy behind the solution assumes that computer support could dramatically improve the quality of the solution, driven by the large number of options explored and calculations necessary to determine an optimal solution.

There are various ways to optimise the development of armed forces' capabilities. One of the approaches suggests solution based on searching for the armed forces' optimal 'configuration-investment' strategy to maximise operational efficiency (OE) within the selected financial framework in the set period. Finally, the transformation of these structures into a capability model is addressed. A possible solution with a high degree of approximation includes the initial mathematical apparatus, structures and relationships, quantifying key factors and specifying criteria for the solution through a mathematical algorithmic approach to modelling the problem and searching for optimal configuration via the vast set of simulations.

2. Current status of advanced M&S tools in military planning

Advanced M&S tools are primarily used for education, research and development. The use of simulations is almost limitless; every procedure and process can be modelled and reproduced using appropriate simulation methods. However, they are rarely used in the military for complex process optimisation. M&S tools are used for planning and decision support in the army, e.g. in military operations^{511,512}. An analysis of operational research activities during the 'Enduring Freedom OEF and Iraqi Freedom OIF' showed that modelling and simulation were used only to a limited extent, because sophisticated computational models were difficult to calibrate to a specific situation, rendering them ineffective in the process of planning operations.

In a report⁵¹³, Hanley et al. identified only two modelling and simulation applications applicable to operational planning. These include the 'Peace Support Operation Model (PSOM)' application for evaluating force deployment plans and 'ATHENA' application used by experienced intelligence analysts to predict the potential outcomes of complex operations

⁵¹¹ Connable, 2014.

⁵¹² Veldhuis, 2020.

⁵¹³ Hanley, 2011.

in problem areas of the world⁵¹⁴. In planning, NATO uses a system analysis tool that is part of the Toolkit for Planning Operations, Force Activation and Simulation. In recent years, NATO has witnessed a renewed interest in planning missions and operations using simulations, as evidenced by several research working groups ((MSG-088, MSG-124, and MSG-155)⁵¹⁵.

The national armed forces of NATO member states, such as the Dutch Armed Forces, employ qualitative modelling methods such as causal loop diagrams and analysis of relationships between variables using enriched loops (called MARVEL)^{516,517}. The MARVEL method shares some tools with other established techniques, such as the PSM SODA problem structuring method (creation and analysis of strategic options), system dynamics and fuzzy cognitive maps. In addition, the MARVEL method uses causal loop diagrams enriched with qualitatively labelled values and standardised equations, facilitating the analysis of the structure and behaviour of the model⁵¹⁸.

The German Armed Forces use modelling and simulation to digitise logistics, taking into consideration factors such as flexibility in the models. It is used to identify risks and vulnerabilities in the logistics chain⁵¹⁹. The German commercial military technology company ESG presents successful simulation and analysis projects. ESG proposes further lines of action, such as simulation-based analysis for optimising military supply systems. This data-driven decision support method (AnyLogic tool, Bundeswehr guidelines for simulation-based analysis and model-based documentation) focuses on critical questions such as the material and operational readiness of a system developed for the future, assuming certain parameters/factors and what improves system performance.

Reviewing operations research applications and military modelling capabilities include research on military training modelling and search for possible methodologies applicable to building trained forces⁵²⁰. The Training Force Sustainment Model is designed to assist Army Training Command in identifying critical resource and planning issues to meet training requirements, satisfying training demand efficiently and effectively.

⁵¹⁴ Chamberlain, 2013.

⁵¹⁵ Horne, 2017.

⁵¹⁶ Veldhuis, 2020.

⁵¹⁷ Barros, 2011.

⁵¹⁸ Veldhuis, 2015.

⁵¹⁹ Kleint, 2021.

⁵²⁰ Wang, 2005.

Effective force planning is essential for all organisations; for example, for Australian Armed Forces, having a sufficient number of people with the required competencies at a reasonable cost is critical in planning⁵²¹. For example, Markov chain-based methods, computer simulation, optimisation and system dynamics were used and compared in a review of applications for operations research in workforce planning and capability modelling of military forces⁵²². These methods focus on different aspects of managing and optimising force planning processes. The Markov chain theory is one of the most widely used mathematical tools for assessing a system's dynamic behaviour. A stochastic process with discrete time that can be used according to Markov chain theory is called Markov process⁵²³. In the case study 'The modelling of manpower by Markov chains-a case study of the Slovenian armed forces'⁵²⁴, Markov chain models are used for human resource planning by the Slovenian Armed Forces.

The paper *Military Impact of Canadian Operational Research and Analysis*⁵²⁵, refers to the CATCAM methodology developed to support planning in the Canadian Armed Forces. It enables defence planners to list the capabilities of the Canadian Armed Forces. Capability-based planning defines the target Canadian Armed Forces' capabilities to select the right mix of plans, people, equipment and activities, i.e. to optimise the Canadian Armed Forces' ability to perform the assigned tasks. A new cost model for the Canadian Armed Forces was developed in conjunction with CATCAM. While it is relatively easy to determine costs (on an annual basis) such as salaries, purchases and consumables, it is challenging to determine the actual incremental costs. They include support infrastructure, major equipment such as light armoured vehicles, rifles and computers that wear out over time and need to be replaced. The costs are also time-varying. Although it is still under development, the new strategic cost model represents a significant advancement in operational research and analysis (OR&A) and directly impacts complex decision-making. Many of the critical issues facing the Canadian Armed Forces relate to personnel. Personnel intake must correspond to the system's training capacity. Demographic modelling is commonly conducted to support OR&A, with

⁵²¹ Sharp, 2003.

⁵²² Wang, 2005.

⁵²³ Hron, 2018.

⁵²⁴ Škulj, 2008.

⁵²⁵ Evans, 2006.

extensive information databases supporting it. Mining this data and employing historically derived attrition and recruitment data allows dynamic predictive models to be developed. These models are used to shape force expansion plans.

Advancements in AI technology have opened vast opportunities and methodologies for application in the strategic decision domain. Generally, AI-driven tools can potentially analyse enormous and complex data sets to forecast threats, optimise resource allocation and enhance readiness for various scenarios. Machine learning algorithms can identify patterns in historical data to predict future conflicts, assess force deployment options and recommend optimal asset utilisation. AI is also integrated into war-gaming simulations, enabling military planners to explore multiple strategic outcomes and stress-test various courses of action.

A review of the application of advanced AI in defence identified a few cases, but none in military capability planning. This is contrary to documents such as national, NATO and EU strategies or concepts that encouraged or recommended AI in defence applications.

A real-world example is the US Department of Defense's Project Maven⁵²⁶, which employs AI to analyse drone footage and automatically identify targets, reducing the cognitive load on human analysts. Similarly, NATO is leveraging AI for predictive maintenance⁵²⁷ of military equipment, evaluating sensor data to anticipate mechanical failures and optimise logistics or operational aspects⁵²⁸. The UK Ministry of Defence has also launched the Defence AI Strategy, integrating AI into defence-enhancing capabilities like cybersecurity, intelligence analysis and battlefield decision support⁵²⁹. These applications highlight AI's critical role in the military, and

⁵²⁶ Available at: <https://www.defense.gov/News/News-Stories/Article/Article/1254719/#:~:text=Project%20Maven%20focuses%20on%20computer%20vision%20--%20an%20aspect%20of> (Accessed: 02 May 2024).

⁵²⁷ Available at: <https://www.mdpi.com/2076-3417/14/2/898#:~:text=Using%20cutting-edge%20technologies%20like%20data%20analytics%20and%20artificial%20intelligence> (Accessed: 02 May 2024).

⁵²⁸ Available at: <https://www.natofoundation.org/wp-content/uploads/2021/12/NDCF-Paper-Berger-NATO-and-Artificial-Intelligence-151121.pdf#:~:text=In%20a%20context%20where%20an%20enhanced%20AI%20adoption%20in%20the> (Accessed: 02 May 2024).

⁵²⁹ Available at: <https://www.ft.com/content/94d59a36-099a-4add-80d3-475127b231c7#:~:text=The%20UK%20armed%20forces%20will%20use%20artificial%20intelligence%20to%20predict> (Accessed: 02 May 2024).

support its broader application in the capability planning process presented in this paper.

3. Methodology and approaches to problem-solution

The decision-making process in the military usually fulfils management optimisation characteristics, like achieving goals with minimum cost or asset consumption or maximum achievement within an available budget, asset and force disposition. We could take inspiration or analogy from the Japanese management systems, which transformed the country into one of the most technologically-advanced and wealthiest countries in the world. Suppose, there is a method to quantify the decision/optimisation criteria and decision process model, the operations research methodology can be effectively applied, particularly multi-criteria optimisation, where individual criteria are 'encoded' within the objective function, to search for minimised or maximised solutions (input parameters). This solution represents the particular settings, steps or actions that bring maximal benefit within the individual decision. The modelling of complex decision problems typically spans more domains, seldom making the solutions straightforward and simple.

The solution described in this paper employs various methods from different fields intersecting the AI domain, including linear algebra, probability theory, statistics, random processes, operational art, algorithm development, modelling and simulation, operational research, linear, nonlinear and dynamic programming, graph theory, automation, AI and software engineering.

The solution architecture can be derived from the intuitive–logical framework of the operational performance graph consolidation and the search for optimal armed forces configuration (CAF) regarding the maximum resilience to future threats, but considering an 'optimal' investment plan that also fits within the anticipated defence budget.

Based on historical experience and indicators of the security environment's evolution, it is judicious to balance the armed forces to fulfil a range of capabilities, rather than solely relying on any 'alliance' that covers the rest of the undeveloped specialties. This is highly risky if the potential involvement would significantly harm the allays, and thus, a wide range of capabilities is preferred. This assumption is crucial in determining

the range of specialisations of the Armed Forces Elementary Construction Entity (ESU).

The solution (to the mentioned problem) is challenging and can be categorised into a tree of independent subproblems with diverse degrees of acceptable approximation. It can also be assumed that the final solution creates further accompanying problems. It is important to realise that the fundamental nature and importance of this approach focuses on discovering the operational configuration of the armed forces in each period (usually years). It highlights the personal and technical resources the armed forces should maintain annually, ensuring adequate combat performance in the future security environment.

There are various options to address this problem. An effective and logical approach is to focus on the development of elementary organisational structures (of the armed forces), constructing the state graph of all possible configurations over time (in individual years) and applying 'constructive wargaming'⁵³⁰ with a potential enemy. The result will be the mathematical graph (tree) populated with coefficients of OE⁵³¹, which subsequently enable the calculation (or estimation) of the financial costs of individual configuration variations.

A series of operational research methods (using dynamic programming) can be applied to the given graph to develop the optimal configuration of the armed forces (organisational structures) in relation to the anticipated threats and the amount of the planned defence budget.

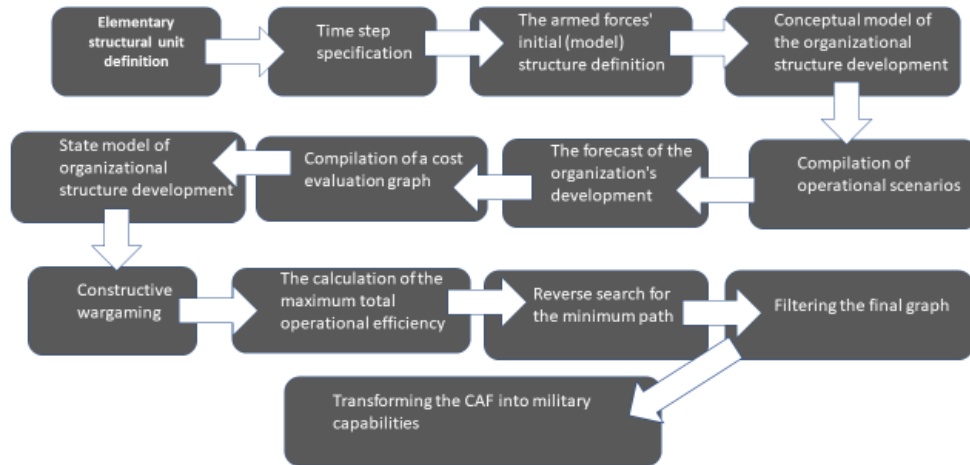
In the past, alternative approaches aimed to optimise capabilities first (instead of force configurations)⁵³², characteristic of a high degree of abstraction. This approach presents considerable challenges while quantifying the force configuration concerning military capability unambiguously. Transforming the armed forces' configuration into military capabilities is a straightforward, definitive process that logically supports the solution approach focused on modelling the construction of the armed forces in the initial phase, rather than reciprocal action (modelling the

⁵³⁰ Constructive wargaming is an area of computer simulation of armed conflict, which is based on models of warring parties, technical level and number of their units entities, conceptual or doctrinal models of combat, scenarios and the operational environment in which the conflict takes place.

⁵³¹ Operational efficiency reflects the level of ability to face the selected threat at a given time in a given territory, the threat in the case is represented by the enemy's armed forces in at least two variants, namely optimistic and pessimistic.

development of military capabilities). The solution architecture is demonstrated in Figure 1:

Figure 1 The solution process architecture.



As already mentioned, the problem of modelling armed forces architecture can be perceived as an optimisation task to maximise ‘OE’ in the context of the engagement of potential threats, while considering the constraints emerging from the planned defence budget. In this context, the following objective function of OE can be defined, describing a multi-criteria ‘compromise’ of priorities and constraints imposed on the solution. Considering the effort to maximise overall OE of the system of individual CAF configurations, it is imperative to ‘maximise’ the purpose function, with the fact that the cost in individual years must remain within the available resource plan (for the particular year):

$$\max \rightarrow \sum_{i=1}^n OE(DM_{KOS\ i}) \wedge FN(DM_{KOS\ i}) \leq ZDR_i \forall i \in \langle 1, n \rangle,$$

(1)

where

- $OE()$ – operational effectiveness function
 DM_{KOS} – data model of individual configurations, or the sequence of CAF in particular years,

$FN()$	– cost function configuration of the armed forces,
ZDR	– available resource framework in the corresponding year,
n	– total number of years,
i	– index.

The logically intuitive approach for the chosen problem solution illustrated in Figure 1, which aggregates armed forces architecture optimisation through the operations research methodology and M&S approach (constructive wargaming), is described in the following steps:

3.1. Elementary structural unit definition

Determining the elementary structural unit (ESU) of the armed forces organisational structure (initially, we recommend battalion level as the optimal choice for that purpose). This represents a pragmatic–logical compromise between practical resolution and computational operations for search and state space consolidation.

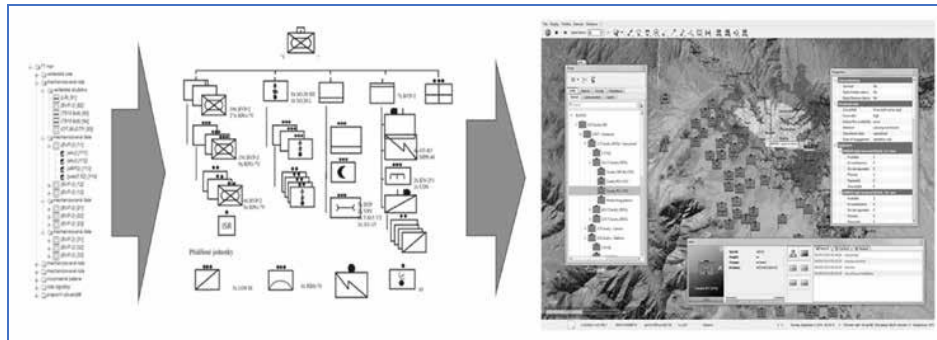
3.2. Time step specification

It is possible to determine a discrete time step for an ESU's evolvement or 'upgrade'. Given the length of acquisition processes and the defence sector's conservative development, it is likely that it may change in the future. The initial (discrete) time step can be set minimally for one year.

3.3. The armed forces' initial (model) structure definition

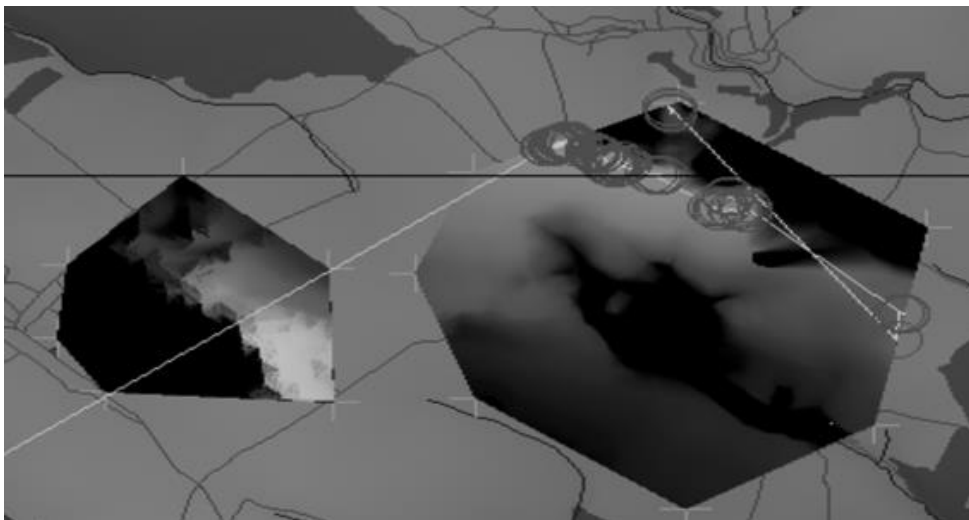
The armed forces' initial (model) structure has to be created from the ESU and its 'operational-efficiency calibration', which is based on its current state. It quantifies the coefficients of operational efficiency of individual components or systems within the organisational structure. In this case, the quantities and technical capabilities of ESUs are similar, instead of being appropriately arranged within the hierarchical structure of command and control (which may be a bit unusual for operational commanders, but necessary to simplify the process). A model example of the transformation of organisational structure into tactical entities in the synthetic environment is illustrated in Figure 2, reflecting the transformation of the (entity) data model (containing operational–tactical parameters) into organisational (hierarchical) infrastructure and then doctrinal deployment in a specific position in the simulation environment.

Figure 2 Example of data model transformation into organisational structures and basic tactical entities in the SWORD simulator.



ESU deployment is relatively complex, but can be addressed by geo-tactical analyses that support ESU's doctrinal behaviour in a particular operational situation. For example, Figure 3 could demonstrate the convenient observation/shooting positions identified with the intent to cover a particular area by ground observation or fire.

Figure 3 Observation optimisation.



3.4. Conceptual model of the organisational structure development

The organisational structure development conceptual model is primarily related to the ESU. It should determine possible generic options for ESU modifications within the organisational structure (in the context of individual ESU upgrades). Let us assume the following possibilities:

- ESU status remains unchanged;
- ESU status increased (incrementing - technological or organisational attributes);
- ESU is cancelled;
- A new ESU is created.

In the wake of rapid technological advancements, some ESUs could start at different times, and processes based on DTAG/CDAG (well-established in NATO) can potentially be used to identify configurations of these high-tech ESUs.

3.5. State model of organisational structure development

The next step is to create a state model of organisational structure development based on the conceptual model. It includes all possible configurations of individual ESUs within the selected time and a set of rules for discretising individual qualitative levels. The transition between adjacent ESU states is also limited to prevent the excessive expansion of option tree. In practice, ESU upgrades are long-term processes. The following options are expected to address the problem of state graph development of organisational structure variants:

The organisational structure⁵³³ model works with elementary units of the ESU, reaching the following states in the selected periods:

- incremental – additional resources and efforts are invested to enhance ESU quality (quality is increased by +1);
- stagnant – the ESU is maintained at current operational costs (the quality level does not change);
- destructive – the ESU is cancelled;
- constructive – a new ESU with a corresponding quality level is created.

⁵³³ For the purposes of the solution, it is primarily a flat organizational structure, focusing on individual battalions of combat forces, combat support forces and combat security forces.

The option of stepwise degradation of ESU is not considered within the modelling of the rules of ESU evolvement. This approach seems practically illogical, as it essentially involves the rearmament of the organisational unit (ESU) to a qualitatively lower level. In any case, prolonged stagnation could result in some degradation of ESU. If reducing maintenance cost of the ESU is the primary goal, it is effective to cancel the entire ESU and invest the saved funds in the development of other ESUs or for the creation of an entirely new ESU.

3.6. *Compilation of a cost evaluation graph*

The next step involves compiling a ‘shadow’ cost evaluation graph of all configuration transitions at time n to the state $n + i$, where i denotes a discrete time step. It is possible to calculate the financial demands of a particular armed forces configuration and determine whether a given strategy⁵³⁴ fits within the planned budget, see Figure 2. All transitions between individual discrete periods (ESU transformations) are necessary to assess their financial demands. It is worth noting that it is challenging to accurately quantify financial investments representing the relationship between the transformation of individual ESUs to higher quality levels. Each ESU can acquire specifics that cannot be easily generalised, or all the factors for accurate calculation are unknown. In any case, for the initial solution and automation of the vast configuration’s assessment, the cost could be empirically estimated or statistically evaluated based on previous experience of modernisation of individual capabilities. In case of further estimation improvement and simulation fidelity, an advanced algorithm can be developed, taking into account other circumstances. Considering the overall complexity of the realistic estimation, the initial approximative cost options can be calculated for the need for an expeditious initial solution, such as:

- Investments to enhance ESU quality.
- Investments to maintain ESU quality.
- Investments leading to ESU abolition.
- Investments to create a new ESU.

The advanced calculation algorithm necessary for the ‘debugging’ phase of the final solution should consider various variable conditions and

⁵³⁴ In this respect, the strategy means a path in the state graph of armed forces configurations.

environment development dynamics, especially investments in qualitative transformations of individual ESU across different years, which may not necessarily require the same amount of resources (the latter ESU upgrades will likely lead to ‘nonlinear’ spending increase, compared to previous years).

The following proposal can be used as one of the possible flat-rate approaches to calculate the costs of ESU transformations in individual years, which requires determining a matrix of coefficients in individual years (r-year, i-index ESU):

- Financial costs of transforming the ESU to a higher level of quality: $FTVKE_{ri}$.
- Financial cost of maintaining the quality level of the ESU: $FUKE_{ri}$.
- Financial costs of dissolving the ESU: FZE_{ri} .
- Financial costs of setting up the ESU: FVE_{ri} .

Consolidation of a (3D) RV matrix containing line vectors defining a transformation variant of the armed forces configuration (according to the conceptual model, individual components usually take values of 1 or 0). The total costs for a given year form the sum of linear combinations of the vector RV_{ri} , and other individual components of the transformation costs, according to:

$$FN_r = \sum_{i=0}^n (RV_{ri0} * FTVKE_{ri} + RV_{ri1} * FUKE_{ri} + RV_{ri2} FZE_{ri} + RV_{ri3} FVE_{ri}) , \quad (2)$$

where

FN_r - total investment costs for the year (for all ESU),

RV_{ri} - transformation vectors for each year and each ESU,

i - index of individual ESU,

R - index corresponding to individual years.

Based on the calculation of the financial complexity of the evaluation of individual configurations of organisational structures in the status chart, it is possible to calculate the total costs of all potentially promising and other 'investment strategies'¹, mainly those covered and not covered by the estimated budget. It is necessary to realise that the set of promising (perspective) and set of other investment strategies should be subjected to further analysis, as some other strategies may have significantly higher cost/benefit ratios (CBRs) than those in the promising set. Therefore, appropriate evaluation is vital. In particular cases, a marginal increase in the defence budget can exponentially influence the OE of the armed forces and the security environment.

3.7. Forecasting the organisation's development

The next step involves forecasting the development of the organisation's potential enemy (to increase the probability of estimating actual development), which is usually processed in several variants, between which the states can be interpolated. Creating a model of organisational structures of the presumed enemy should be based on a qualified forecast, or extrapolation of the current state of forces and resources in individual years (or periods). Considering the high level of uncertainty of any (especially long-term) socio-economic forecasts in the dynamic security environment, it is recommended to count on a minimally optimistic and pessimistic version of the prognosis. Professional models usually work with five or more options based on interpolation or separate estimates (advancement in particular capabilities, orientation to different types of combat, applied technology, level of command and control, etc.). The reason for processing multiple options of the enemy configuration is to obtain a comprehensive data set for determining the 'so-called' solution stability coefficient, which expresses resistance to multi-spectral threats. A comprehensive description of (organisational structures) model development of a potential enemy goes

¹ The investment strategy is a sequence of expenditures on the development of armed forces over time.

beyond the scope of this paper and acquires the character of a separate project.

The development of enemy organisational structures is a particular analogy to the process of the own structure's configuration elaboration and generation of possible ESU configurations in individual years. As we expect the development and integration of new units and capabilities on the friendly side, the enemy will develop, too, in many cases, with higher dynamics. A database of unit configurations is generated for our forces and the enemy concurrently and qualitatively over time. The pessimistic option of the enemy's development (from their perspective) is usually characterised by the fact that the qualitative development of the enemy's units (ESU) shifts over time (i.e. technological development is delayed).

3.8. Compiling operational scenarios

The next step involves compiling an array of operational scenarios (for our units and the enemy) and potential areas for their implementation. Creating operational scenarios and their automation is key to establishing the overall architecture of constructive 'wargaming' processes and their subsequent implementation. Operational scenarios should represent the expected operational spectrum of the use of the CAF and the means for securing the military-strategic objectives of the defence of a particular territory. It is necessary to highlight that the set of operational scenarios must be designed to verify the operational effectiveness of all possible configurations of CAF in combat activities with the presumed enemy. Therefore, the primary focus is not on determining an optimal (tactical) course of action, but rather evaluating the ability of personnel and technology to engage against enemy units. The operational scenarios model the assumed spatiotemporal structure of the assumed conflict in the operational domains like LAND, AIR, SEA, CYBER and potentially SPACE. Although the number of operational scenarios is not theoretically limited, it is preferable to restrict the number to a maximum of ten, ideally three, to achieve practical results in a reasonable time. The next step in the architecture of wargaming processes is to select locations for individual scenarios. It can theoretically be a large territory of the whole state or continent, but even parts can be selected as the most likely scenarios² (based on military-strategic goals of individual states) to

² In the study of military history, we frequently encounter cases highlighting some of the successes of risky 'operational' intentions and the surprise of a counterpart unprepared to fight in unlikely locations or a way of fighting that does not follow established convention.

reduce calculations significantly, thereby shortening the solution time. For example, the concentration of NATO member states' defence efforts in Eastern Europe, where the main defence focus is on the border with a potential enemy. In this regard, it is necessary to analyse the areas suitable for effective employment of the particular military capabilities or other potential (focus areas will differ if the enemy has a predominance of tanks or light combat units, etc.). Identifying the anticipated areas for military combat can be automated based on initial criteria imposed on the scenario and character of the operation through computer geographical analysis; in specific cases, areas can be identified empirically or intuitively. Generally, automated processing algorithms are in the initial stage and require further research; conversely, the conceptual methodologies are already well defined and can be found; for example, ATP 2-01.3 / 2019 (Intelligence Preparation of the Battlefield). A possible example of an algorithmic approach to this problem can be found in the publication^{3,4}.

3.9. Constructive wargaming

Another step is constructive wargaming of all configurations of CAF with the assumed enemy configuration (all options, minimally-optimistic and pessimistic) for each operational scenario and selected geographical area in a statistically representative amount (ideally a hundred times or more for each operational scenario). Evaluation and quantification of the 'operational efficiency' (OE) of each force configuration and substitution of the given coefficient (1/OE) into the mathematical graph of force development. For now, constructive wargaming is the only possible and logically acceptable main component of the rational evaluation of many operational courses of action (COAs). Automating all parts of the solution chain is necessary to calculate the solution's intended scope and depth.

For a statistically representative data sample necessary for the relevant assessment, it is vital to repeat each simulated alternative with moderately modified initial conditions (shifted location boundaries, different unit

This moment of surprise was usually based on the enemy's 'static-conservative' behaviour and its underestimation of ISR (Intelligence Surveillance and Recognition), with this factor already being used in today's globalised news (Internet, satellites, long-range radars and similarly), cannot be relied upon, although there are nevertheless some chances of deceiving the enemy and moving primarily to the cyber operational domain.

³ Mazal, 2012.

⁴ Mazal, 2010.

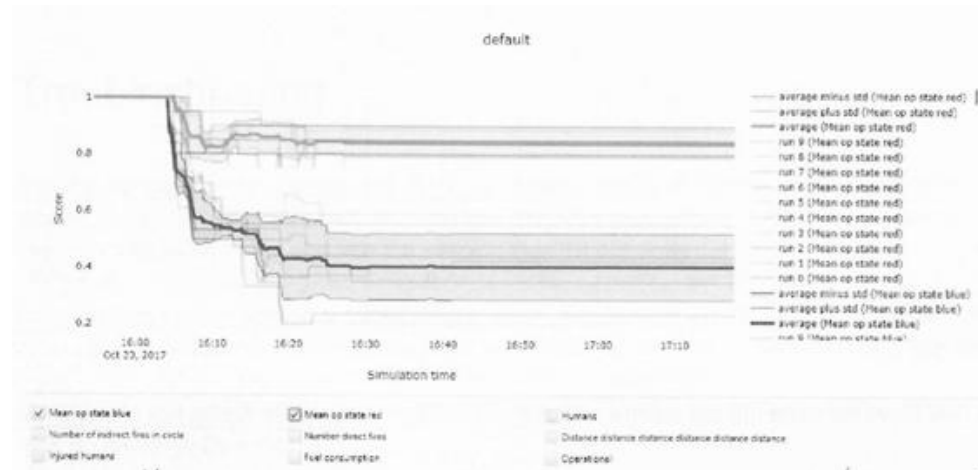
positions, etc.). Next, to increase the ‘stability’ of the solution, it is also important to choose the appropriate operational simulator, which should implement the appropriate degree of stochasticity already within the simulation. Essentially, two simulations with the same initial parameters in the operational dimension/environment do not have the same results as in real situations.

As mentioned, according to the statistical rules, it is recommended to repeat the simulation of the operating scenario at least 100 times (preferably 1,000 times or more) for all possible configurations. Based on the results of a large number of simulations, it is possible to perform its overall evaluation and quantification of ‘operational efficiency⁵’ (OE) of each organisational configuration and substitution of the coefficient $OE^{-1} = \frac{1}{OE}$ into the mathematical graph of force development⁶. Figure 4 demonstrates the development of losses (in time) of friendly forces and enemies within a series of simulations of one scenario using the operational simulator MASA-SWORD:

⁵ According to available information from MASA, the frequent use of SW SWORD is for analytical purposes of prepared acquisitions, which is in a way similar to the case described in this section (examination of operational efficiency of variant types of acquired technology in the entire operating spectrum of defined scenarios). The NATO working group – MSG-179 mentioned in the analytical part –also deals with the same topic.

⁶ In the graph of the development of the armed forces, the minimum path is then sought; therefore, it is necessary to substitute, for example, inverted OEx values, in this case we can initially choose OE^{-1} .

Figure 4 Graph of the percentage of losses of own units (blue) and enemy units (red)



The resulting analysis and determination of the coefficient of OE can take various approaches; for example, by a statistical mean value (from all simulations) of the original and final ratio of losses of friendly and enemy forces:

$$OE_{v1} = \frac{CP_v}{PP_v},$$

$$OE_{n1} = \frac{CP_n}{PP_n},$$

where

OE_{v1} – operational efficiency of friendly forces, variant no. 1

OE_{n1} – operational efficiency of enemy forces, variant no. 1

CP_v – final number of friendly forces,

CP_n – final number of enemy forces,

PP_v – initial number of friendly forces,

PP_n – initial number of enemy forces.

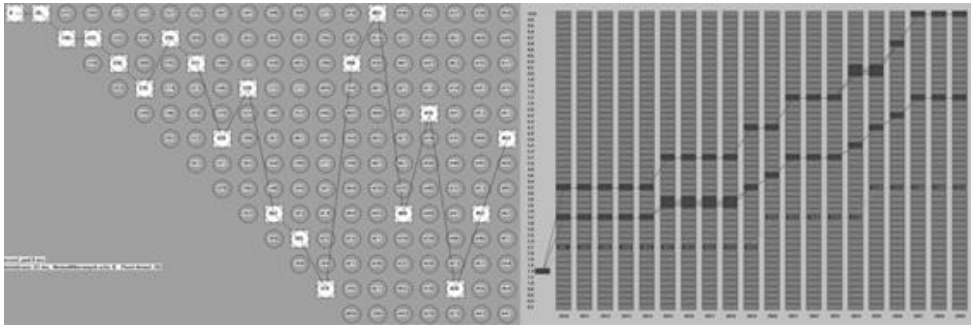
Selected criteria for the future development of the armed forces organisation depend on optimisation goals and strategic approach. Constructive wargaming, a simulation-based technique, offers a significantly higher fidelity of OE estimation compared to alternative model-based techniques. Wargaming simulations are critical for evaluating future technologies aggregated in particular tactical entities (tanks, BMPs, jetfighters, etc.) that has yet to be developed. They can estimate the future effectiveness or combat potential of this technology in advance, thereby contributing to technological evaluation and affecting military planning.

3.10. Calculation of maximum total operational efficiency

The next step is calculating the maximum OE of each node of the development graph of CAF (for each configuration). It uses, for example, the Critical Path Method (CPM), Dijkstra, or A* algorithm to determine the minimum path to each node in the directed mathematical graph (see Figure 4). The procedure for calculating the first part of the solution can be categorised into two phases. The first seeks optimal solution as a minimum path to each organisational structure configuration graph node through the minimal sum of OE coefficients (by storing $1 / \text{OE}$ values because the maximum total efficiency is pursued), while the financial cost of the given configuration is also calculated. The second (described further) is preceded by the solution stability analysis of the resulting graph, to determine an optimal sequence for the configuration of the CAF within a selected time period (usually decades). In principle, this is a multi-criteria problem solution based on the fusion of a modified CPM approach/method with other solutions or constraints. The problem solution is characterised by the primary factor of maximal OE pursued, which should usually be maximised from a long-term perspective. The same but secondary aim is followed for the financial demands of capability investments, which, according to the expected plan of the military budget, set restrictive limits for the development of the CAF and indirectly for capability development. Most prospective strategies (paths) can easily hit the financial limit. However, their total pragmatism ($\text{CBA} = \text{OE} / \text{financial costs}$) may be higher than the partial development strategies falling within the 'fundable' interval. Another important step is to determine the minimum financial cost of the target configuration of CAF, which can be calculated either during the 'forward' phase or within the second phase of the 'backward' search of the minimum path for each node of the graph or only for target nodes. Calculating the

minimal path for each node of the graph allows for greater depth in subsequent analysis, and the results can be subjected to further operations, such as the mentioned CBA, which is always recommended, at least for the final (fine-tuned) development models of the CAF.

Figure 4 *Demonstration of optimal investment strategies.*



3.11. Reverse search for the minimum path

According to the reverse search for the minimum path for all nodes of the graph (covering all CAF configurations), each configuration's minimum (total) financial demands can be calculated.

The final analysis of the CAF configurations graph and their OE in the context of the achievable maximum or acceptable level of defence is one of the key steps in the entire algorithmic framework. It primarily aims to determine whether the acceptable configuration in the target year/s is/is not achievable, the efficiency trend of optimal development of CAF in individual years (balanced, unbalanced) and whether this trend does not represent another risk (for example, initial concentration to technologies that will prove their effectiveness later and until then the defence system will not be sufficiently effective to face a potential threat). The search for optimal strategies (there may be more than one with the same total operational efficiency) for the development of the CAF is realised by selecting target configurations with the highest values of OE from those options that still fall within the area covered by the expected budget in individual years. In a situation where the financial limit for CAF development exceeds a state that would be able to counter the predicted threats effectively, it is possible to proceed inversely until the efficiency of the configurations of CAF reaches acceptable values. Secondly, the stability of the solution should be

analysed for each CAF configuration within the determined optimal configuration sequence. Stability analysis comprises processing differential characteristics of each configuration's neighbourhood values (surroundings) in the CAF development graph and assessing the development trend of OE coefficients around the target node. If the values around the target node differ significantly, it indicates a potentially unstable configuration, and it is necessary to prioritise the given strategy during subsequent evaluation (further analyses are usually needed).

3.12. Filtering the final graph

The final step is filtering the resulting graph into two parts of configurations. One can be financed within the assumed defence budget plan, while the other cannot. The necessary step is a final analysis of the (graph) CAF configurations and their OE in the context of achievable and acceptable level of defence. The efficiency trend of optimal development of CAF in individual years (balanced, unbalanced) should be analysed to determine whether this trend does not impose another risk (for example, initially focusing on technologies that prove their effectiveness much later, and until then, the defence system cannot effectively avert a possible threat).

3.13. Transforming CAF into military capabilities

A force configuration data model can be relatively easily transformed into a capability level model if the mapping vector function is known $FS()$, which extracts individual components from the armed forces configuration model according to:

$$MS = FS(DM_{KOS}) \quad (5)$$

MS – Capability Model

FS – Function to map the model of armed forces organisational structures to a capability level vector.

DM_{KOS} – Armed Forces Configuration Data Model

The capability model consolidates the states of individual capability levels developed within a given army/system, which express the corresponding coverage of a given capability by specific army 'components' (select units, command levels, special equipment, troop types, etc.) within

the components of ‘vector’ capabilities. The capabilities model can be defined as a linear data structure representing the levels of individual components of military capabilities, and the given structure is best represented by a mathematical vector.

The specific identification of individual military capabilities and possibly its other components (sub-capabilities) may differ within the particular NATO armies. Therefore, the data model represented by the vector is sufficiently generic and not constrained by the number of identified capabilities. However, the transformation of configuration of armed forces into capabilities depends on the definition of the FS() function, and is driven by the specifics of the individual capability components. It must be balanced in the context of national specifics.

3.14. Brief summary

The algorithmic framework demonstrates a variable degree of precision and complexity of individual parts. Even though the system concept of the solution theoretically follows purely logical steps leading to the desired solution, its practical implementation exposes various challenges and difficulties, primarily dependent on the fidelity of constructive wargaming and from the development of the security environment forecast (especially the enemy). To mitigate the negative factors of inaccurate estimates and error accumulation within one simulation, virtual experimentations are repeated several times, and operating environment forecast intervals (in which the experimentation takes place) are variably chosen, so that the resulting solution reaches the state space character of potential solutions rather than a specific option. In any case, the process transforms the spectrum of all possible cases to potentially promising ones, recommending that the set of perspective solutions should be further analysed. This aspect should be the subject of further research.

4. Conclusion

Computer support for decision-making processes at all levels of command is currently highly actual; it generally offers a significant increase in efficiency in various human domains, and with the rapid development of modern technologies, its importance continues to grow. This phenomenon is reflected in today's vast area of real applications, which were unthinkable several years ago.

The primary objective of this paper is to design a basic algorithmic framework (approach) for the armed forces' capability development and optimisation (implementing advanced approaches and tools from the field of modelling, simulation and operational research), which creates optional opportunities for its subsequent evolution within following projects or activities. In this context, a conceptual framework of individual steps was proposed, most of these steps represent a separate complex problem by itself. Potential solutions were described at the appropriate level of approximation, and some steps may be modified according to current needs or findings. From the perspective of overall operational performance, the key processes pursue the quantification of operational efficiency, where the most logical approach of constructive wargaming evaluation is applied. The quality of the final results depends on various aspects, potentially presenting another topic for future research.

From a pragmatic point of view, even the contemporary strategic planning process is complex and systematic. It lacks the vast state space search of potential strategic solution paths count, and no such alternative has been introduced yet to a presented concept architecture.

The main SW components and theoretical procedures are available for initial solution of the mentioned problem, and all that remains is to integrate them correctly. The correlation to the reality of the solution is highly dependent on several components, such as the fidelity of the wargaming simulations and the prognosis of future opponent evolution. This creates the centre of gravity of the potential future research and development of the presented concept.

However, the overall concept is very challenging, and its implementation is feasible over several years, and the research and development investment will undoubtedly yield positive outcomes.

Bibliography

- [1] Barros, A., Monsuur, H. (2011) 'Operationele analyse: Science at the frontline', *Militaire. Spectator*, 180, pp. 248-259.
- [2] Connable, B., Perry, W. L., Doll, A., Lander, N., Madden, D. (2014) *Modeling, simulation, and operations analysis in Afghanistan and Iraq: operational vignettes, lessons learned, and a survey of selected efforts* [Online]. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR382/RAND_RR382.sum.pdf (Accessed: 01 May 2024).
- [3] Škulj, D., Vehovar, V., Štampelj, D. (2008) 'The Modelling of Manpower by Markov Chains – A Case Study of the Slovenian Armed Forces', *Informatica*, 32, pp. 289-291.
- [4] Evans, J. R., Dickinson, R. G., Rey, M. (2006) *Military Impact of Canadian Operational Research and Analysis*. Paper presented to 23rd International Symposium on Military Operational Research, Hampshire, UK.
- [5] Hanley, N., Gaffney, H. (2011) 'The Peace Support Operations Model: Modeling Techniques Present and Future', *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 8(2), pp. 79-84 [Online]. Available at: <http://journals.sagepub.com/doi/10.1177/1548512910388200> (Accessed: 02 May 2024).
- [6] Horne, G., Seichter, S. (2018) *Developing Actionable Data Farming Decision Support for NATO*. Technical Report RDP STO-TR-MSG-124. Neuilly-sur-Seine: NATO Research and Technology Organisation [Online]. Available at: [https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-MSG-124/\\$\\$TR-MSG-124-ALL.pdf](https://www.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-MSG-124/$$TR-MSG-124-ALL.pdf) (Accessed: 01 May 2024).

-
- [7] Fačevicová K., Hron K., Kunderová P. (2018) *Markovovy řetězce a jejich aplikace*, Univerzita Palackého v Olomouci. 7. 12. 2018
- [8] Chamberlain, R. G., Duquette, W. H. (2013) *Athena in 2013 and Beyond*. JPL Publication 13-9, Pasadena: Jet Propulsion Laboratory, CA 91109-8099.
- [9] Kleint, R., Geck, A. (2021) *Simulation-Based Decision Support for the Logistic System of the German Armed Forces* [Online]. Available at:
<https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-184/MP-MSG-184-13.pdf> (Accessed: 02 May 2024).
- [10] Mazal, J., (2009) Algoritmy vlivu geografických faktorů na optimální pohyb vojenských vozidel po komunikacích i v terénu (in Czech), projekt obranného výzkumu METEOR, UO Brno, pp. 87.
- [11] Mazal, J. Stodola P., Mašlej M., Rybanský M. (2012) *Integration of The Geographical and Operational Analyses*. Brno: Univerzita obrany.
- [12] MO ČR (2002) *Koncepce výstavby profesionální Armády České republiky a mobilizace ozbrojených sil České republiky*. Praha: Ministerstvo obrany.
- [13] MO ČR (2015) *Bezpečnostní strategie České republiky*. Praha: Ministerstvo zahraničních věcí České republiky.
- [14] MO ČR (2017) *Obranná strategie České republiky: The defence strategy of the Czech Republic*, Praha: Ministerstvo obrany České republiky - VHÚ Praha.
- [15] MO ČR (2018) *Metodika střednědobých koncepcí*. Usnesení vlády ČR č. 10 ze dne 3. 1. 2001. Metodická pomůcka: Tvorba koncepčních dokumentů rezortu MO.

-
- [16] MO ČR (2019) *Koncepce výstavby Armády České republiky 2030*, Praha: Ministerstvo obrany.
- [17] MO ČR (2019) *Dlouhodobý výhled pro obranu 2035: The defence strategy of the Czech Republic*, Praha: Ministerstvo obrany České republiky - VHU Praha.
- [18] Procházka, J. (2018) *Strategické přístupy k adaptaci ozbrojených sil: tvorba rozvojových strategií: habilitační práce*, Brno: Univerzita obrany v Brně.
- [19] Sharp, P. (2003) *Report of the strategic workforce planning review*. Canberra ACT: Commonwealth of Australia.
- [20] Veldhuis, G.A., Scheepstal P., Rouwette E, Logtens T. (2015) 'Collaborative problem structuring using MARVEL', *EURO Journal on Decision Processes*, 3(3-4), pp. 249-273 [Online]. Available at: <https://linkinghub.elsevier.com/retrieve/pii/S2193943821000492> (Accessed: 02 May 2024).
- [21] Veldhuis, G.A., M de Reus N., and MJ Keijser B. (2020) Concept development for comprehensive operations support with modeling and simulation, *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 17(1), pp. 99-116. [Online]. Available at: <http://journals.sagepub.com/doi/10.1177/1548512918814407> (Accessed: 02 May 2024).
- [22] Wang, J. (2005) *A review of operations research applications in workforce planning and potential modeling of military training*. Edinburgh: DSTO Systems Sciences Laboratory.

ANNA MOLNÁR*

The growing role of the European Commission in defence capability development**

ABSTRACT: The aim of this research is to present and analyse the growing role of the European Commission in defence capability development. In the first section, I review the literature on the theoretical background of the Commission's role in the European defence policy. In the second section, I briefly present the decision-making processes in the fields of Common Foreign and Security Policy and Common Security and Defence Policy. Following the discussion of the external factors that underpin these developments, I elaborate on the past role of the European Commission and how it has changed after the recent Russian aggression in the Ukraine. I then use SWOT analysis to highlight the strengths, weaknesses, opportunities and threats to the role of the Commission in European defence. Although several EU member states and institutions supported the further integration of defence policy following the creation of the European Security and Defence Policy in early 2000, the defence-related activities of the EU remained weak and limited. Similar to the wars in Yugoslavia in the 1990s, the full-scale Russian invasion in Ukraine in recent years has spurred further development and "Europeanisation" of this policy area. During the last decade, the EU has set the defence agenda in motion and has launched new military-related initiatives due to the deteriorating security environment in the EU's neighbourhood. This has sometimes even involved breaking the taboos on defence and strengthening the role of the

* Prof. Dr., Head of the Department of International Security Studies, Ludovika University of Public Service, Hungary. <https://orcid.org/0000-0002-7958-6985>, molnar.anna@uni-nke.hu.

** The research and preparation of this study was supported by the Central European Academy.

Commission significantly in the defence industry and space sectors. Following the creation of the European Defence Fund, the most important development in this area concerned the possibility of using EU budget money for defence purposes. Although the defence industry and market of the EU is still fragmented and underfinanced, the European Commission has launched important initiatives to overcome these challenges.

KEYWORDS: Defence industry, European Commission, Common Security and Defence Policy, Europeanisation, SWOT.

1. Introduction

According to the EU Treaties, the Common Security and Defence Policy (CSDP) constitutes an integral component of the Common Foreign and Security Policy (CFSP). It is the youngest and one of the least integrated policy areas of the European Union. A prominent feature is still the strong intergovernmental character of its decision-making processes. The robust interconnection between CFSP and CSDP is not fortuitous, given that there is a common perception of security threats and their impact on shaping the foreign, security and defence policy. Foreign policy responses to external challenges and threats also play a role in shaping the interconnection between the two policy areas.

Although several EU member states (MSs) and institutions have supported further integration of defence policy following the creation of the European Security and Defence Policy in early 2000s, defence-related activities of the EU remained weak and limited until 2016.¹ Similar to the wars in Yugoslavia in the 1990s, the full-scale Russian invasion in Ukraine in recent years has given new impetus to further develop and “Europeanise” this policy area. During the last decade, due to the deteriorating security environment in the EU’s neighbourhood, the EU has set the defence agenda in motion and has launched new military-related initiatives sometimes even breaking the taboos on defence. The creation of the European Defence Fund has resulted in the most important development in this area: the possibility of using EU budget money for defence purposes. Although the defence industry and market of the EU is still fragmented and underfinanced, the

¹ Béraud-Sudreau and Pannier, 2021; Molnár 2022; Molnár and Jakusné 2023.

European Commission has launched important initiatives to overcome these challenges.

Despite the continued dominance of intergovernmental decision-making processes in the realm of the Common Foreign and Security Policy—and the Common Security and Defence Policy (as an integral component thereof)—the role of the European Commission has gradually, yet consistently, been strengthened. Since 2016, the traditional boundaries between intergovernmental and supranational decision-making procedures have also become blurred in this policy domain. Due to the spill-over effect, the Commission's core tasks—like agenda-setting, initiating legislation or executive functions—have been extended to the field of defence, especially to the defence industry.²

As a result of the Russian annexation of Crimea in 2014 and the deteriorating security environment near the EU, Jean-Claude Juncker, then President of the European Commission, stated in an interview in March 2015 that he considered it necessary to set up an EU army and that NATO was not sufficient for territorial defence.³ Although the creation of an EU army has not materialised and remains unthinkable, the EC's role has been strengthened in areas related to the EU's external action and human security policies traditionally belonging to the European Commission (e.g., enlargement and neighbourhood policy, aid or development policy), and in areas related to the development of European defence capabilities.

In 2017, the European Defence Fund (EDF) was established based on the European Defence Action Plan (EDAP) prepared by the European Commission. The fund coordinates and complements member states' investments in defence research, prototype development, and the procurement and acquisition of defence equipment and technology.⁴ The significance of its establishment lies in the fact that it became possible to finance military expenditures from the EU budget for the first time. Since

² Haroche, 2020, p. 853; Håkansson, 2021, pp. 590-591; Fotini, 2020.

³ Euractive (2015) Juncker: NATO is not enough, EU needs an army. [Online]. Available at: <http://www.euractiv.com/section/global-europe/news/juncker-nato-is-not-enough-eu-needs-an-army/> (Accessed: 30 April 2024).

⁴ European Commission (2017) A European Defence Fund: €5.5 billion per year to boost Europe's defence capabilities, 7 June 2017, [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1508 (Accessed: 30 April 2024); Chappell et al., 2020, p. 583.

then, the Commission has actively promoted the idea of creating a European Defence Union and realising strategic autonomy.⁵

The aim of this research is to present and analyse the growing role of the European Commission in the development of defence capabilities. In the first section, I provide a literature review on the theoretical background of the Commission's role in CSDP, discussing neofunctionalism, historical institutionalism, Europeanisation, and the conflict between intergovernmentalism and supranationalism. In the second section, I briefly present the decision-making processes in the field of CFSP and CSDP. Following the introduction of the external factors behind these developments, I discuss the role of the EC in the past and after the Russian aggression. In this article, SWOT analysis is used to highlight the strengths, weaknesses, opportunities and threats regarding the role of the Commission in European defence. Based on available academic works this SWOT analysis can be used to project future developments and identify threats that may impede the achievement of the EC's objectives.

2. Theoretical framework

There is a growing body of literature on the increasing role of the European Commission in the field of security and defence. According to Smith, after the launch of the CSDP, it became clear that this policy area was only partially Europeanised, and the distinction between the national and the EU interest had become blurred. The EU sought to create a more integrated CFSP/CSDP governance and institutional structure following the Lisbon Treaty with the establishment of the European External Action Service (EEAS) and the position of the High Representative of the Union for Foreign Affairs and Security Policy—who is also Vice-President of the Commission (HR/VP). However, they still had to compete with national diplomacies in the initiation and implementation of CFSP/CSDP decisions.⁶ That is why the EEAS has a *sui generis* character in international relations. Europeanisation has been widely discussed and debated by researchers and, being a multifaceted process, it focuses on the impact of the EU membership and integration processes on different domestic policies and politics.⁷ While Europeanisation in general can be a top-down and bottom-

⁵ Molnár 2022.

⁶ Smith, 2012, pp. 253-254.

⁷ Radaelli, C., 1997.; Radaelli, C. M., 2004.

up process, in the case of the European defence market, the top-down process is more relevant as the role of the Commission is significant.

Since the beginning of this millennium, the European Commission has gone through intense change due to external pressure and internal evolution.⁸ As a result of these processes and thanks to the strengthening link between the supranational actors—like the Commission and the European Parliament—the Commission has become a more political and less technocratic institution, especially under the Juncker Commission.⁹ Following the financial and economic crisis and due to the reforms on the economic governance the Commission started to expand its activities beyond its original competences.¹⁰ According to the historical institutionalist approach, path-dependent processes, historical events and institutional structures influence the development and behaviour of institutions.¹¹ Both institutional reforms in the early 2000s—resulting from the big bang enlargement—and the multi-faced and multi-level crisis, accelerated the evolution of the Commission. Internal and external factors, and the evolving security challenges have led to the Commission's increasing involvement in defence-related activities as an agenda-setting and policy entrepreneur institution.

According to Haroche, the creation of the EDF highlights a 'new type of offensive functional spillover from the economy to defence'.¹² Håkansson used the revised neofunctionalism to describe the process of further integration within CSDP. According to the cultivated spillover effect, the Commission can support integration 'by acting as policy entrepreneurs'. Due to functional spillover, the inter-dependence between different policy fields can create tensions thus furthering integration.¹³ The Commission has enhanced its power through cumulative bricolage tools, and by alleviating member states' sovereignty concerns and motivating for deeper integration in security and defence. According to Müller and contributors,

⁸ Cini, 2014.

⁹ Egeberg, Gornitzka and Trondal, 2014; Nugent and Rhinard, 2019.

¹⁰ Zeilinger, 2021; Farrall, 2021.

¹¹ Cini, 2015.

¹² Haroche, 2020.

¹³ Håkansson, 2021, pp. 590-591.

bricolage means the pragmatic usage and reconfiguration of existing tools to achieve something new. It highlights the fact that a bricoleur must rely on a limited number of available means to pursue its preferences. At the same time, it also means that available instruments of the bricoleur are known and acknowledged by other political actors.¹⁴

Sabatino argues that the growing role of the Commission in the field of defence industry policy can be considered as a game changer as there is a 'partial shift from intergovernmental to supranational governance in the European defence market'.¹⁵

3. Decision-making processes in the field of CFSP and CSDP

The European Council and the Council remain key institutions for the decision-making processes and coordination of the CFSP and CSDP. From 1992, in the pillar structure established by the Maastricht Treaty, despite the description "common", the intergovernmental approach remained the dominant form of decision-making in this policy area. Regarding the CSDP, no real community (exclusive or shared) policy such as the common commercial or common agricultural policy has been established. Later, despite the abolition of the pillar structure by the Lisbon Treaty, this structure was not changed significantly: decision-making processes continued to be characterised primarily by intergovernmentalism, the pursuit of consensus, and thus the lowest common denominator.

The European Council, the Council of the EU (namely the Foreign Affairs Council) and the High Representative of the Union for Foreign Affairs and Security Policy (HR/VP) have a significant role in setting the agenda for European security and defence. The European Commission has traditionally played a limited role in the domain of CFSP and CSDP. Originally, the EU's external relations activities included the design and the implementation of the traditional external action policy areas of the EU and its predecessors, the European Communities. These included the development, humanitarian aid and enlargement policies. The Commission began to strengthen its role in crisis management and in conflict prevention processes with the implementation of the Rapid Reaction Mechanism in

¹⁴ Müller, Slominski and Sagmeister, 2023, p. 1673.

¹⁵ Sabatino, 2022.

2004 and the Instrument for Stability in 2007, playing a crucial part in tackling the security-development nexus.¹⁶

The Commission's role has evolved considerably over the past decades. This process was supported by the fact that according to the Lisbon Treaty the HR/VP also became the Vice-president of the European Commission. The actions of the HR/VP reflect a "communitised" role, which complements and strengthens the foreign policy of the member states. The creation of the new position and the establishment of the European External Action Service, means that the HR/VP has had a multifaceted role with various hats: 1) undertaking the traditional diplomatic activities in the field of CFSP 2) chairing the Foreign Affairs Council 3) seeking consensus among the 27 EU member states, and 4) building coherence between the Commission's various external policy instruments such as aid, trade, crisis management and the CFSP. The HR/VP represents the EU in international fora (e.g., the United Nations) and acts as head of the European Defence Agency and the EU Institute for Security Studies.¹⁷

Compared to other policies, in the field of CSDP, the European Commission has the right of initiative only through the High Representative of the Union for Foreign Affairs and Security Policy (who is also the Vice-President of the European Commission) and does not exercise significant executive power in this field. This situation has been significantly changed and affected by the Russian aggression in Ukraine. As a result, the Commission, together with other EU institutions, has promoted the establishment of the European Security and Defence Union by 2025 and the collaborative defence industrial cooperation.

4. Factors behind the developments

The creation of ESDP/CSDP was driven by the devastating experience of the Yugoslav wars and the reality that the EU alone was not able to stop those military conflicts. The US and NATO were required to play an active role in that peace enforcement and crisis management situation. Nowadays, the war in Ukraine has become a novel driving force for further integration in the field of defence. Besides the Russian aggression in Ukraine, other factors behind the increased defence cooperation include the changing

¹⁶ Lavallée, 2013.

¹⁷ European Union External Action, The Diplomatic Service of the European Union, [Online]. Available at: https://www.eeas.europa.eu/_en.

foreign policy of the United States (and the consequent weakening of transatlantic relationship). This was evident during the Trump administration and exacerbated by the decision of the United Kingdom (UK) to leave the European Union (Brexit). Further, during the financial and economic crisis, member states spent less on the military.¹⁸

Nowadays, the formulation of defence policy plays a decisive role among the priorities of European governments. This is evident in the 9% decrease in the defence spending of EU MSs between 2008 and 2016,¹⁹ following the years of the financial crisis. Today, they are spending significantly more, with defence expenditure reaching €270 billion in 2023. However, although defence spending increased, only 18% of the investment was realised in a collaborative way within the European Union.²⁰

In 2016, Brexit represented a window of opportunity for developing the defence policy. Despite the fact that the UK was well known for its Eurosceptic approach and for hindering further integration of CSDP, we must emphasise that not every initiative has been blocked by the UK—only those representing a clear supranationalism and Europeanisation in this field (like the creation of a EU-level military command or the establishment of PESCO). Conversely, the UK supported industrial initiatives related to common procurement and research, which later led to the establishment of the EDF.²¹

The evolution of the European Commission's institutional role has been influenced by several factors, including shifts in the personalities of key figures such as the President of the Commission or Commissioners with specific portfolios in key areas, or changes in the political attitudes of some member states, and the impact of pivotal issues such as internal tensions resulting from the migration crisis.

5. The role of the European Commission in the field of defence

The growing activity of the Commission in defence-related issues dates to the 1990s, when this institution vainly supported the amendment to Article

¹⁸ Béraud-Sudreau and Pannier, 2021.

¹⁹ Béraud-Sudreau and Pannier, 2021, p. 297.

²⁰ Besch, S. (2024) Understanding the EU's New Defense Industrial Strategy, [Online]. Available at: <https://carnegieendowment.org/2024/03/08/understanding-eu-s-new-defense-industrial-strategy-pub-91937> (Accessed: 30 April 2024).

²¹ Béraud-Sudreau and Pannier, 2021, pp. 299-300.

223 of the EEC Treaty (now Article 346 TFEU) on the safeguard of national security interests. According to this article, member states may take measures related to arms production and trade for the protection of their essential security interests. Although this attempt was not successful, the Commission has launched its defence-related activities to gradually extend the rules of the internal market to the defence market. In 1996 and 1997, the Commission recommended that community instruments and its DGs (Directorate Generals) should be used to improve the national defence industries. It also proposed the establishment of a new agency for defence-related activities.²²

Parallel to the process of establishing the European Security and Defence Policy led by member states and the Council, the Commission started to focus on the initiatives concerning the defence industry and market-related issues. In 2003, the European Commission proposed the gradual creation of a “European Defence Equipment Market” (EDEM) to strengthen the European Defence Technological and Industrial Base (EDTIB). The European Defence Agency (EDA) was created in 2004. Although this is the only agency explicitly mentioned by the Lisbon Treaty, and it functions under the authority of the Council of the EU as an intergovernmental body, it has had an important role in the implementation of CSDP decisions. In 2007, the EDA issued its strategy on the European Defence Technological and Industrial Base. The objective of the strategy adopted by the member states was to gradually integrate national capability development and the defence market to improve supply security, thus shifting capability development from the national to the European level. The objectives included the creation of a better coordinated, more competitive defence market—with less duplication—that better serves European defence policy.²³

In 2004, the European Commission made significant steps in the field of research by publishing a Communication on Security Research, creating a Group of Personalities on Security Research, and by launching a Preparatory Action on Security Research. In 2007, a civilian European Security Research Programme (ESRP) was established, blurring borders between civilian and military research also partially covering dual-use technologies. Following the Commission’s proposals, in 2009, new directives were adopted on defence procurement (Directive 2009/81/EC)

²² Håkansson, 2021, pp. 590-591.

²³ European Parliament, 2013, pp. 68-78.

and on guidelines for transfers inside the EU (Directive 2009/43/EC) to decrease the fragmentation of the European defence market.²⁴ Although some significant steps were taken during the Barroso Commissions between 2004–2014, the issue of European defence and defence market was still politically very sensitive and further integration was not supported by the critical number of member states. Until the 2010s, however, the EU member states fulfilled the EDTIB strategic objectives to a limited extent.

The Russian annexation of Crimea (2014) can be considered as a watershed for these processes. The new EC President, Juncker, and the High Representative, Mogherini, started to express their views on the need for stronger European defence policy. Barnier was Juncker's special advisor on defence between 2015–2016. He also supported the idea of further defence integration. Mogherini and Juncker have a federalist vision of the integration process, representing a new approach to defence and a greater EU role in that field. Slowly but steadily the process has started, as the Commission and the European Parliament, and a growing number of member states support the idea.²⁵

Brexit represented a policy window for setting the renewed agenda of European defence. According to Tocci—the main policy advisor of the then HR/VP Mogherini, 'The EU is a bit like a bicycle—unless it's moving, it falls; and at the moment it's not moving on the economy, and it's not moving over migration, so let's just make a big deal in defence'.²⁶ As decision-making slowed down in other policy areas, the EU MSs needed to show unity after Brexit and the CSDP was the appropriate forum to do so. Following the adoption of the Global Strategy in 2016, the Commission started to play a decisive role in defence research and development funding. This strategy proposed the realisation of strategic autonomy. This idea was mainly motivated by France, which is why "strategic autonomy" appeared in the EUGS.²⁷

In his annual speech to the European Parliament on 14 September 2016, Juncker, the former President of the EC, emphasised that the field of defence has been given a special role. Juncker stressed, among other things, that the High Representative for Foreign Affairs and Security Policy, who is also the Vice-President of the European Commission, should become a

²⁴ Håkansson, 2021, pp. 590–591.

²⁵ Béraud-Sudreau and Pannier, 2021. pp. 304–305.

²⁶ Béraud-Sudreau and Pannier, 2021. p. 300.

²⁷ Béraud-Sudreau and Pannier, 2021. pp. 297–301.

European foreign minister. This opinion showed that the Commission intended to see itself as an authentic governmental body. Regarding the defence union, he emphasised:

Europe needs to toughen up. Nowhere is this truer than in our defence policy. The Lisbon Treaty enables those Member States who wish, to pool their defence capabilities in the form of a permanent structured cooperation. I think the time to make use of this possibility is now.²⁸

Since the publication of the EU Global Strategy in 2016, the implementation of initiatives to achieve capability development goals has been resting on four pillars: 1) the usage of the Permanent Structured Cooperation (PESCO), 2) the launch of the Co-ordinated Annual Review on Defence (CARD), 3) the establishment of the European Defence Fund (EDF) and 4) the new regulations on common procurement. We must emphasise that the responsibilities of the European Commission and those of the EEAS and the EDA have been steadily expanding. This fact has also led to an institutional competition between them.

The ideas of EDF, PESCO CARD and defence market-related common procurement regulations were also promoted by European defence companies, as they were able to benefit from them. The defence industry supported the realisation of the Preparatory Action on Defence Research (PADR), the European Defence Industrial Development Programme (EDIDP), and the EDF supporting collaborative research and development from the beginning.²⁹

The European Commission's role in defence-related matters has evolved significantly over the last decade.³⁰ In 2017, the European Defence Fund (EDF) was proposed by the Commission to support collaborative defence research and development projects among EU member states. The preparatory programs, like the PADR and EDIDP led to the creation of the EDF in 2021. Although the Commission proposed €13 billion for the EDF,

²⁸ Juncker, J.-C. (2016) The State of the Union 2016: Towards a Better Europe – A Europe that Protects, Empowers and Defends. September 14, 2016 [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_3042 (Accessed: 30 April 2024).

²⁹ Béraud-Sudreau and Pannier, 2021. pp. 304-305.

³⁰ Håkansson, 2021.

because of budget negotiations, €590 million was finally available for the period 2017–2020 and only €7.953 billion for the period 2021–2027.³¹

A “Group of Personalities” was established in 2015 in the framework of the DG Grow and the EDA. The Group of Personalities consisted of chief executive officers (CEOs) of the defence industry, politicians, as well as academics and experts, playing an important role in preparing recommendations about the support of the EU for defence research programs.³² Although the available financial support remained less than expected, the establishment of the EDF represented an important step in blurring the traditional distinction between the intergovernmental and supranational decision-making institutional framework.³³

The defence industrial or market-oriented issues, and the decision-making processes have been included in the Europeanisation attempts of the Commission. In 2018, Juncker highlighted the need for more efficient decision-making in the CFSP in his annual EP speech. The European Commission has also drafted a proposal on the need to introduce qualified majority voting (QMV). However, this would only be possible through a comprehensive treaty amendment or the application of the *passerelle* clause according to Article 48(7) TEU. According to Article 31(3) of the TEU, the EC proposed the use of the *passerelle* clause. In line with this, the European Council may unanimously decide—except for decisions having military or defence applications—that the Council may also act by qualified majority in cases other than those mentioned in Article 31 (2). The European Commission has identified three areas where qualified majority decision-making could be used: 1) the promotion of human rights, 2) EU sanctions and 3) the launch of civilian missions. Although the EP supported the European Commission’s proposal to extend the QMV, not all MSs support the idea, and no decision has yet been made at the level of the European Council.³⁴

In September 2019, the new President of the EC, von der Leyen, announced the creation of the “Geopolitical Commission” in a “mission letter” to

³¹ European Commission (2017) An European Defence Fund: €5.5 billion per year to boost Europe's defence capabilities, 7 June 2017, [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1508 (Accessed: 30 April 2024).

³² Béraud-Sudreau and Pannier, 2021, pp. 304–305.

³³ Håkansson, 2021.

³⁴ European Parliament, 2019.

Borrell.³⁵ Without offering a specific and clear definition, she emphasised the importance of connecting the internal and external aspects of different policies. She noted that the European Commission must become ‘strategically stronger, more decisive and more united’, including the use of its financial instruments. Von der Leyen also emphasised the need to create a European Defence Union.³⁶

An important innovation in 2019 was the creation of a new directorate-general (DG) within the European Commission—the Directorate-General for Defence Industry and Space (DG DEFIS),—supplementing the existing directorates-general dealing with more traditional external relations (DG DEVCO, DG ECHO, DG NEAR and DG Trade).³⁷ The new DG was created on the basis of units coming from the DG Grow with the responsibility of managing space-related issues, the implementation of defence procurement regulations (Directive 2009/81/EC), Military Mobility and the EDF. By the creation of the DG DEFIS, the Commission has empowered itself significantly in the field of defence industry and space sector. This new DG functions under the leadership of Commissioner for Internal Market, Breton. In the field of defence industry, DG DEFIS is responsible for supporting the competitiveness and innovation of the European Defence industry by guaranteeing the development of an effective European defence technological and industrial base. The DG DEFIS has an important role in the implementation of the oversight of the European Defence Fund. Its main task is to promote the evolution of ‘an open and competitive European defence equipment market and enforcing EU procurement rules on defence’. It also has an important role in the implementation of the Action Plan on Military Mobility and the space program of the EU (like COPERNICUS, GALILEO and EGNOS). It supports the realisation of climate objectives in space and defence and security-related activities.³⁸

³⁵ Von der Leyen, U. (2019) Mission letter to Josep Borrell. Brussels: European Commission, [Online]. Available at: https://ec.europa.eu/commission/commissioners/sites/default/files/2019-04/cwt2019/files/commissioner_mission_letters/mission-letter-josep-borrell-2019_en.pdf (Accessed: 30 April 2024).

³⁶ Zwolski, 2020.

³⁷ Müller, Slominski and Sagmeister, 2023.

³⁸ European Commission, Defence Industry and Space, [Online]. Available at: https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/defence-industry-and-space_en (Accessed: 30 April 2024).

The full-scale Russian invasion in Ukraine in 2022 was a turning point in strengthening the Commission's role in defence related issues. The war clearly showed the shortages and the problems deriving from the undersizing, and the fragmentation and underfunding of European defence industry. On 11 March 2022, during the informal meeting of the European Council in Versailles, member states of the EU expressed their commitment to enhancing the European defence technological and industrial bases and invited the European Commission to continue planning in this policy area.³⁹

The urgent demand generated by the war provided both a great challenge and an opening opportunity for the European defence industry. The European Commission with the High Representative of the Union for Foreign Affairs and Security Policy (who is also the Head of EDA) expressed several goals in their joint communication entitled 'On the Defence Investment Gaps Analysis and Way Forward'.⁴⁰ As a consequence, the Commission along with the High Representative, have established the Defence Joint Procurement Task Force (DJPTF) to support the short-term coordination of urgent procurement needs in May 2022. The objective of the task force was to help close the gap between supply and demand by identifying needs and creating incentives. Subsequently, the essential regulatory process has begun.⁴¹ This institutional adaptation clearly shows the growing role of the Commission in defence.

The European Commission has proposed two legal incentives⁴² because the increased demand could lead to procurement outside the EU, and consequently delay the realisation of the objectives related to the European defence technological and industrial base. In the short term, the approval of the "European Defence Industry Reinforcement through Common Procurement Act" (EDIRPA), and in the long term, the European Defence Investment Programme (EDIP), were proposed to encourage joint procurement, and to increase production capacity, thus making European defence industry more competitive.⁴³ Although EU defence spending was raised to a record high of €270 billion in 2023,⁴⁴ between March 2022 and

³⁹ European Council, 2022.

⁴⁰ European Commission and High Representative, 2022.

⁴¹ Schnitzl, 2023, p. 2.

⁴² European Commission, 2022b.

⁴³ Schnitzl 2023, p. 1.

⁴⁴ Besch, S. (2024) Understanding the EU's New Defense Industrial Strategy, [Online]. Available at: <https://carnegieendowment.org/2024/03/08/understanding-eu-s-new-defense-industrial-strategy-pub-91937> (Accessed: 30 April 2024).

June 2023, 78% of the military procurement was from outside the EU (63% of which was from the US) and collaborative spending remained weak.⁴⁵

Due to the increased demand, on 3 May 2023, the Commission submitted a proposal⁴⁶ for the adoption of the Regulation on Establishing the Act in Support of Ammunition Production (ASAP). The new regulation complemented the one on EDIRPA. The purpose of ASAP was to support the EU in increasing its ammunition and missile production capacity in the interests of the Ukraine and the EU member states. The Commission proposed that the budget of ASAP (€500 million) could come from the transfer of various instruments, especially from the European Defence Fund and EDIRPA.⁴⁷

After reaching political agreement, the European Parliament and the Council adopted the ASAP regulation which was published in the Official Journal of the European Union on 20 July 2023. The new regulation complemented the one on EDIRPA,⁴⁸ which was adopted by the European Parliament and the Council in autumn 2023. The new regulation was published in the Official Journal of the EU on 26 October 2023.⁴⁹ After the State of the Union Address of President von der Leyen in 2023, the European Commission initiated a consultation process to develop a new European Defence Industrial Strategy (EDIS). The strategy was elaborated by the Commission and the HR/VP after extensive consultation with key stakeholders. The European Defence Agency played an active role in this process.

In March 2024, the European Commission and the High Representative published the European Defence Industrial Strategy (EDIS)—the first defence industrial strategy of the EU to increase the resilience of the European defence industry. The main purpose of the strategy is to address the challenges posed by the full-scale Russian invasion in Ukraine. It aims to strengthen European defence industry through actions that support collaborative research, investment, production and procurement. This strategy provides a vision for the European defence industrial policy until 2035. The strategy specifies clear indicators for the future. It invites member states 1) to ‘procure at least 40% of defence

⁴⁵ Maulny, 2023.

⁴⁶ European Commission, 2023a.

⁴⁷ European Parliament, 2023.

⁴⁸ Official Journal of the EU, 2023a.

⁴⁹ Official Journal of the EU, 2023b.

equipment in a collaborative manner by 2030'; it sets as a goal that, 2) 'by 2030, the value of intra-EU defence trade represents at least 35% of the value of the EU defence market', and calls on member states 3) 'to make steady progress towards procuring at least 50% of their defence investments within the EU by 2030 and 60% by 2035'.⁵⁰

According to the EDIS, a Defence Industrial Readiness Board ("The Board") will be established to bring together representatives of member states, the High Representative/Head of the Agency and the Commission. The main tasks of the new board will include 1) 'to perform the EU defence joint programming and procurement function envisaged in the Joint Communication on Defence Investment Gap Analysis' and 2) 'to support the implementation of EDIP'. This new board will continue the work of the Defence Joint Procurement Task Force. The Board will 'also support the coordination and de-confliction of Member States procurement plans and provide strategic guidance in view of more effectively matching demand and supply'. The board will be prepared and co-chaired jointly by the Commission and the High Representative/Head of Agency. The Board will be formally established within the EDIP Regulation supporting the implementation of EDIP. A high-level European Defence Industry Group will be established to ensure effective cooperation and dialogue between governments and industry. The new board's 'programming and procurement function will be based on the existing instruments and initiatives, notably the Capability Development Plan (CDP), the Coordinated Annual Review on Defence (CARD) and the Permanent Structured Cooperation (PESCO)'.⁵¹

The growing ambitions of the Commission are also demonstrated by the fact that in 2024, at the Munich Security Conference, von der Leyen proposed the new position of commissioner for defence.⁵² This statement

⁵⁰ European Commission (2024) EDIS | Our common defence industrial strategy, p. 15, [Online]. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en (Accessed: 30 April 2024).

⁵¹ European Commission (2024) EDIS | Our common defence industrial strategy, pp. 8-9, [Online]. Available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en (Accessed: 30 April 2024).

⁵² Brzozowski, A. (2024) EU defence commissioner proposal gains traction, EurActiv, 19. February, [Online]. Available at: <https://www.euractiv.com/section/defence-and-security/news/eu-defence-commissioner-proposal-gains-traction/> (Accessed: 30 April 2024).

shows clearly the results of this process—the strengthened role of the Commission in defence (and defence industry) issues.

6. SWOT analysis of the role of the European Commission in defence

This SWOT analysis enables the identification of areas of strengths, the elimination of weaknesses, the use of opportunities and the mitigation of threats.⁵³ Strengths are positive internal factors that are controlled by the organisation, in this case, by the European Commission, which provides institutional background for defence-related activities. Weaknesses are internal, of a negative nature, and within the control of the organisation. Identifying them creates the possibility to implement key improvements. Opportunities can be defined as external positive possibilities that can be capitalised on. Such opportunities are frequently beyond the influence of the EU, or situated at the margins (for example, the evolution of international public opinion concerning one of the EUs decisions). The threats are identified as difficulties, external obstacles or constraints that have the potential to prevent the development of a policy area (for example, the defence industry). Threats fall beyond the competences or the influence of the EU, or are also situated at its margin (for example, the development of the war in Ukraine).⁵⁴

⁵³ Karppi, Kokkonen and Lähteenmäki-Smith, 2001, p. 16; Dealtry, 1992, p. 2.

⁵⁴ Europa.eu (2024) SWOT analysis - strengths, weakness, opportunities, threats, Evaluation Unit DEVCO, [Online]. Available at: <https://wikis.ec.europa.eu/display/ExactExternalWiki/SWOT+analysis+-+strengths%2C+weaknesses%2C+opportunities+and+threats> (Accessed: 30 April 2024).

Strengths	Weaknesses
<ul style="list-style-type: none"> - institutional framework and Background of the European Commission - experience of the European Commission in the field of planning, implementing and controlling the EU financial programs - creation of the European Defence Fund - strategic thinking at the EU level - available financial support from the EU budget - institutional innovation: the creation of the DG DEFIS 	<ul style="list-style-type: none"> - lack of significant collaborative defence investment - lack of substantial financial support from the EU budget - fragmented institutional background on the EU - Institutional competition between the European Commission and other actors, like the more intergovernmental agency, the EDA - The differences in the member states' threat perceptions, their strategic cultures and their diverging relationship with the US and NATO
Opportunities	Threats
<ul style="list-style-type: none"> - the Commission's role as a policy entrepreneur to support further integration - the spill-over deriving from the interdependences between different policy fields - the implementation of the EDF, EDP and EDIS - Institutional developments, like the establishment of the Defence Industrial Readiness Board - The worsening security environment - The social support of the European citizens - new financial opportunities (the lending of the European Investment Bank Group) 	<ul style="list-style-type: none"> - absence of political support from member states for further integration - absence of political support from member states for further budgetary reform - diverging strategic industrial interests of member states and of industrial players - the increasing support of Eurosceptic political parties at national and European level - hybrid threats and external interference

Source: Author

The creation of the European Defence Fund is the primary strength. It has solidified the role of the Commission, which has had several decades of experience in the field of planning, implementing and controlling the EU financial programs. According to Sabatino, the EDF has become a “game changer for defence” supporting the introduction of partial supranational governance in the European defence market.⁵⁵ Strategic thinking is also a strength because strategic documents like the Strategic Compass (2022) or the European Defence Industrial Strategy provide a clear vision for further development. Available financial support from the EU budget represents an important incentive and strength for further development. As data shows, after the second call of the EDF, 41 collaborative defence research and development projects with a total EU support of almost €832 million were selected for funding in 2023.⁵⁶ The Commission has empowered itself significantly in the field of defence industry and space sector⁵⁷ through the new institutional structure within the Commission—by the creation of the DG for Defence Industry and Space (DG DEFIS). This manages the Commission’s activities regarding the implementation of European Defence Fund, and the Action Plan on Military Mobility.

The lack of significant collaborative defence investment and substantial financial support from the EU budget are a weakness that can negatively affect the implementation of the ambitious objectives. Another weakness is that the institutional background on the EU level is still fragmented, and the European Commission must compete with other actors, like the intergovernmental agency—the EDA. The differences in the member states’ threat perceptions, their strategic cultures and their diverging relationship with the US and NATO have the potential to weaken the Commission’s effort to assume a more prominent role in this field and to advance deeper integration.⁵⁸

Opportunities derive from the Commission’s role as a policy entrepreneur to support further integration. Interdependences between different policy fields can create tensions thus creating a spill-over effect

⁵⁵ Sabatino, 2022.

⁵⁶ European Commission (2023b) Result of the EDF 2022 Calls for Proposals, [Online]. Available at: https://defence-industry-space.ec.europa.eu/funding-and-grants/calls-proposals/result-edf-2022-calls-proposals_en (Accessed: 30 April 2024).

⁵⁷ Müller, Slominski and Sagmeister, 2023.

⁵⁸ Tardy, 2018.

from the economy to defence.⁵⁹ The implementation of the EDF, EDP and EDIS indicates a bureaucratic spillover that could accelerate the initiatives of the Commission.⁶⁰ Institutional developments—like the establishment of the Defence Industrial Readiness Board—will further strengthen the Commission’s role in the field of defence. The worsening security environment in the proximity of the European Union—particularly the war in Ukraine—could act as both a threat or an opportunity for the Commission to play a stronger geopolitical role.⁶¹ It is notable that developments in the field of defence are also supported by the citizens. According to Standard Eurobarometer (100 Autumn 2023), 77% of respondents are in favour of ‘a common defence and security policy among EU member states’.⁶² Another opportunity is provided by the proposal of ECOFIN in April 2024 to update policies and framework for the lending of the European Investment Bank Group (EIB Group) to the security and defence industry.⁶³

Potential threats were highlighted by the fact that the European Commission was not fully supported by the member states during the EU budget negotiations. According to Besch, ‘In theory, cooperation offers economic benefits such as reduced equipment duplication, increased production, and lower costs. In practice, national interests and protectionism, coupled with operational and bureaucratic inefficiencies, have historically impeded effective collaboration’.⁶⁴ Sabatino (2022) argues that ‘diverging strategic industrial interests of member states and of industrial players seek to prevent a deeper integration of the European defence market’.⁶⁵ The absence of substantial support from member states for further budgetary reform represents a significant obstacle to progress.

⁵⁹ Håkansson, 2021, pp. 590-591.; Haroche, 2020.

⁶⁰ Haroche, 2020.

⁶¹ Håkansson, 2024.

⁶² Standard Eurobarometer 100 - Autumn 2023 - Europeans' opinions about European Union's priorities – Report, [Online]. Available at: <https://europa.eu/eurobarometer/surveys/detail/3053> (Accessed: 30 April 2024).

⁶³ European Investment Bank (2024) EU Finance Ministers set in motion EIB Group Action Plan to further step-up support for Europe’s security and defence industry, [Online]. Available at: <https://www.eib.org/en/press/all/2024-143-eu-finance-ministers-set-in-motion-eib-group-action-plan-to-further-step-up-support-for-europe-s-security-and-defence-industry> (Accessed: 30 April 2024).

⁶⁴ Besch, S. (2024) Understanding the EU’s New Defense Industrial Strategy, [Online]. Available at: <https://carnegieendowment.org/2024/03/08/understanding-eu-s-new-defense-industrial-strategy-pub-91937> (Accessed: 30 April 2024).

⁶⁵ Sabatino, 2022. p. 134.

The increasing support of Eurosceptic political parties at national and European level may also hinder the strengthening of the Commission's role in general and in the field of defence. Hybrid threats and external interference can negatively affect the deeper integration in this field.

7. Conclusions

During the last decades, the European Commission has gone through severe changes accelerated by external factors and internal developments. Institutional reforms (like the creation of the HR/VP position and the establishment of the European External Action Service) and several crisis situations (from the financial crisis to the war in Ukraine) have pushed the development of the Commission. Additionally, Russian aggression in Ukraine, the changing US foreign policy, especially during the Trump administration, Brexit and the financial and economic crisis underpinned these developments. The increasing role of the Commission in defence industry policy has been interpreted as a game changer for realising a 'partial shift from intergovernmental to supranational governance in the European defence market'.⁶⁶

Originally, the role of the Commission was only limited in the areas of CFSP and CSDP. This mainly only included the implementation of the traditional external action policy areas of the EU—like the development policy, the humanitarian aid policy or the enlargement policy. This institutional structure has been significantly changed by the Russian aggression in Ukraine. Consequently, the intention to establish the European Defence Union by 2025 and the realisation of collaborative defence industrial cooperation have been promoted by the Commission. The creation and management of the EDF has blurred the traditional distinction between intergovernmental and supranational decision-making processes. Through the creation of the DG DEFIS in 2019, the role of the Commission was strengthened significantly in the field of defence industry and space sector. The commencement of full-scale war in Ukraine has highlighted shortages and the problems deriving from the undersizing, fragmentation, and underfunding of the European defence industry. Thus the Commission's agenda-setting and regulatory role were also reinforced in the field of defence policy.

⁶⁶ Sabatino, 2022.

Bibliography

- [1] Béraud-Sudreau, L., Pannier, A. (2021) 'An 'improbable Paris-Berlin-Commission triangle': usages of Europe and the revival of EU defense cooperation after 2016', *Journal of European Integration*, 43(3), pp. 295-310; <https://doi.org/10.1080/07036337.2020.1740215>.
- [2] Chappell, L., Exadaktylos, T. Petrov, P. (2020) 'A more capable EU? Assessing the role of the EU's institutions in defence capability development', *Journal of European Integration*, 42(4), pp. 583-600; <https://doi.org/10.1080/07036337.2019.1666115>.
- [3] Cini, M. (2014) 'The European Commission after the reform', in Magone, J. (Ed.) *Routledge Handbook of European Politics*, UK: Routledge, pp. 235-247.
- [4] Cini, M. (2015) 'Good Governance and Institutional Change: Administrative Ethics Reform in the European Commission', *Journal of Contemporary European Research*, 12(1), pp. 440-454; <https://doi.org/10.30950/jcer.v12i1.705>.
- [5] Dealtry, T. R. (1992) *Dynamic SWOT analysis. Developer's Guide*. Birmingham: Dynamic SWOT Associates.
- [6] Egeberg, M., Gornitzka, Å., Trondal, J. (2014) 'A Not So Technocratic Executive? Everyday Interaction between the European Parliament and the Commission', *West European Politics*, 37(1), pp. 1-18; <https://doi.org/10.1080/01402382.2013.832952>.
- [7] Farrall, S. (2021) 'Historical and Constructivist Institutionalisms', in Farrall, S. (ed.) *Building Complex Temporal Explanations of Crime. Critical Criminological Perspectives*. UK: Palgrave Macmillan, Cham, pp. 29 – 50; https://doi.org/10.1007/978-3-030-74830-2_3.

-
- [8] Fotini, B. (2020) 'The Strategic Context of the European Security and Defence Policy', in Voskopoulos, G. (ed.) *European Union Security and Defence, Policies, Operations and Transatlantic Challenges*, Springer, Cham, pp. 25-37; https://doi.org/10.1007/978-3-030-48893-2_2.
- [9] Håkansson, C. (2021) 'The European Commission's new role in EU security and defence cooperation: the case of the European Defence Fund', *European Security*, 30(4), pp. 589-608; <https://doi.org/10.1080/09662839.2021.1906229>.
- [10] Håkansson, C. (2024) 'The Ukraine war and the emergence of the European commission as a geopolitical actor', *Journal of European Integration*, 46(1), pp. 25-45; <https://doi.org/10.1080/07036337.2023.2239998>.
- [11] Haroche, P. (2020) 'Supranationalism strikes back: a neofunctionalist account of the European Defence Fund', *Journal of European Public Policy*, 27(6), pp. 853-872, <https://doi.org/10.1080/13501763.2019.1609570>.
- [12] Karppi, I., Kokkonen, M., Lähtenmäki-Smith, K. (2001) 'SWOT-analysis as a basis for regional strategies', *Nordregio Working Paper*, 2001/4, [Online]. Available at: <https://www.diva-portal.org/smash/get/diva2:700483/FULLTEXT01.pdf> (Accessed: 30 April 2024).
- [13] Lavallée, C. (2013) 'From the rapid reaction mechanism to the instrument for stability: The empowerment of the European commission in crisis response and conflict prevention', *Journal of Contemporary European Research*, 9(3) Special Issue, pp. 372-389; <https://doi.org/10.30950/jcer.v9i3.517>.
- [14] Maulny, J (2023) *The impact of the war in Ukraine on the European defence market*. [Online]. Available at: https://www.iris-france.org/wp-content/uploads/2023/09/19_ProgEuropeIndusDef_JPMaulny.pdf (Accessed: 30 April 2024).

- [15] Molnár, A. (2022) 'The idea of a European Security and Defence Union', in Molnár, A., Fiott, D., Asderaki, F., Paile-Calvo, S. (eds.) *Challenges of the Common Security and Defence Policy*. ESDC 2nd Summer University Book. Luxemburg: Publications Office of the European Union, pp. 19–36.
- [16] Molnár, A., Jakusné Harnos, É. (2023) 'The Postmodernity of the European Union: A Discourse Analysis of State of the Union Addresses', *The International Spectator*, 58(1), pp. 58–74; <https://doi.org/10.1080/03932729.2022.2149177>.
- [17] Müller, P., Slominski, P., Sagmeister, W. (2023) 'Supranational Self-Empowerment Through Bricolage: The Role of the European Commission in EU Security and Defence', *Journal of Common Market Studies*, 61(6), pp. 1672–1691; <https://doi.org/10.1111/jcms.13564>.
- [18] Nugent, N., Rhinard, M. (2019) 'The 'political' roles of the European Commission', *Journal of European Integration*, 41(2), pp. 203–220; <https://doi.org/10.1080/07036337.2019.1572135>.
- [19] Radaelli, C. (1997) 'How does Europeanization produce domestic policy change? Corporate Tax Policy in Italy and the United Kingdom' *Comparative Political Studies*, 30(5), pp. 553–575; <https://doi.org/10.1177/0010414097030005002>.
- [20] Radaelli, C. M. (2004) 'Europeanisation: Solution or Problem?' *European Integration Online Papers* 8(16), [Online]. Available at: <https://eiop.or.at/eiop/pdf/2004-016.pdf> (Accessed: 30 April 2024).
- [21] Sabatino, E. (2022) 'The European defence fund: a step towards a single market for defence?', *Journal of European Integration*, 44(1), pp. 133–148; <https://doi.org/10.1080/07036337.2021.2011264>.

-
- [22] Schnitzl, G. (2023) *EDIRPA/EDIP: Risks and opportunities of future joint procurement incentives for the European defence market*. French Institute for International and Strategic Affairs, 2023 (March), [Online]. Available at: <https://www.iris-france.org/wp-content/uploads/2023/03/ARES-81-Policy-paper.pdf> (Accessed: 30 April 2024).
- [23] Smith, M. E. (2012) '13 Developing a 'Comprehensive Approach' to International Security: Institutional Learning and the CSDP', in Richardson, J. (ed.) *Constructing a Policy-Making State? Policy Dynamics in the EU*, online edn, Oxford: Oxford Academic, pp. 252–269; <https://doi.org/10.1093/acprof:oso/9780199604104.003.0013>.
- [24] Tardy, T. (2018) 'Does European defence really matter? Fortunes and misfortunes of the Common Security and Defence Policy', *European Security*, 27(2), pp. 119–137; <https://doi.org/10.1080/09662839.2018.1454434>.
- [25] Zeilinger, B. (2021) 'The European Commission as a Policy Entrepreneur under the European Semester', *Politics and Governance*, 9(3), pp. 63–73; <https://doi.org/10.17645/pag.v9i3.4102>.
- [26] Zwolski, K. (2020) 'Diversified in unity: the agenda for the geopolitical European Commission', *Global Affairs*, 6(4–5), pp. 519–535; <https://doi.org/10.1080/23340460.2020.1834427>.
- [27] European Commission (2022b) *Proposal for a regulation of the European Parliament and of the Council on establishing the European defence industry reinforcement through common Procurement Act*. COM/2022/349, [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0349> (Accessed: 30 April 2024).

- [28] European Commission (2023a) *Proposal for a Regulation of the European Parliament and of The Council on establishing the Act in Support of Ammunition Production*. Brussels, 3.5.2023 COM(2023) 237 final 2023/0140(COD), [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0237> (Accessed: 30 April 2024).
- [29] European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2022a) *Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the Defence Investment Gaps Analysis and Way Forward*. 18 May 2022. [Online]. Available at: https://commission.europa.eu/system/files/2022-05/join_2022_24_2_en_act_part1_v3_1.pdf (Accessed: 30 April 2024).
- [30] European Council (2022) *Informal meeting of the Heads of State or Government, Versailles Declaration 10 and 11 March 2022*. [Online]. Available at: <https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf> (Accessed: 30 April 2024).
- [31] European Parliament (2013) The development of a European Defence technological and Industrial Base (EDTIB). EXPO/B/SEDE/2012/20. [Online]. Available at: [https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/433838/EXPO-SEDE_ET\(2013\)433838_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/433838/EXPO-SEDE_ET(2013)433838_EN.pdf) (Accessed: 30 April 2024).
- [32] European Parliament (2019) The state of the debate on the Future of Europe European Parliament resolution of 13 February 2019 on the state of the debate on the future of Europe (2018/2094(INI)), P8_TA(2019)0098, European Parliament, [Online]. Available at: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0098_EN.pdf?redirect (Accessed: 30 April 2024).

-
- [33] European Parliament (2023) *European defence industry reinforcement through common procurement act (EDIRPA)*. *EU legislation in progress*, [Online]. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739294/PRS_BRI\(2023\)739294_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739294/PRS_BRI(2023)739294_EN.pdf) (Accessed: 30 April 2024).
- [34] Official Journal of the EU (2023a): Regulation (EU) 2023/1525 of the European Parliament and of the Council of 20 July 2023 on supporting ammunition production (ASAP), [Online]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1525&qid=1695904709752> (Accessed: 30 April 2024).
- [35] Official Journal of the EU (2023b): Regulation (EU) 2023/2418 of the European Parliament and of the Council of 18 October 2023 on establishing an instrument for the reinforcement of the European defence industry through common procurement (EDIRPA), [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302418 (Accessed: 30 April 2024).

GRZEGORZ OCIECZEK*

The Internal Security Agency and Poland's Critical Infrastructure Protection: Challenges and Solutions**

ABSTRACT: This article is devoted to critical infrastructure protection issues, with a focus on national regulations. It does not omit issues concerning the authorities which, according to the regulations, are responsible for critical infrastructure protection, including: relevant ministers, the Government Security Centre as well as the Internal Security Agency. The publication also presents issues related to ensuring information and communication technology security and countering terrorist threats, espionage and cyber-attacks. The empirical aspect of citing an excerpt from a research on terrorism, which was conducted in 2022 by ABW officers among representatives of academia as well as representatives of services and institutions belonging to the anti-terrorism community involved in terrorism studies, has not been disregarded either. The research points to a growing threat to the European Union from terrorist attacks. The article concludes with postulates on the need to increase the protection of critical infrastructure, in particular through proper risk assessment, as well as the need to develop an IT model for threat knowledge management.

Keywords: critical infrastructure, terrorism, cyber-terrorism, crisis management, Internal Security Agency.

*Assistant professor, Faculty of Law in the Department of Criminal Procedure, UKSW, Warsaw, Poland. <https://orcid.org/0000-0002-2785-4677>, g.ocieczek@uksw.edu.pl.

** The research and preparation of this study was supported by the Central European Academy.

1. National critical infrastructure

Critical infrastructure plays an extremely important role in this day and age, especially in the current socio-economic context. Its protection is of particular importance given the recent events beyond Poland's eastern border in connection with the aggression of the Russian Federation against Ukraine. It is the responsibility of the state and its authorities to provide adequate and, above all, effective protection for systems and their constituent equipment, facilities, installations as well as services belonging to critical infrastructure.

The first references to the protection of critical infrastructure in Poland (although not directly in such terms), appeared in the Act of 21 November 1967 on the universal duty to defend the People's Republic of Poland¹. Article 2 of the Act emphasises that all organs of state authority and administration, state institutions, units of the socialised economy, social organisations and every citizen is obliged to strengthen the defence of the People's Republic of Poland and national property in the event of a threat to the security of the State. In addition, Article 2 refers to an extremely important element from the point of view of critical infrastructure, which is cyberspace. Cyberspace should be understood, according to Article 2(1b) of the said Act, as the space for processing and exchanging information created by information and communication systems.² The currently in force Act of 11 March 2022 on homeland defence, *inter alia*, in Article 1, point 19, defines the competence of the authorities in matters of applying for the recognition of an object as particularly important for the security or defence of the state³. The essential national legislative acts governing the protection of critical infrastructure are:

¹Act of 21 November 1967 on the universal duty to defend the People's Republic of Poland, Journal of Laws of 1967 no. 44 item 220.

²Act of 17 February 2005 on computerisation of the business entities pursuing public tasks, Journal of Laws of 2005 no. 64 item 565.

³ Act of 11 March 2022 on homeland defense, Journal of Laws of 2022, item 655; see also Act of 29 August 2002 on martial law and the powers of the Supreme Commander of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland, Journal of Laws of 2002 No. 156 item 1301; Act of 29 August 2002 on martial law and the powers of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional bodies of the Republic of Poland, Journal of Laws of 2002 No. 156 item 1301.

- Act of 22 August 1997 on the protection of persons and property⁴;
- Act of 22 January 1999 on the protection of classified information⁵;
- Ordinance of the Council of Ministers of 24 June 2003 on objects of particular importance for state security and defence and their special protection⁶;
- Act of 26 April 2007 on crisis management⁷;
- and Resolution No. 210/2015 of the Council of Ministers of 2 November 2015 on the adoption of the National Programme for the Protection of Critical Infrastructure with Annex No. 1 on standards to ensure the efficient functioning of critical infrastructure - good practices and recommendations.

The first of the aforementioned acts determines, *inter alia*, the issues concerning the area and transport subject to mandatory protection. Pursuant to Article 5 of the Act, areas, facilities, equipment and transports that are essential for defence, the economic interest of the state, public security and other compelling interests of the state are subject to mandatory protection by specialised armed protection formations or appropriate technical protection. In this respect, a classification of objects, areas, and equipment has been undertaken, namely:

- with regard to national defence (Article 5(2) (1a-c));
- with regard to the protection of the economic interest of the state (Article 5(2) (2a-c));
- with regard to public security (Article 5(2) (3a-c));
- with regard to other compelling interests of the state (Article 5(4) (a-d));
- facilities, including buildings, equipment, installations, services included in the consolidated list of critical infrastructure facilities, installations, equipment and services (Article 5(2) (5)).

In turn, the Act on the protection of classified information of 22 January 1999 covers issues concerning the protection of ICT critical infrastructure. Pursuant to Article 14 of the Act, state protection services (the Internal Security Agency and the Military Counterintelligence Service) are authorised, *inter alia*, to carry out functions concerning the security of

⁴ Journal of Laws of 1997 No. 114 item 74.

⁵ Journal of Laws of 1999 Nr 11 item 95.

⁶ Journal of Laws of 2003 No. 116 item 1090.

⁷ Journal of Laws of 2007 No. 89 item 590.

ICT systems and networks. However, on the basis of Article 1, the Act defines the principles of protection of information that requires protection against unauthorised disclosure, as constituting a state or official secret, regardless of the form and manner of its expression, also in the course of its development, hereinafter referred to as ‘classified information’.

The most comprehensive as well as the most important legal act addressing issues concerning the protection of critical infrastructure is the Act on crisis management referred to in point four and the Resolution of the Council of Ministers of 2 November 2015 on the adoption of the National Programme for the Protection of Critical Infrastructure. The Act on crisis management defines basic concepts such as critical infrastructure, European critical infrastructure, critical infrastructure protection, emergency situation, etc. Pursuant to Article 3(2) of the Act on crisis management, critical infrastructure is defined as ‘systems and their constituent objects, including buildings, equipment, installations, services that are key to the security of the state and its citizens and that serve to ensure the efficient functioning of public administration bodies, as well as institutions and entrepreneurs’. In turn, Article 3(2) lists individual systems comprising critical infrastructure, which includes the systems of:

- a) supply of energy, energy resources and fuels,
- b) communications,
- c) data communication networks,
- d) finance,
- e) food supplies,
- f) water supply,
- g) healthcare,
- h) transport,
- i) rescue,
- j) ensuring continuity of public administration,
- k) production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances.

The definition of European critical infrastructure, in turn, can be found in Article 3(2a), of the Act on crisis management, according to which European critical infrastructure consists of systems and their functionally related facilities, including buildings, equipment and installations crucial for the security of the state and its citizens and for ensuring the efficient functioning of public administration bodies, as well as institutions and entrepreneurs, referred to in point 2(a) and (h), with regard to electricity, oil

and gas, road, rail, air, inland waterways transport, ocean and short-sea shipping and ports, located in the territory of the Member States, the disruption or destruction of which would significantly affect two or more Member States. This definition is in conformity with that formulated on the basis of the Council Directive of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection⁸. An important aspect in qualifying individual systems as critical infrastructure is the need to meet certain criteria, which are sectoral and cross-cutting in nature⁹.

The National Programme for the Protection of Critical Infrastructure was an important document that was first developed and subsequently adopted by the Council of Ministers on 26 March 2013. It has now been revised and updated by Resolution No. 210/2015 of the Council of Ministers of 2 November 2015 on the adoption of the National Programme for the Protection of Critical Infrastructure, taking into account Resolution No. 116/2020 of the Council of Ministers of 13 August 2020 amending the resolution on the adoption of the National Programme for the Protection of Critical Infrastructure and Resolution No. 38 of 21 March 2023 amending the resolution on the adoption of the National Programme for the Protection of Critical Infrastructure. This instrument was developed on the basis of Article 5b of the Act on crisis management, according to which the Council of Ministers adopts, by resolution, the National Programme for the Protection of Critical Infrastructure, hereinafter referred to as ‘the programme’, the purpose of which is to create conditions for the improvement of the security of critical infrastructure, in particular with regard to: preventing the disruption of critical infrastructure; preparing for emergencies that may adversely affect critical infrastructure; responding to situations of destruction or disruption of critical infrastructure and the restoration of critical infrastructure.

The instrument is divided into twelve parts, which include:

1. basic definitions;
2. scope;
3. objectives;
4. priorities and principles of the programme;

⁸ Article 2b of Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection, OJ of the European Union 23.12.2008, L 345/75.

⁹ Milewski, 2016; Szewczyk and Pyznar, 2010.

5. identification of critical infrastructure;
6. bodies and actors involved in the implementation of the programme;
7. their roles and responsibilities;
8. protection of critical infrastructures;
9. action plan for a period of 2 years following the adoption of the National Critical Infrastructure Protection Programme update by the Council of Ministers;
10. the international aspect of the protection of critical infrastructures;
11. evaluation of the effectiveness of the programme;
12. list of annexes.

The initial part of the document, namely point 1, presents basic definitions related to critical infrastructures including, inter alia, issues such as:

- CI system coordinator,
- CI protection (mandatory, specific),
- CI operator, crisis situation.

Among the main principles guiding the protection programme are: the principle of proportionality and risk-based action, recognition of differences between systems; the leading role of the minister in charge of the system; equality of operators and complementarity¹⁰.

At the end of 2018 and the beginning of 2019, a decision was taken on the need to amend Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection. The work led to the development of important legislation at European Union level, namely:

- Regulation of the European Parliament and of the Council (EU) on digital operational resilience for the financial sector;¹¹
- Directive concerning measures for a high common level of security of network and information systems across the Union (NIS2);¹²
- Directive on the resilience of critical entities (CER) Directive of 27 December 2022.¹³

¹⁰ It should be noted that there are approximately 760 objects classified as critical infrastructure facilities in Poland, the largest number of which are communication and energy supply facilities, vide: Karolewski, Rejman – Karolewska, 2015, p. 108.

¹¹ Regulation (EU) of the European Parliament and of the Council of 27 December 2022 on digital operational resilience for the financial sector (OJ EU L 333/1).

¹² Directive concerning measures for a high common level of security of network and information systems across the Union (NIS2) of 27 December 2022. OJ EU L 333/80.

Immediately prior to the promulgation of the aforementioned Directives, the Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure¹⁴. Inter alia, this recommendation identified issues relating to evolving threats such as the war in Ukraine. Point 5 of the recommendations highlights that “in view of the fast-evolving threat landscape, resilience-enhancing measures should be taken as a matter of priority in key sectors such as energy, digital infrastructure, transport and space, and in other relevant sectors identified by the Member States. Such measures should focus on enhancing the resilience of critical infrastructure taking into account relevant risks, especially cascading effects, supply chain disruption, dependence, impacts of climate change, unreliable vendors and partners, and hybrid threats and campaigns including foreign information manipulation and interference.” It also stressed that Member States should, in accordance with EU and national law, use all available tools to make progress and contribute to strengthening physical resilience and cyber resilience, as well as strengthening the ability to respond quickly and effectively to disruptions of critical services by critical infrastructure¹⁵.

An important aspect from the point of view of the national critical infrastructure is the proper cooperation and coordination between the authorities responsible for its security. It should be noted that these authorities are extremely numerous, hence there is need to develop appropriate protective procedures. In addition, only proper national legislation, coordinated with European acts, can ensure the proper operation of the relevant state services.

2. Authorities responsible for the protection of critical infrastructure

Given the thematic scope of this study, the main emphasis will be on issues related to the authorities that, within the scope of their powers, have competencies to ensure the protection of critical infrastructures and, in particular, the special services and the Government Security Centre.

¹³ Directive on the resilience of critical entities (CER) Directive of 27 December 2022. OJ EU L 333/164.

¹⁴ Council Recommendation of 8 December on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (2023/C 20/01).

¹⁵ Ibid paragraphs 7 and 12 of the Council Recommendations.

2.1 Ministers

According to the 2023 National Programme for the Protection of Critical Infrastructure, individual ministers have a specific role in protecting it. The table below shows the list of the ministers responsible for individual critical infrastructure systems.

Table 1 List of ministers responsible for individual critical infrastructure protection systems.¹⁶

Minister responsible for the critical infrastructure system	Critical infrastructure system
1. Minister responsible for state assets. 2. Minister responsible for energy. 3. Minister responsible for the management of mineral deposits.	Energy, energy resources and fuels supply system
1. Minister responsible for information technology. 2. Minister responsible for communications.	Communication system
1. Minister responsible for information technology.	ICT network system
1. Minister responsible for budget. 2. Minister responsible for public finance. 3. Minister responsible for financial institutions.	Financial system
1. Minister responsible for agriculture. 2. Minister responsible for agricultural markets.	Food supply system
1. Minister responsible for water management.	Water supply system
1. Minister responsible for health.	Healthcare system
1. Minister responsible for transport. 2. Minister responsible for maritime	Transport system

¹⁶ National Programme for the Protection of Critical Infrastructure, 2023, p. 18.

affairs.	
1. Minister responsible for home affairs.	Rescue system
1. Minister responsible for information technology.	System for continuity of public administration
1. Minister responsible for climate.	System for production, storage, warehousing and use of chemical and radioactive substances, including pipelines for hazardous substances

The above list of responsible ministers for individual critical infrastructure protection systems was amended by Resolution of the Council of Ministers No. 116/2020 of 13 August 2020 amending the resolution on the adoption of the National Programme for Critical Infrastructure Protection. As is apparent, one or several ministers may be charged with the responsibility for a particular protection system, depending on the competences assigned. Examples of such systems for which three ministers are responsible are the energy, energy resources and fuels supply system and the financial system.

2.2. Government Centre for Security (RCB)

The Government Centre for Security was established on the basis of Article 10 of the Act of 10 April 2007 on crisis management, which, as a budgetary unit, is subordinate to the Prime Minister. The Government Centre for Security is headed by a director, who is appointed by the Prime Minister.

The RCB's organisational units include:

- Analysis and Response Office, consisting of the Operations and Analysis Department and the Information Policy Department;
- Logistics and Finance Office consisting of Administration and Finance Department, IT and Communications Department, Accounting Department and an Independent Logistics Officer;
- Office of Civil Planning and Critical Infrastructure Protection, which is divided into:

- Department of Risk Assessment and Planning;
- Department of Critical Infrastructure Protection;
- Department of International Cooperation;
- Independent Protection and Control Office and independent position for legislative services.

This body provides services to the Council of Ministers, the Prime Minister, the team and the minister responsible for internal affairs in matters of crisis management and acts as a national crisis management centre. The basic tasks of the Government Centre for Security are described in Article 11(2) of the Act on crisis management. Thus, the tasks of the Government Centre for Security include:

1. civil planning, including:
 - a) outline specific ways and means of responding to and mitigating risks,
 - b) developing and updating the National Crisis Management Plan, in cooperation with the relevant organisational units of the offices serving ministers and heads of central offices,
 - c) analysing and assessing the possibility of risks or their development,
 - d) gathering information on risks and analysing the material collected,
 - e) drawing up conclusions and proposals for preventing and countering risks,
 - f) planning the use of the Armed Forces of the Republic of Poland to perform the tasks referred to in Article 25(3),
 - g) planning the support by public administration bodies of the implementation of the tasks of the Armed Forces of the Republic of Poland,
2. monitoring potential threats; agreeing crisis management plans drawn up by ministers in charge of government administration departments and heads of central offices,
3. preparing the activation, in the event of emergencies, of crisis management procedures; preparing draft opinions and positions of the team,
4. preparing and providing technical and organisational support for the work of the team,
5. ensuring the coordination of the information policy of public administration bodies during a crisis situation,
6. liaising with entities, cells and organisational units of the North Atlantic Treaty Organisation and the European Union and other

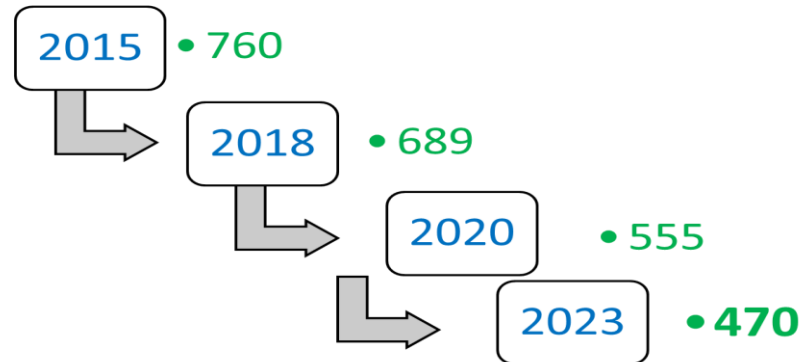
- international organisations responsible for crisis management and critical infrastructure protection,
7. organising, conducting and coordinating crisis management training and exercises and participating in national and international exercises,
 8. ensuring the circulation of information between national and foreign authorities and crisis management structures; implementation of the tasks of the standby duty within the framework of state defence readiness; implementation of tasks in the field of prevention, counteraction and elimination of the consequences of events of a terrorist nature
 9. cooperating with the Head of the Internal Security Agency in preventing, counteracting and removing the effects of terrorist incidents,
 10. implementation of planning and program tasks in the field of critical infrastructure protection and European critical infrastructure protection, including the development and updating of the functional annex to the National Crisis Management Plan on critical infrastructure protection, as well as cooperation, as a national point of contact, with the institutions of the European Union and the North Atlantic Treaty Organization and their member countries in the field of critical infrastructure protection,
 11. preparation of a draft ordinance of the Prime Minister referred to in Article 7(4) (list of undertakings and procedures of the crisis management system taking into account obligations resulting from membership in the North Atlantic Treaty Organization and bodies responsible for their activation).

The critical infrastructure protection plan should include elements such as: critical infrastructure characteristics (processes implemented, resources); risk assessment (hazard identification, risk analysis, risk assessment), essential options for action (procedures - response), cooperation with state authorities (at local, provincial, national level).

An important element in the scope of the RCB's activities is the need to prepare the National Programme for the Protection of Critical Infrastructure. In addition, the RCB performs the function of a national Crisis Management Centre.

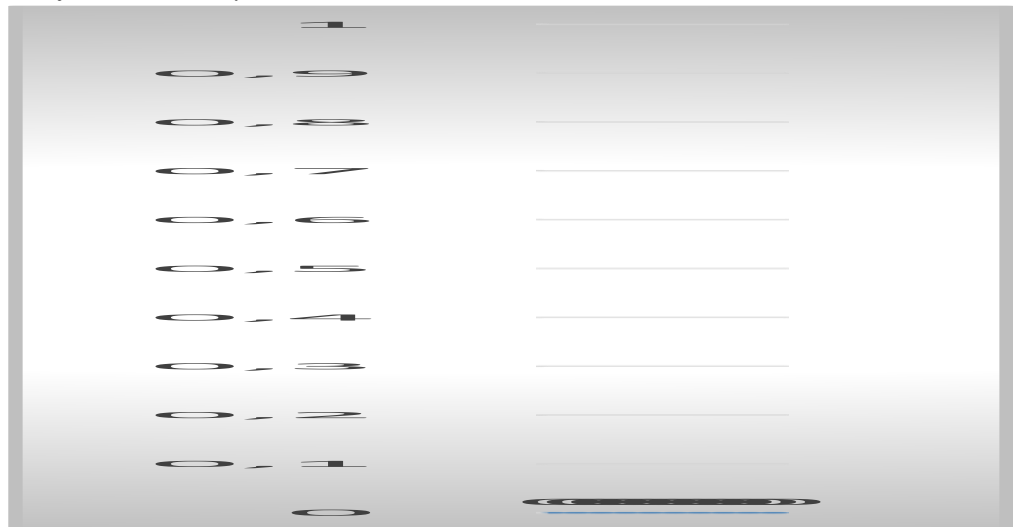
The chart below presents a list of critical infrastructure facilities in Poland.

Figure 1 Number of critical infrastructure facilities between 2015 and 2023.¹⁷



In turn, the chart below shows the quantitative distribution of critical infrastructure facilities in critical infrastructure systems in 2020.

Figure 2 Quantitative distribution of critical infrastructure facilities in critical infrastructure systems in 2020.¹⁸



¹⁷ GCS (Polish: RCB – Rządowe Centrum Bezpieczeństwa, [Online]. Available at: <https://www.gov.pl/web/rcb> (Accessed: 17 December 2024).

¹⁸ RCB, [Online]. Available at: <https://www.gov.pl/web/rcb> (Accessed: 17 December 2024).

- 252-energy supply infrastructure
- 124-telecommunication infrastructure
- 61-water supply infrastructure
- 57-transport infrastructure
- 23-infrastructure ensuring continuity
- 18-rescue infrastructure
- 17-financial infrastructure
- 8-ICT networks infrastructure
- 3-medical infrastructure
- 2-production and storage facilities.

As is apparent, the largest number of critical infrastructure facilities are energy supply and communications facilities (376 facilities out of 555). One of the most important organisational units of the RCB is the Operations and Analysis Department, which is part of the Analysis and Response Office. Its main tasks include: coordinating the circulation of information, monitoring and risk analysis, preparing and activating crisis management procedures. As was correctly ascertained in the Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, it contributes to broader efforts to counter hybrid threats and campaigns against the Union and its Member States. The need to ensure the protection of facilities and equipment belonging to critical infrastructure is a key guarantor of national security. The recent EU directives mentioned above indicate the importance of ensuring the protection of critical infrastructures, which directly translates into security in a global sense.

2.3. The Internal Security Agency (ABW)

One of the special services that plays a fundamental role in the security of the state, its constitutional order, including, inter alia, the protection of critical infrastructure, is the Internal Security Agency (ABW). It is a special service which was created on 29 June 2002¹⁹ after the dissolution of the Office of State Protection. As a result of the dissolution of the Office of State Protection, two civilian special services were separated, the Internal Security Agency and the Foreign Intelligence Agency.

¹⁹ Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, Journal of Laws of 2023, item 1136.

The tasks of the Internal Security Agency are set out in Article 5 of the Act, according to which the ABW is, *inter alia*, responsible for:

- 1) identifying, preventing and combatting threats to the internal security of the State and its constitutional order, and in particular to the sovereignty and international standing, independence and inviolability of its territory, as well as to the defence of the State;
- 2) the identification, prevention and detection of the following crimes:
 - (a) espionage, terrorism, unlawful disclosure or use of classified information and other offences against state security,
 - (b) crimes that harm the economic basis of the state,
 - (c) corruption of persons performing public functions, as referred to in Articles 1 and 2 of the Act of 21 August 1997 on restrictions on the conduct of business activities by persons performing public functions (Journal of Laws of 2022, item 1110, and of 2023, item 497), if this may harm state security,
 - (d) production and marketing of goods, technologies and services of strategic importance for state security,
 - (e) the illicit manufacture, possession and trafficking of arms, munitions and explosives, weapons of mass destruction and narcotic drugs and psychotropic substances, in international traffic,
 - (f) act against the administration of justice, referred to in Article 232, Article 233, Article 234, Article 235, Article 236 § 1 and Article 239 § 1 of the Act of 6 June 1997. - Criminal Code (Journal of Laws of 2022, item 1138, 1726, 1855, 2339 and 2600 and of 2023, item 289), if they remain in connection with the offences referred to in items (a)-(e) and prosecution of their perpetrators;
- 2a) identification, prevention and detection of threats to the security, relevant to the continuity of the state's functioning, of ICT systems of public administration bodies or ICT network system covered by the uniform list of objects, installations, devices and services constituting critical infrastructure, as well as ICT systems of owners and holders of objects, installations or devices of critical infrastructure, referred to in Article 5b (7) item 1 of the Act of 26 April 2007 on crisis management (Journal of Laws of 2023, item 122)²⁰;
- 2b) the disclosure of property threatened with forfeiture in connection with the offences referred to in point 2;

²⁰ Ibid.

- 3) carrying out, within the limits of its competence, tasks relating to the protection of classified information and performing the functions of a national security authority with regard to the protection of classified information in international relations;
- 4) obtaining, analysing, processing and transmitting to the competent authorities information likely to be of importance for the protection of the State's internal security and constitutional order;
- 5) undertaking other activities specified in separate acts and international agreements²¹.

Additionally, the activity of the Internal Security Agency outside the borders of the Republic of Poland may be carried out in connection with its activity on the territory of the State only within the scope of the performance of the tasks set out in section 1 item 2(3). The Head of the Internal Security Agency shall perform the tasks of the contact point for data exchange referred to in Article 16(3) of the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12)²².

With regard to the tasks of the Internal Security Agency, it is important to emphasise that the Constitutional Tribunal, in its ruling of 30 July 2014, expressed its opinion on Article 5(1)(2)(a) of the Act on Internal Security Agency and Foreign Intelligence Agency insofar as it includes the phrase "and other offences detrimental to state security", as well as on Article 5(1)(2)(c) of Act on Internal Security Agency and Foreign Intelligence Agency. This is attributable to the fact that the wording raised doubts as to the scope of the service's activities. In its judgment, it ruled, *inter alia*, that: "The values protected in Article 5 of the Internal Security Agency and Foreign Intelligence Agency Act are covered by the content of the following notions: state security, internal security of the state and its constitutional order, sovereignty and international position of the state, inviolability of its territory, defence of the state, economic basis of the state, as well as, *inter alia*, public morality and efficiency of functioning of state institutions, international legal obligations of the state with their axiological premises. By their very nature, these constitutionally significant values

²¹ Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, *Journal of Laws* of 2023, item 1136.

²² Article 16(3) of the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).

cannot be specified in detail in the law, hence the necessity for the legislator to use a general concept, ‘collecting’ specific values”²³.

2.4. ICT security

It is worth noting that one of the key tasks of the Internal Security Agency is to ensure the state’s ICT security. According to the Act of 21 December 2001 amending the Act on the organisation and operational mode of the Council of Ministers and the scope of ministers’ activities, the Act on divisions of government administration as well as amending some acts²⁴, the modern information and communication technologies include the need to ensure security of: IT infrastructure, ICT systems as well as networks and information technology, technology and IT standards.

Besides, it is necessary to support investments in the field of information technology, information education as well as ICT and multimedia services. At the same time, Poland is obliged to apply information technology in the information society, in particular in the economy, banking and education, and to fulfil the international obligations of the Republic of Poland in the field of information technology²⁵. In addition, in the Act of 5 August 2010 on the protection of classified information²⁶ in Chapter 8, one may discover in Articles 48-53, provisions on ICT security of systems and networks in which classified information is processed. Furthermore, in the Regulation of the Prime Minister of 20 July 2011 on basic requirements of information and communication security²⁷, one can find issues concerning the so-called electromagnetic protection of an information and communication system, which is intended to prevent and counteract a breach of confidentiality and availability of classified information processed in an information and communication system. An important aspect related to ICT security, is the possibility of a potential terrorist threat, which can trigger so-called network incidents. In this regard, the relatively newly enacted Act of 5 July 2018 on the national cyber security system²⁸, which implements Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning

²³ Judgment of the Constitutional Tribunal of 30 July 2014, ref. K 23/11.

²⁴ OJ. 2001, item 1800.

²⁵ Poterała, 2021.

²⁶ Journal of Laws of 2005, item 1631 as amended.

²⁷ OJ. 2011, item 948.

²⁸ OJ. 2020, item 1369.

measures for a high common level of security of network and information systems across the Union²⁹, plays a key role. Article 1 of the Act defines the organisation of the national cyber security system and the tasks and responsibilities of the entities comprising this system; the manner of supervision and control in the application of the provisions of the Act as well as the scope of the Cyber Security Strategy of the Republic of Poland. In addition, there are also defined basic concepts such as: cyber security, defined as the immunity of information systems to activities that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems, as well as incidents defined as an event that has or may have an adverse impact on cyber security, including their division into incidents: critical, serious and significant incidents³⁰. The ICT security system has been based on the so-called CSIRTs (Computer Security Incident Response Team). Within the scope of competence of the Head of the ABW remain ICT systems and ICT networks, covered by the uniform list of objects, installations, devices and services included in the critical infrastructure, referred to in Article 5b(7)(1) of the Act on crisis management. In addition, the ABW carries out its statutory tasks concerning terrorist incidents in cyberspace, as well as tasks of a preventive nature³¹.

2.5. Espionage and terrorism

On the basis of Article 5(1) (2a), the tasks of the Internal Security Agency also include the identification, prevention and detection of offences such as espionage and terrorism. The criminal threats for the crime of espionage are in turn described in Article 130 of the Criminal Code, according to which: “Whoever takes part in the activities of a foreign intelligence service or acts on its behalf, against the Republic of Poland, shall be subject to the penalty of deprivation of liberty for a term not shorter than 5 years (§ 1); Whoever, taking part in the activities of a foreign intelligence service or acting on its behalf, provides this intelligence service with information the transmission of which may cause damage to the Republic of Poland, shall be subject to the penalty of deprivation of liberty for a term not shorter than 8 years or life imprisonment (§ 2); Whoever declares readiness to act for the benefit of foreign intelligence against the Republic of Poland or in order to provide foreign intelligence with information the transmission of which may cause

²⁹ OJ EU L 194, 19.07.2016, p. 1.

³⁰ Article 2 of the Act of 5 July 2018 on the National Cyber Security System.

³¹ Poterała, 2021, pp. 89-117.

damage to the Republic of Poland, collects or stores such information or enters an information system in order to obtain it, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years (§ 3)".

In addition, subsequent articles provide for penalties for organising or directing the activities of a foreign intelligence service, for taking part in the activities of a foreign intelligence service not directed against the Republic of Poland and conducted on its territory without the consent of the competent authority granted under separate provisions, as well as for preparation for the aforementioned offences. In recent years, in connection with the intensification of intelligence activities mainly on the part of Russia, the legislator decided to increase the criminal threat for the offence of espionage. The offence of espionage has also been amended to comprise taking part in the activities of a foreign intelligence service or acting on its behalf, conducting disinformation by disseminating false or misleading information with the aim of causing serious disturbance to the system or economy of the Republic of Poland, an allied country or an international organisation of which the Republic of Poland is a member, or inducing a public authority of the Republic of Poland, an allied country or an international organisation of which the Republic of Poland is a member to take or refrain from taking certain actions.

Activities directly related to espionage are also acts of terrorism. Certainly, the enactment of the Act on anti-terrorist activities³² on 10 June 2016 was a great support for counter-terrorist activities. In this law, in addition to defining basic definitions such as anti-terrorist and counter-terrorist activities, there are also definitions concerning public administration infrastructure or indications concerning critical infrastructure which refer directly to the aforementioned Act of 26 April 2007 on crisis management. According to Article 3 paragraph 1, the Head of the Internal Security Agency, hereinafter referred to as the 'Head of the Internal Security Agency', is responsible for the prevention of terrorist incidents, in turn, the minister in charge of internal affairs is responsible for preparing to take control of terrorist incidents through planned undertakings, responding in the event of the occurrence of such incidents and restoring resources to respond to such incidents. The present Act has been divided into seven chapters, of which the provisions relating to actions to prevent terrorist incidents (Chapter 2), alert degrees (Chapter 3) as well as anti-terrorist

³² OJ 2021, item 2234 as amended.

actions at the scene of a terrorist incident, including counter-terrorist actions (Chapter 4) are of particular importance. Particularly important powers have been conferred on the Head of the Internal Security Agency in Article 9 of the cited Act. Pursuant to this provision, in order to recognise, prevent, combat and detect offences of a terrorist nature or an offence of espionage and to prosecute their perpetrators, the Head of the Internal Security Agency may order, for a period of no longer than 3 months, the discreet conduct of activities with regard to a person who is not a citizen of the Republic of Poland, with regard to whom there is a concern as to the possibility of his/her conducting terrorist activity or committing an offence of espionage, consisting of: obtaining and recording the content of conversations conducted by technical means, including by means of telecommunications networks, obtaining and recording images or sound of persons from premises, means of transport or places other than public places, obtaining and recording the content of correspondence, including correspondence conducted by means of electronic communication, obtaining and recording data contained on computer data carriers, telecommunications terminal equipment, information and data communication systems, gaining access to and controlling the contents of consignments.

An important role in combatting terrorist threats is played by the Anti-Terrorist Centre (CAT), established on the basis of: the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency, the Act of 10 June 2016 on anti-terrorist activities and Order No. 163 of the Prime Minister of 26 September 2018 on granting the statute of the Internal Security Agency.

The Anti-Terrorist Centre's role is to coordinate the process of information sharing between participants in the counter-terrorism defence system and to implement timely joint response procedures in the event of the occurrence of one of the four categories of defined threat: a terrorist event on Polish territory affecting the security of Poland and its citizens, a terrorist event occurring outside the borders of the Republic of Poland, affecting the security of the Republic of Poland and its citizens, obtain information on potential threats that may occur in Poland and abroad and obtaining information on 'money laundering' or financial transfers that may be indicative of the financing of terrorist activities³³.

The Centre operates on a 24/7 basis. The service in the unit is performed by officers, soldiers and civilian employees of national entities

³³ Obuchowicz, 2010, pp. 275 et seq.

dealing with counteracting terrorist threats, i.e. the Foreign Intelligence Agency, the Internal Security Agency, the Military Intelligence Service, the Military Counterintelligence Service. The service in this unit may also be performed by officers of: Polish National Police, Polish Border Guard, State Protection Service, State Fire Service, National Fiscal Administration, Military Police and the Government Security Centre³⁴. In addition to the Anti-Terrorist Centre, there is also the Terrorist Prevention Centre at the Internal Security Agency, which, being a specialised unit, deals with broadly understood anti-terrorist prevention³⁵.

It should also be added that on the basis of the Order of the National Public Prosecutor in the Mazovian Branch of the Department for Organised Crime and Corruption of the National Public Prosecutor's Office in Warsaw, the Espionage Unit was established on 24 September 2018. Prosecutors performing their duties in this division supervise proceedings conducted by the Internal Security Agency concerning crimes of espionage, disinformation and terrorist acts. In conclusion, it is worth noting that the most recent surveys on both terrorism in Poland and the directions of its development clearly indicate that

in the opinion of a large percentage of respondents, Poland may become an attractive country for terrorists. Although there has been little indication of this in recent years, the belief that the situation will deteriorate in the near future seems to be quite widespread. (...) Concerns are at least partly related to threats coming from Russia³⁶.

It is worth quoting the partial results of a survey conducted in April 2022 by Internal Security Agency officers among academics and representatives of services and institutions belonging to the anti-terrorism community involved in terrorism studies. The results of the survey clearly indicate that, according to the respondents, critical infrastructure facilities are the most 'popular' in the sphere of a terrorist attack within the European Union at 39.3%, followed by open urban spaces (32.9%), then by tourist infrastructure and sports facilities (14.8%), military bases (7.4%) and

³⁴ Kolaszyński, 1989, p.14.

³⁵ Available at: [https://CentrumPrewencjiTerrorystycznejABW\(tpcoe.gov.pl\)](https://CentrumPrewencjiTerrorystycznejABW(tpcoe.gov.pl)), (Accessed: 22 January 2024).

³⁶ Vidino, 2023, p. 254.

government office buildings (5.3%). On the other hand, in terms of the answer to the question: which tools, devices or technologies present the most significant security risks to citizens from the perspective of services, the largest group of respondents, 69.1%, answered that it is the unmanned aerial vehicles. When asked which terrorist organisation posed the greatest threat to the security of EU countries, the vast majority answered that it was ISIS (62.7%), followed by Al-Qaida (15.9%) and the Russian Federation's special services (11.7%). It is also worth noting the question related to the greatest technological challenge for ICT security services. According to respondents, these are: highly advanced control process automation technologies (35.1%), artificial intelligence (26.6%) and cloud storage (22.3%). This was followed by the development of 5G transmission standards (12.7%), quantum technology (2.1%) and encryption of communications (1%)³⁷.

3. Summary

The protection of critical infrastructures today is particularly important from the point of view of the society and has a transnational as well as a multidimensional dimension. Only a correct assessment of threats, their estimation and counteraction can lead to a reduction of the negative effects associated with the danger of their occurrence. Also of importance are the National Programmes for the Protection of Critical Infrastructure, which are prepared and adapted to current situations; the Government Centre for Security, which cooperates with ministers and heads of central offices competent in matters of national security, is responsible for drafting them. It is evident that only through mutual international cooperation and collaboration in the field of critical infrastructure protection can we effectively mitigate risks, enhance early detection capabilities, and prevent crises. To this end, it is necessary to ensure a common European security policy and, consequently, to develop legal solutions of an international and supra-regional nature. The dynamics of the change in today's security environment requires a systematic response and the introduction of new legal solutions. Examples of such solutions are, for example, those mentioned in this publication:

³⁷ Szlachter, 2022, pp. 148-185.

- Directive concerning measures for a high common level of security of network and information systems across the Union (NIS2) of 14 December 2022³⁸,
- Directive amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector
- Directive on the resilience of critical entities (CER) of 14 December 2022, repealing Council Directive 2008/114/EC³⁹.

Moreover, a key document of exceptional importance for the security of EU countries is the developed EU Security Strategy, which contains common assumptions for ensuring security.

An important aspect concerning the need to undertake urgent changes at least in the legislative field is the issue of the so-called hybrid threats. In 2016, the European Commission and the European External Action Service (EEAS) developed a Joint Framework on countering hybrid threats a European Union response, containing 22 actions to be taken by Union Member States and institutions to identify hybrid threats, raise awareness of these threats, and take steps to build resilience⁴⁰.

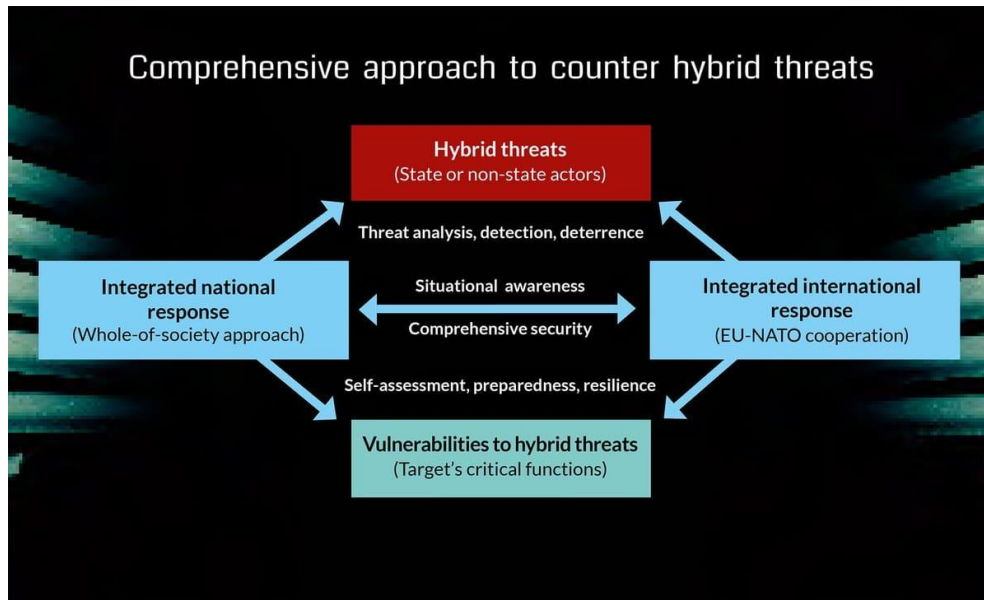
In April 2017, an agreement was signed in Helsinki about a centre to combat hybrid threats, of which Poland and 18 other countries are members. The main threats listed include propaganda threats, cyber threats and disinformation in the broadest sense. The chart below shows a comprehensive approach to hybrid threats.

³⁸ Directive concerning measures for a high common level of security of network and information systems across the Union (NIS2) of 27 December 2022. OJ EU L 333/80.

³⁹ Directive on the resilience of critical entities (CER) Directive of 27 December 2022. OJ EU L 333/164.

⁴⁰ Available at: <https://www.nato.int/docu/review/pl/articles/2018/11/23/> (Accessed: 23 January 2024).

Figure 3 Comprehensive approach to hybrid threats⁴¹



The demands made years ago on the need to develop IT-based threat knowledge management as well as the development of a risk assessment model to properly respond to possible threats seem right. Such a model can certainly contribute to the broader optics of managing the issues of possible threats⁴².

⁴¹ NATO, [Online]. Available at: <https://www.nato.int> (Accessed: 23 January 2024).

⁴² Trocicka, 2019.

Bibliography

- [1] Milewski, J. (2016) 'Identyfikacja infrastruktury krytycznej i jej zagrożeń. Systemowe wymogi bezpieczeństwa' [Identification of critical infrastructure and its threats. Systemic security requirements], *Zeszyty Naukowe AON*, 4(105), pp. 99-115.
- [2] Szewczyk, T., Pyznar, M. (2010) 'Ochrona infrastruktury krytycznej a zagrożenia asymetryczne' [Critical infrastructure protection against asymmetric threats], *Przegląd Bezpieczeństwa Wewnętrznego*, 2(2), pp. 55-56.
- [3] Karolewski, A., Rejman – Karolewska, M. (2015) 'Ochrona infrastruktury krytycznej, Przegląd naukowo – metodyczny' [Protection of critical infrastructure, Scientific and methodical review]. *Edukacja dla bezpieczeństwa*, 2/2015 (27), p. 108.
- [4] Potała, G. (2021) 'Zadania ABW w zakresie bezpieczeństwa teleinformatycznego państwa' [Tasks of the ABW in the field of information and communication security of the state] in: Burczaniuk, P. (ed.) *Prawne aspekty funkcjonowania służb specjalnych na przykładzie Agencji Bezpieczeństwa Wewnętrznego* [Legal aspects of the functioning of special services on the example of the Internal Security Agency]. Warszawa: DIG Publishing House, pp. 89-117.
- [5] Obuchowicz, M. (2010) 'Pięć lat funkcjonowania Centrum Antyterrorystycznego ABW (2008-2013)' [Five years of functioning of the ABW Antiterrorist Centre (2008-2013)], *Przegląd Bezpieczeństwa Wewnętrznego*, 10, pp. 275 et seq.
- [6] Kolaszyński, M. (2016) *Status ustrojowy polskich służb specjalnych po 1989 roku*. [Regime status of Polish secret services after 1989], Kraków: Jagiellonian University Publishing House.

-
- [7] Vidino, L. (2023) 'Badania ankietowe poświęcone terroryzmowi w Polsce i kierunkom jego rozwoju' [Survey research on terrorism in Poland and directions of its development], *Terroryzm, studia, analizy, prewencja* [Terrorism, studies, analysis, prevention], 2023(4), p. 254.
- [8] Szlachter, D. (2022) 'Terroryzm w Polsce i kierunki jego rozwoju. Wyniki badań ankietowych' [Terrorism in Poland and directions of its development. Survey results (abridged report)], *Terroryzm, studia, analizy, prewencja* [Terrorism, studies, analysis, prevention], 2022(2), pp. 148-185.
- [9] Trocicka, J. W. (2019) 'Metodyka typowania i szacowania ryzyka zagrożeń dla bezpieczeństwa państwa' [Methodology of typing and estimating the risk of threats to state security] in Kośmider, T., Kołtun, L. (eds.) *Współczesny wymiar bezpieczeństwa publicznego. Kształtowanie bezpiecznych przestrzeni. Działania profilaktyczne*. [Contemporary dimension of public security. Shaping safe spaces. Preventive actions], Warszawa: IWS Publishing House.

ANDRZEJ PAWLIKOWSKI*

The EU's defence ambitions in the field of defence technological and industrial development**

Abstract: The European Union (EU) has long aspired to bolster its defence capabilities, particularly in the realm of defence technological and industrial development. This study scrutinises the EU's evolving defence ambitions against the backdrop of a rapidly changing global security landscape. Faced with multifaceted security challenges and growing geopolitical uncertainties, the EU has embarked on a journey to enhance its strategic autonomy and bolster its defence industry's competitiveness. Through a comprehensive analysis of EU policy documents, defence strategies, and industrial initiatives, this study delineates the EU's efforts to foster innovation, collaboration, and interoperability within its defence ecosystem. Moreover, it explores the mechanisms employed by the EU to leverage synergies between civilian and military research, harness emerging technologies, and fortify its defence industrial base. By delving into the complexities of EU defence initiatives and their implications for transatlantic relations, regional security dynamics, and industrial cooperation, this study contributes to a nuanced understanding of the EU's quest for strategic sovereignty and technological prowess in an increasingly contested world.

Keywords: European defence policy, defence technological development, EU defence industry, defence innovation, defence self-sufficiency, EU

* University Professor, Director of the Strategic Studies Institute, National Security Faculty, War Studies University, Warsaw, Poland. <https://orcid.org/0000-0002-9449-1204>, a.pawlikowski@akademia.mil.pl.

** The research and preparation of this study was supported by the Central European Academy.

military cooperation, strategic defence technologies, EU arms industry, defence cybersecurity, critical infrastructure protection.

1. Introduction

In an era characterised by unprecedented geopolitical uncertainties and the continual evolution of security landscapes, the European Union (EU) stands at a critical juncture, compelled to redefine its defence ambitions in response to emerging challenges. This imperative arises from a complex interplay of factors, including geopolitical shifts, the rise of non-traditional threats, and the accelerating pace of technological advancements. The EU is actively steering itself towards a future characterised by enhanced autonomy and technological sophistication, recognising the indispensable role cutting-edge defence technologies play in ensuring not only the territorial integrity of its member states but also the overarching strategic interests of the EU.

The emergence of defence technologies is no longer merely a matter of military strategy; it has evolved into a strategic imperative essential for the very foundation of the EU's security architecture. As Europe grapples with an array of threats, ranging from conventional military challenges to cyberthreats and asymmetric warfare, the need for a robust defence technological and industrial base becomes increasingly paramount. This extended introduction seeks to delve deeper into the nuanced and intricate layers surrounding the development of defence technologies in Europe.

At its core, this exploration aims to unravel the historical trajectory that has shaped Europe's approach to defence, tracing the collaborative efforts originating in the aftermath of World War II. These historical roots laid the foundation for regional security alliances and paved the way for collective defence mechanisms that continue to evolve in response to contemporary challenges. By examining this historical continuum, we gain insights into the evolution of the European defence landscape and its adaptation to shifting global dynamics.

The contemporary challenges facing Europe are multifaceted and dynamic, requiring a multifaceted response. From traditional military threats to the complexities of hybrid warfare and intricacies of cyber-vulnerabilities, the security paradigm has become increasingly complex. Against this backdrop, the imperative for technological innovation in defence becomes not only strategic but also existential. Consequently, the EU is actively engaged in navigating these challenges by recognising the

critical need to fortify its defence capabilities through a holistic and forward-looking approach.

Considering these imperatives, this extended introduction sets the stage for a comprehensive exploration of Europe's defence ambitions. The subsequent sections will delve into specific aspects, including ongoing initiatives, collaborative projects, and the strategic vision underpinning the EU's endeavours. By scrutinising historical contexts, analysing contemporary challenges, and emphasising the indispensable role of a robust defence technological and industrial base, this study seeks to contribute to a nuanced understanding of Europe's trajectory towards a more secure, autonomous, and technologically advanced future.

2. Methodology and Selected Research Methods

This study's methodology is structured rigorously, beginning with the precise formulation of a research goal: to critically evaluate the strategic and defence frameworks within the EU, with an emphasis on fostering greater security and defence industrial cooperation among member states. The research identifies a central problem—fragmentation of defence policies across the EU—which complicates the integration of emerging technologies and strategic initiatives at the EU level. This problem is analysed systematically and its persistence is verified in the study's conclusions, which highlight the ongoing challenges in achieving a cohesive and unified European defence strategy despite numerous policy initiatives.

The research methods employed in the study are multifaceted and robust, combining both qualitative and quantitative approaches. The study undertakes a thorough analysis of historical developments in European defence policy, using a synthesis of geopolitical trends to inform strategic forecasting. This forecasting is underpinned by scenario planning and risk assessment techniques, which are designed to anticipate future security challenges and inform potential policy responses. The methodological framework also includes an examination of strategic documents, policy frameworks, and expert analyses, providing a comprehensive and nuanced understanding of the EU's evolving defence posture.

A critical examination of the sources reveals that the documents analysed are predominantly programmatic and strategic, reflecting the official policy objectives of the EU. These sources are essential for understanding the theoretical underpinnings of the EU's defence strategies.

However, they also carry inherent risks related to their implementation. The study acknowledges that while these documents outline ambitious goals and strategies, the realisation of these objectives is often hindered by practical challenges, such as political divergences among member states, economic constraints, and complex logistics of coordinating defence efforts across diverse national contexts. Thus, this study not only provides a critical analysis of existing strategies but also underscores the potential discrepancies between strategic planning and practical execution within the European defence framework.

3. Historical Perspective

The roots of Europe's defence endeavours lie within the tumultuous aftermath of World War II, a period marked by widespread devastation and a profound need for collaborative reconstruction and security efforts across the continent. The ravages of conflict served as a compelling catalyst for nations to recognise the imperative of unity in not only physically rebuilding their war-torn territories but also establishing a collective security apparatus that could safeguard against future threats. This pivotal juncture in history witnessed the birth of collaborative initiatives that laid the foundation for Europe's defence architecture.

One most significant milestone during this transformative period was establishment of the North Atlantic Treaty Organization (NATO) in 1949. NATO, formed by a coalition of European and North American nations, embodied a collective commitment to mutual defence against potential external aggressors. The alliance, with its cornerstone principle of collective defence, served to create a unified front against the backdrop of escalating Cold War tensions. NATO's formation represented a pivotal moment in European history, fostering solidarity and cooperation among nations with shared democratic values in the face of an ideologically divided world.

After NATO's establishment, Europe witnessed a series of regional security initiatives that further fortified the continent's collective defence mechanisms.¹ These initiatives were characterised by a commitment to cooperation and coordination, reflecting the shared understanding that security challenges transcended national borders. The evolving nature of these collaborative efforts not only responded to the immediate post-war

¹ Western European Union – 1954; European Union's Common Security and Defence Policy – 1999; Nordic Defence Cooperation – 2009; Baltic Defence Cooperation – 1994.

needs but also laid the groundwork for a resilient and adaptive defence framework capable of addressing the geopolitical shifts of the future.

Over the ensuing decades, the European defence landscape underwent transformative phases, each shaped by the prevailing geopolitical dynamics. The Cold War era, dominated by bipolar tensions between the Western and Eastern blocs, saw Europe as a focal point of global power struggles. The continent became a theatre where the ideological standoff manifested in military posturing, strategic alliances, and the constant spectre of nuclear conflict.

With the conclusion of the Cold War, Europe entered a new epoch marked by the dissolution of traditional alliances and emergence of a post-Cold War security paradigm. Shifting from a focus on deterrence and containment, the emphasis moved towards cooperative security. Nations sought to redefine their relationships, forge new alliances, and foster collaboration based on shared interests rather than ideological divides. This post-Cold War era witnessed the blossoming of cooperative initiatives, arms control agreements, and concerted efforts to address emerging threats through diplomatic means.

In essence, Europe's defence landscape is a tapestry woven with the threads of collaboration, adaptation, and resilience. From the immediate aftermath of World War II to the shifting alliances of the Cold War and the cooperative security initiatives of the post-Cold War period, the trajectory of Europe's defence endeavours reflect continual evolution in response to the dynamic geopolitical currents shaping the continent's destiny.²

4. Evolution of Defence Industries

The evolution of defence industries in Europe is intricately woven into the fabric of broader economic and political developments that have defined the continent's history. Throughout various epochs, defence industrial complexes have stood as pillars, not only contributing to the advancement of military capabilities but also playing pivotal roles in technological innovation, job creation, and regional stability. The symbiotic relationship between defence industries and the broader economic and political forces has often been a driving force in shaping the trajectory of European nations.

² See European Union, 2018; European Union External Action, 2021; NATO, 2012; NATO 2018; NATO, 2021.

Historically, defence industrial complexes emerged as catalysts for technological innovation, serving as incubators for cutting-edge advancements. The demands of military requirements often spurred research and development, leading to breakthroughs that eventually found applications beyond the defence sector. The defence industry's contribution to technological progress extended far beyond the battlefield, influencing civilian technologies and bolstering overall industrial competitiveness.

Moreover, defence-related projects have traditionally been engines for job creation, providing employment opportunities and contributing to economic growth. The scale and complexity of defence endeavours necessitate a skilled workforce, driving investments in education and training. This not only enhances technological expertise but also fosters a workforce capable of addressing broader societal challenges.

However, the landscape of defence industries in Europe has undergone profound shifts in response to changing global dynamics and the emergence of asymmetric threats. The once predominantly state-centric defence industrial complex has witnessed a transformation, with greater emphasis on collaboration between the public and private sectors. The evolving nature of security challenges, including cyberthreats, non-state actors, and unconventional warfare, has underscored the imperative for agility and technological sophistication in defence capabilities.

The need for technologically advanced defence capabilities has taken centre stage as Europe navigates a security environment marked by fluid geopolitical landscapes and unpredictable threats. The European defence sector faces the formidable task of adapting to these challenges, necessitating a paradigm shift in approaches to research, development, and innovation. The traditional defence industrial complex must evolve to embrace emerging technologies, leverage synergies with the civilian sector, and foster a culture of innovation that can swiftly respond to evolving security needs.

Amidst these challenges, ensuring continuous development of cutting-edge technologies becomes paramount. The European defence sector is tasked with balancing the dual objectives of enhancing security and maintaining economic competitiveness. Collaborative efforts between member states, strategic partnerships with industry leaders, and a commitment to research and development are crucial elements in overcoming these challenges.

In summary, the evolution of defence industries in Europe is a dynamic journey shaped by historical contexts, economic imperatives, and geopolitical realities. As Europe confronts the demands of a rapidly changing security landscape, the defence sector must adapt, innovate, and collaborate to ensure not only the continent's security but also its position at the forefront of technological progress and economic resilience.

5. Contemporary Challenges

The contemporary security environment in Europe unfolds against a backdrop marked by an intricate web of challenges, transcending conventional notions of military threats. The EU navigates through a landscape where traditional military challenges coexist with an array of unconventional, cyber, and hybrid threats. This multifaceted security matrix necessitates a holistic and adaptive approach, prompting the EU to confront the imperative of fortifying its defence capabilities to effectively safeguard against emerging threats.

Traditional military threats, while not diminishing in significance, now share the stage with a spectrum of non-traditional challenges. Unconventional warfare, characterised by asymmetric tactics employed by non-state actors, demands a recalibration of defence strategies. The ability to respond to irregular and unpredictable threats becomes imperative in maintaining regional stability and the protection of vital interests.

Furthermore, the advent of cyberwarfare has ushered in a new era of vulnerability, where digital infrastructure and interconnected systems are potential battlefields. The EU, like other global actors, must grapple with the constant evolution of cyberthreats that can undermine national security, economic stability, and even the functioning of critical infrastructure. Developing resilient cybersecurity measures becomes a crucial component of any comprehensive defence strategy.

Hybrid warfare, a blend of conventional and unconventional tactics, poses additional challenges. This form of warfare involves a combination of military, economic, and informational elements, often employed simultaneously to exploit vulnerabilities and achieve strategic objectives. The nuanced nature of hybrid threats demands a flexible and multifaceted defence posture, capable of responding to diverse challenges with agility and precision.

As the geopolitical landscape continues to evolve, the EU faces the urgent need to fortify its defence capabilities, to not only respond to current challenges but anticipate and address those that may emerge in the future. The interplay of technological advancements adds another layer of complexity to this imperative. Cutting-edge technologies, such as artificial intelligence, autonomous systems, and advanced sensors, offer both opportunities and challenges. The EU must harness the transformative potential of these technologies to enhance its defence capabilities while also navigating ethical considerations and potential risks.

Economic considerations further underscore the urgency for a coherent and forward-looking defence strategy. Investments in defence technologies not only contribute to security but also drive economic growth, foster innovation, and create high-skilled jobs. Striking a balance between economic viability and security imperatives becomes crucial in crafting a sustainable defence framework.

At the heart of this complex interplay lies the imperative for strategic autonomy. The EU seeks to assert its ability to act independently in matters of defence, reducing dependencies on external actors and ensuring self-sufficiency in critical areas. Achieving strategic autonomy requires a comprehensive understanding of evolving threats, a commitment to technological innovation, and a cohesive defence strategy that aligns with the broader geopolitical ambitions of the EU.

In conclusion, the contemporary security challenges facing Europe demand a comprehensive and dynamic response. The EU, recognising the multifaceted nature of threats, must fortify its defence capabilities through a combination of strategic foresight, technological innovation, and economic considerations. Crafting a coherent and forward-looking defence strategy is not merely a response to current challenges but a proactive endeavour to secure the future stability and resilience of the European continent in an ever-changing global landscape.

6. Imperative for Technological Advancement

In the dynamic landscape of the 21st century, technological innovation has surged forward at an unprecedented pace, ushering in breakthroughs across various domains such as artificial intelligence, cyber-capabilities, space exploration, and autonomous systems. Recognising the transformative potential inherent in these advancements, the EU has embarked on a

visionary journey to harness cutting-edge technologies, strategically integrating them to enhance its defence capabilities. This deliberate and forward-thinking approach is emblematic of the EU's commitment to not only adapt to the evolving security paradigm but actively shape it.

The intersection of civilian and military technologies has emerged as a focal point in the EU's pursuit of a technologically advanced defence apparatus. The emphasis on dual-use applications, which can simultaneously bolster economic competitiveness and security resilience, underscores the interconnected nature of contemporary challenges and opportunities. This holistic integration acknowledges that advancements in technology are not confined to the realm of defence alone; rather, they permeate every facet of the society and industry.

As the EU navigates the complexities and opportunities presented by these advancements, the development of defence technologies stands as a linchpin in shaping the future of European security. This exploration seeks to peel back the layers of Europe's defence ambitions, as not merely as a reactive response to immediate threats but also a proactive endeavour to position the continent at the forefront of global technological leadership.

The overarching goal of this study extends beyond mere analysis of current challenges; it aims to provide readers a comprehensive understanding of the historical evolution, current challenges, and future trajectories of Europe's defence capabilities. In doing so, it seeks to unravel the intricacies of how Europe, acting collectively, strategically positions itself amid the evolving geopolitical complexities that define the 21st-century security landscape.

Delving into the historical roots of collaborative defence efforts, this study scrutinises the multifaceted challenges posed by diverse security threats, from traditional to emerging unconventional forms. Furthermore, it emphasises the imperative for technological advancements, recognising that the ability to navigate and leverage cutting-edge technologies is integral to maintaining a robust defence posture.

The extended purpose of this study goes beyond a simple examination of defence technologies. It ventures into the intersections of defence and civilian technologies, acknowledging the dual-use potential that not only enhances security but also contributes significantly to economic competitiveness. By doing so, the study aims to unravel the strategic decisions, policy frameworks, and collaborative initiatives undertaken by the EU. These initiatives play a pivotal role in bolstering the EU's defence

technological and industrial base, aligning it with broader economic and strategic objectives.

As it addresses these multifaceted dimensions, the study aspires to foster a nuanced discourse on how Europe navigates the delicate balance between autonomy and collaboration. It recognises that achieving a technologically advanced defence apparatus requires a strategic blend of self-reliance and cooperative endeavours. The insights provided herein aim to serve as a valuable resource for policymakers, scholars, and stakeholders interested in deciphering the complexities and strategic considerations that underpin the EU's defence ambitions.

In conclusion, the extended purpose of this study transcends the immediate landscape of defence technologies; it contributes to informed discussions and insights that can actively shape the future trajectory of European defence endeavours. In an era marked by rapid technological advancements and dynamic geopolitical shifts, this exploration endeavours to be a beacon guiding the EU towards a future where technological innovation is woven seamlessly into the fabric of its security and strategic autonomy.

7. History and Background

Over the years, the concept of joint European defence activities has evolved in response to shifting geopolitical landscapes, security threats, and the imperative of fostering greater cooperation among European nations. This brief history delves into the trajectory of collaborative defence efforts within Europe, tracing the milestones and developments that have shaped the continent's approach to collective security and defence. From the aftermath of World War II to the present day, the journey of joint European defence activities is emblematic of the continent's ongoing quest for peace, stability, and resilience in an ever-changing global environment.

The past decade has marked a significant resurgence in European security and defence efforts, catalysed by pivotal events such as the December 2013 European Defence Summit. This summit served as a catalyst for a fresh wave of collaboration and coordination among European nations, signalling the dawn of a new era characterised by heightened defence cooperation. Amidst the backdrop of escalating geopolitical tensions and an array of challenges confronting Europe from various quarters, the unveiling of the EU Global Strategy in 2016 served as a pivotal

moment. This strategic blueprint, coupled with a flurry of initiatives launched in the aftermath of 2016, underscored the profound transformation underway in the EU's security and defence policy landscape. The EU's response to the evolving security landscape has been multifaceted, reflecting a proactive approach to addressing emerging threats and safeguarding the continent's stability. This period has witnessed a notable shift towards greater integration and solidarity among EU member states, with efforts aimed at bolstering collective defence capabilities and fostering strategic autonomy.

Furthermore, the post-2016 initiatives have sought to enhance interoperability among European armed forces, streamline defence procurement processes, and reinforce strategic partnerships with NATO and other key stakeholders. The emphasis on enhancing resilience, agility, and innovation has been central to the EU's endeavours in strengthening its security and defence architecture.

In response to the intricate geopolitical dynamics of the 21st century, the EU has acknowledged the necessity of adapting and enhancing its security stance to safeguard the interests of its member states and promote enduring peace and stability. The sustained momentum in European security and defence underscores a collective dedication to addressing contemporary challenges and fortifying the continent's resilience for the years ahead.

Illustrative of the EU's expanded aspirations in security and defence policy are pivotal initiatives such as the inception of Permanent Structured Cooperation (PESCO) in 2017, launch of the European Defence Fund (EDF) in 2019, and establishment of the Directorate-General for Defence Industry and Space (DG DEFIS) in 2021, among others. These initiatives exemplify the EU's proactive approach towards fostering greater cooperation, bolstering defence capabilities, and advancing strategic autonomy in safeguarding European interests and promoting global peace and security.³ All of these initiatives will have undeniable consequences for the EU's institutional identity and political transformation from a purely civilian international actor to a potential military and technological power on the international stage. Behind these various policy and institutional developments is an EU-led defence technological and industrial policy intended to shore up the European Defence Technological and Industrial Base (EDTIB). The above developments illustrate a metaphorical alignment of planets that created a favourable environment for defence industrial and

³ See European Commission, no date.

technological policymaking. Geopolitical pressure on Europe, and on larger EU member states in particular, encouraged them to shore up Europe's strategic autonomy in defence. These circumstances gave the European Commission a window of opportunity to take a more proactive role in security and defence technological and industrial matters. The EU's lack of domestic investment in defence, coupled with a growing sense of defensive regionalism regarding the United States, also contributed to this policy environment.

In this post-2016 alignment of interests, high-level European political and policy circles realised that advantages in cutting-edge defence and technological areas help define international influence and strategic autonomy.⁴

The EU's security and defence policy field has experienced increased funding and institutionalisation of security-oriented and defence research and development, including critical dual-use technologies. While acknowledging the link between EU defence and civilian science, technology, and innovation policies, this study focusses on the emergence of EU security and defence research and innovation policy.

The goal is to understand the roots, evolution, and multistakeholder representation leading to a supranational European defence research programme. Transnational interest groups, including security corporations, industry associations, and lobby groups, have played pivotal roles in shaping this development. However, civil society actors and elected representatives have been notably absent from these discussions, raising concerns about democratic accountability and oversight.

This raises significant democracy questions for the EU, especially as it considers transformative security and defence policy changes. Greater involvement of the European Parliament and national legislative bodies in decision-making is essential to ensure democratic legitimacy and transparency. Addressing these issues is crucial for the EU to maintain its identity as a promoter of peace and stability.

Even before the 1990s, the European Commission recognised the importance of preserving the competitiveness of the European defence industry, particularly as the geopolitical landscape began to shift with the end of the Cold War. In the 1970s and 1980s, the European Commission acknowledged the strategic importance of the defence sector, for not only security but also economic reasons, leading to efforts to harmonise defence

⁴See Csernaton, 2021; European Commission, 2021.

procurement policies and promote collaboration among member states' defence industries. In 1985, the European Commission's Communication on Industrial Policy underscored the need to support key sectors, including defence, as part of a broader strategy to enhance European technological capabilities and industrial competitiveness. By 1988, the European Commission had taken further steps by presenting a communication titled 'The European Arms Industry: The Need for Cooperation', which highlighted the necessity of cooperation among European countries to strengthen the competitiveness of the defence industry. This document advocated for reducing market fragmentation, promoting standardisation, and encouraging joint research and development among European defence firms, laying the groundwork for more integrated and competitive defence initiatives in the years to come. Efforts to coordinate defence industrial players with EU security, promote dual-use technological innovation, and advance defence research initiatives have been ongoing. The EU has emphasised the need to maintain the competitiveness of the European defence industry, shaping successive EU-level advisory bodies and influencing research and innovation policy agendas. Relationships between the European Commission, defence industry actors, and expert groups have significantly influenced the creation and priorities of EU security and defence research innovation programmes.⁵

In general, these linkages have actively influenced policy trajectories, often favouring specific stakeholders, and have seen a growing emphasis on dual-use research and capability development initiatives. Initially integrated into the EU's Framework Programmes, these projects have focussed on diverse technological domains such as space, border security, maritime surveillance, cybersecurity, and emerging technologies.⁶

Historical development of closer European security and defence industrial and technological cooperation is a complex affair.⁷ This has entailed intricate and interconnected EU-state-industry relations spanning multiple EU institutions, agencies, interest groups, and actors within the security and defence industrial sector. It also demonstrates member states' growing readiness to grant the EU a more substantial role in security and defence affairs. Considering the ongoing discussions regarding the EU's defence and technological autonomy, it is imperative to thoroughly outline

⁵ Karampekios and Oikonomou, 2018, p. 182.

⁶ See Csernatoni, 2016, pp. 174.

⁷ See Martins and Mawdsley, 2021, pp. 94.

the costs and benefits of European security and defence research and innovation programmes.⁸ Furthermore, it is essential to delve deeper into the contributions of various interest groups and EU institutions. This discussion is closely tied to a growing consensus among member states regarding the necessity for the EU's Common Security and Defence Policy (CSDP) to adopt a higher level of strategic ambition, recognising the advantages of establishing a European defence industrial and technological research and innovation policy.

However, establishment of a unified European approach to security and defence technological and industrial matters has faced challenges. Simultaneously, the European Commission's expanding competencies in these domains remain contentious among other EU institutions and member states. This sensitivity highlights the deeply rooted national protectionism surrounding security and defence issues, as well as the ongoing competition with organisations such as the European Defence Agency (EDA) in shaping the direction of the EU's security and defence policy agenda.⁹

In the aftermath of World War II, Europe faced the daunting task of rebuilding shattered economies and ensuring collective security against future threats. Establishment of institutions such as the European Coal and Steel Community in 1951 laid the groundwork for economic integration and cooperation, setting the stage for broader defence collaboration among European nations.

The onset of the Cold War heightened security concerns across Europe, leading to the formation of military alliances such as NATO in 1949. While NATO primarily focussed on collective defence against the Soviet bloc, it also served as a catalyst for defence industry cooperation among its member states, laying the foundation for future collaborative endeavours. Following the end of the Cold War, major crises such as the Kosovo War of the later 1990s forced Europe to integrate the security structures of the Western EU into the EU's institutional structures. This integration led to the creation of what then was called the European Security and Defence Policy, now known as the CSDP. The 2003 Iraq War facilitated the formulation of the EU's first programmatic document in security and defence, the European Security Strategy, which was followed in 2004 by the establishment of the EDA. Since its creation, the EDA's main purposes were to support members states in the improvement of European military

⁸ Csernaton, 2019, pp. 119–140.

⁹ Fiott, 2015, pp. 542–557.

capabilities, boost the continent's dormant defence industry and market, expand collaboration among member states on defence issues, and rationalise research and development in defence technologies.¹⁰ With consolidation of the policy, institutional, and strategic frameworks in the European Security and Defence Policy (now CSDP), EDA, and European Security Strategy, the political focus in Europe shifted towards capability development for such frameworks, as well as collaborative defence industrial projects and research-and-development initiatives. However, even though the European Security Strategy helped the EU articulate its normative and strategic goals and role in the world, and the EDA's creation responded to member states' need to address military capability shortfalls through closer cooperation, the EU still lacked proper coordination and harmonisation of the security and defence industrial and research efforts.¹¹ The Treaty of Lisbon, which entered into force in 2009, provided a legal framework for enhanced defence cooperation within the EU. This paved the way for the establishment of PESCO in 2017, marking a significant milestone in European defence integration. PESCO facilitates joint defence projects, fosters interoperability among armed forces, and promotes defence industry collaboration among participating EU member states.

In 2019, the EU launched the EDF as part of its efforts to strengthen the continent's defence industrial base and promote innovation in defence technologies. The EDF provides financial support for collaborative research-and-development projects, as well as for the acquisition of defence capabilities, thereby bolstering Europe's strategic autonomy and resilience in an increasingly uncertain security environment.

Recognising the growing importance of the defence sector in Europe's strategic agenda, the EU established the DG DEFIS in 2021. This dedicated body within the European Commission aims to coordinate and promote EU policies related to the defence industry, procurement, and space activities, underscoring the EU's commitment to nurturing a competitive and innovative defence industrial base.

These key moments illustrate the evolution of the defence industry within the EU, marked by milestones in cooperation, integration, and innovation aimed at strengthening Europe's defence capabilities and safeguarding its security interests.

¹⁰ Csernatoni, 2016, pp. 119–140.

¹¹ Oikonomou, 2023, pp. 178, 181.

8. Current Technological State in Defence

Analysis of the current technological status of the defence sector is paramount in understanding the evolving landscape of military capabilities, strategic priorities, and security challenges facing nations worldwide. As technology continues to advance at an unprecedented pace, its integration into defence systems and operations has become increasingly vital for ensuring national security and maintaining military superiority. In this examination, we delve into the latest trends, innovations, and developments shaping the defence sector's technological landscape. From breakthroughs in artificial intelligence and cyberwarfare to advancements in aerospace and unmanned systems, the defence industry is undergoing a profound transformation driven by rapid technological advancements.

Moreover, with the emergence of new threats such as hybrid warfare, terrorism, and asymmetric conflicts, there is growing emphasis on leveraging cutting-edge technologies to enhance situational awareness, decision-making capabilities, and operational effectiveness on the battlefield. This analysis aims to provide insights into the key technological trends and challenges confronting the defence sector today. By understanding the current technological status, policymakers, military leaders, and defence industry stakeholders can better anticipate future needs, opportunities, and risks, thereby ensuring that defence capabilities remain aligned with evolving security dynamics in an ever-changing global landscape.

Identifying key areas of technological development is essential for understanding the trajectory of innovation, anticipating future trends, and strategically allocating resources to drive progress in various industries. In this analysis, we explore the pivotal domains where technological advancements are shaping the present and future landscape of innovation. From artificial intelligence and machine learning to biotechnology, renewable energy, and beyond, the pace of technological evolution is unprecedented, offering both opportunities and challenges across sectors. By identifying the key areas of technological development, stakeholders can gain insights into emerging trends, potential disruptions, and areas ripe for investment and collaboration. This analysis aims to shed light on the most promising domains of technological advancement, considering their implications for industries, economies, and societies at large. By recognising these key areas of development, policymakers, business leaders, and

innovators can harness the power of technology to drive sustainable growth, address pressing challenges, and foster a more prosperous and resilient future.

9. Challenges Facing the Defence Industry

The defence industry in the EU faces myriad challenges that pose significant implications for security, innovation, and economic competitiveness. In this discussion, we explore the primary obstacles confronting the defence sector within the EU and their broader ramifications. From budget constraints and technological gaps to geopolitical uncertainties and regulatory complexities, the defence industry grapples with multifaceted challenges that demand strategic foresight and coordinated action. These hurdles not only impact the ability of EU member states to safeguard their national security but also influence the continent's role as a global player in defence and security affairs. Since the European Council declared in 2013 that 'defence matters' for Europe, the EU has gained new momentum in defence cooperation. After decades of reducing national defence expenditures in the post-Cold War era—a decline exacerbated by the global financial crisis of 2008—the EU and its member states found themselves under pressure to coordinate defence policy, spending, and procurement at the EU level. The current moment in European defence integration unfolds against the backdrop of growing geostrategic threats, increasing instability in the EU's neighbourhood, competition among major powers, a fierce global race in technological innovation, and (lately) repercussions of the coronavirus pandemic.¹² These structural challenges have created an opportunity for a new work ethos among EU institutions, security entities, industry, and member states, aiming for closer cooperation in security and defence in areas of grand policy.¹³ This represents a significant shift from the EU perspective, as security and defence issues have traditionally been the exclusive prerogative of national sovereignty and operated within the intergovernmental decision-making process in the EU rather than within the supranational approach adopted in other areas.

Creating a more cohesive and integrated EU vision on security and defence is part of broader efforts to mitigate new security threats and hybrid challenges arising from an increasingly competitive geopolitical context and

¹² Csernatoni, 2020.

¹³ James, 2018, pp. 18, 23.

evolving technological trends. The aim is to find practical solutions that enhance the EU's role as a security guarantor, both within member states and globally.¹⁴ Various policy documents¹⁵ have indicated that for the EU to become a more strategic global defence actor, it will need a stronger European defence industry and defence market that can address gaps in expected military capabilities as well as increased spending on research and innovation in border security and defence.¹⁶ To safeguard Europe's independence as well as its "way of life and values"—whatever that phrase may signify in terms of normative identity—its strategic autonomy in security matters and defence technologies will be crucial. Since the early 2000s, the European Commission has been crafting a narrative legitimising this trend. It has underscored the benefits of pursuing a more coordinated security research programme at the EU level, encouraging Europe to leverage its technological assets and potential opportunities offered by new technological trends.

Civil, security, and defense applications increasingly rely on the same technological foundation, creating new synergies across different research sectors. Utilizing technology as a facilitator for creating a secure Europe requires cutting-edge branches of industry, robust knowledge infrastructure, adequate funding, and optimal resource utilization. Europe boasts high-quality research institutes and a significant and diverse industrial base that can meet technological requirements in the security domain. However, structural deficiencies at the institutional and political levels hinder Europe from harnessing its scientific, technological, and industrial potential. The division line between defense and civilian research, lack of detailed frameworks for security research at the EU level, limited cooperation among member states, and lack of coordination between national and European efforts exacerbate the lack of public funding for research and pose serious obstacles to delivering cost-effective solutions.¹⁷

This text is as relevant now as it was at the time of its publication in 2004. Ultimately, through "creating new synergies across different research sectors" and "between defence research and civilian research," earlier and current thinking has supported efforts to enhance civil-military innovation

¹⁴ See European Commission, 2016a.

¹⁵ See European Commission, 2016b; European Commission, 2019; European Defence Agency, no date; European Union External Action, 2016.

¹⁶ Hill, 1993, pp. 305–328.

¹⁷ See European Commission, 2004.

and deepen cross-border technological and industrial integration in European security and defence.¹⁸ Such thinking would likely breathe new life into the European political project as it emphasises goal convergence. Member states are seeking political (and financial) investments at the EU level. Meanwhile, the European Commission has underscored greater efficiency and regulation of the market regarding security and defence expenditures. As mentioned earlier, this alignment of planets has occurred at a much-needed time for European security and defence initiatives.

This discussion aims to dissect the main challenges faced by the defence industry in the EU, shedding light on their origins, impacts, and potential pathways for mitigation. By addressing these challenges head-on, policymakers, industry leaders, and stakeholders can work towards fostering a more robust and resilient defence ecosystem capable of meeting the evolving security needs of Europe and beyond.

The analysis of security threats requiring new technologies is imperative for understanding the evolving landscape of global security challenges and developing innovative solutions. In this discussion, we delve into the pressing security threats facing nations worldwide and the corresponding need for advanced technologies to address them effectively. From cyberattacks and terrorism to geopolitical tensions and hybrid warfare, the spectrum of security threats is diverse and dynamic. Traditional approaches to defence and security are increasingly inadequate in the face of the emerging risks and evolving tactics employed by adversaries. As such, there is growing recognition of the necessity for novel technologies to bolster defence capabilities, enhance resilience, and safeguard national interests.

This analysis aims to explore the security threats driving the demand for new technologies, examining their nature, implications, and potential countermeasures. By identifying these threats and understanding their technological requirements, policymakers, military leaders, and industry stakeholders can prioritise research, development, and deployment efforts to address the most critical security challenges of the 21st century.

10. European Defence Ambitions

Presentation of the EU's defence goals within the context of European Defence Ambitions is crucial for understanding the collective aspirations

¹⁸ Iraklis Oikonomou, 2012, pp. 179–181.

and strategic objectives of European nations in the realm of security and defence. In this presentation, we explore the overarching goals and aspirations of the EU in strengthening its defence capabilities and promoting stability in the region. Against the backdrop of evolving security threats and geopolitical dynamics, the EU has articulated ambitious defence objectives aimed at enhancing strategic autonomy, fostering greater cooperation among member states, and reinforcing Europe's role as a credible security actor on the global stage. These goals are encapsulated within the framework of European Defence Ambitions, which outlines the collective vision and priorities for European defence cooperation.

This presentation aims to elucidate the key elements of the EU's defence goals, highlighting their alignment with European Defence Ambitions and their significance in addressing contemporary security challenges. By articulating these objectives and aspirations, the EU seeks to forge a more secure and resilient Europe while advancing its interests and values in an increasingly complex and uncertain world.

The analysis of strategic defence documents within the context of European Defence Ambitions provides valuable insights into the overarching vision, priorities, and strategic objectives of the EU in the realm of defence and security. In this analysis, we delve into the key strategic documents that guide the EU's defence policies and initiatives, examining their alignment with the broader framework of European Defence Ambitions. As Europe confronts myriad security challenges ranging from traditional military threats to hybrid warfare, terrorism, and cyberattacks, the EU has articulated a comprehensive approach to bolstering its defence capabilities and safeguarding its interests. Central to this approach is the concept of European Defence Ambitions, which seek to enhance European strategic autonomy, strengthen defence cooperation among member states, and promote a more integrated and capable European defence.

Through the analysis of strategic defence documents such as the EU's Global Strategy, the Capability Development Plan, and European Defence Action Plan, we aim to elucidate how these documents contribute to the realisation of European Defence Ambitions. By examining the goals, priorities, and initiatives outlined in these documents, we can gain a deeper understanding of the EU's vision for defence cooperation and efforts to address the evolving security landscape in Europe and beyond.

11. Technological and Industrial Initiatives

In the context of the EU's defence ambitions and emergence of defence technological and industrial development, several specific projects and initiatives have been launched to bolster Europe's defence capabilities. These endeavours aim to enhance the EU's autonomy in defence technology and reduce its reliance on external actors. Here are some notable examples:

- **EDF:** EDF is a flagship initiative designed to support collaborative defence research-and-development projects among EU member states. It provides funding to consortia composed of companies' research institutions and defence agencies to develop cutting-edge defence technologies and capabilities. The EDF aims to foster innovation, strengthen industrial cooperation, and enhance Europe's defence industrial base.
- **PESCO:** PESCO is a framework for enhanced defence cooperation among EU member states that are committed to jointly developing military capabilities. Under PESCO, participating countries collaborate on various defence projects, including the development of next-generation weapons systems, cyber-defence capabilities, and strategic transport aircraft. PESCO aims to promote interoperability, improve efficiency, and increase the effectiveness of European defence efforts.
- **European Defence Industrial Development Programme:** This programme is a funding mechanism aimed at supporting the development of defence technologies and capabilities within the EU. It provides grants to projects that contribute to the advancement of key defence priorities such as cybersecurity, unmanned systems, and space-based assets. Further, this programme aims to strengthen Europe's defence industrial base, stimulate innovation, and enhance competitiveness of the European defence sector.
- **EDTIB:** The EDTIB initiative seeks to promote collaboration and integration within the European defence industry. It encompasses efforts to harmonise defence procurement policies, facilitate cross-border cooperation, and promote the sharing of defence research-and-development resources. The EDTIB aims to ensure the sustainability, resilience, and competitiveness of Europe's defence industrial base in the face of evolving security challenges.

- **EDA Initiatives:** The EDA plays a central role in coordinating and facilitating defence cooperation among EU member states. EDA oversees various initiatives aimed at enhancing defence capabilities, such as collaborative research projects, capability development programmes, and defence technology initiatives. The EDA works to foster synergy efficiency and innovation across the European defence landscape.

These projects and initiatives underscore the EU's commitment to advancing its defence technological and industrial development agenda, thereby strengthening Europe's ability to address emerging security threats and safeguard its strategic interests. By investing in innovation, collaboration, and capability development, the EU aims to build a more resilient and autonomous defence posture in an increasingly complex geopolitical environment.

International cooperation in the field of defence plays a crucial role in promoting security stability and peace among nations. Through collaborative efforts, countries can address common security challenges, mitigate threats, and enhance their defence capabilities. Here is an analysis of international cooperation in defence:

- **Shared Security Challenges:** Many security challenges that nations face today transcend borders and require collective responses. Threats such as terrorism, cyberattacks, proliferation of weapons of mass destruction, and transnational organised crime cannot be tackled effectively by individual countries alone. International cooperation allows nations to pool resources, expertise, and intelligence to address these shared challenges comprehensively.
- **Alliance and Partnership Building:** Alliances and partnerships are fundamental pillars of international defence cooperation. Formal alliances, such as NATO, and regional security arrangements, such as the ASEAN Defence Ministers' Meeting, foster trust, interoperability, and collective defence among member states. Bilateral partnerships between countries also contribute to mutual security interests through joint exercises, intelligence sharing, and defence technology collaboration.
- **Peacekeeping and Conflict Resolution:** International cooperation in peacekeeping missions is vital for resolving conflicts and promoting stability in regions affected by violence and instability. United Nations peacekeeping operations, often conducted with contributions from

multiple countries, help mitigate conflicts, protect civilians, and facilitate post-conflict reconstruction. Cooperation among regional organisations such as the African Union and EU further enhances peacekeeping efforts by leveraging regional expertise and resources.

- **Arms Control and Non-Proliferation:** Multilateral agreements and treaties play a critical role in arms control and non-proliferation efforts. Treaties such as the Treaty on the Non-Proliferation of Nuclear Weapons and Chemical Weapons Convention aim to prevent the spread of weapons of mass destruction and promote disarmament. International cooperation is essential for verifying compliance with these agreements through inspections, monitoring, and intelligence sharing.
- **Defence Trade and Technology Transfer:** Defence trade and technology transfer agreements facilitate the exchange of defence equipment, technology, and expertise among nations. These agreements strengthen defence industrial bases, promote innovation, and enhance interoperability among partner countries' armed forces. However, they also raise concerns about arms proliferation technology leakage and national security risks, necessitating careful regulation and oversight.
- **Humanitarian Assistance and Disaster Relief (HADR):** International cooperation in HADR operations is vital for providing timely assistance to countries affected by natural disasters, humanitarian crises, and emergencies. Military forces often play a significant role in these operations, providing logistical support, medical assistance, and disaster response capabilities. Multinational exercises and training enhance interoperability and coordination among military forces, enabling more effective HADR responses.

In conclusion, international cooperation in the field of defence is essential for addressing shared security challenges, promoting peace and stability, and enhancing collective security. By working together, nations can leverage their strengths, resources, and expertise to build a safer and more secure world for all.

12. Using Innovation in European Security

The discussion surrounding the impact of technological innovations on the effectiveness of European security activities is paramount in understanding

the evolving landscape of security challenges and responses within the EU. In this discussion, we explore how advancements in technology shape the capabilities, strategies, and outcomes of security efforts undertaken by European nations and institutions. From artificial intelligence and big data analytics to cybersecurity, surveillance technologies, and unmanned systems, technological innovations have revolutionised the way security activities are conducted and managed. These innovations offer unprecedented opportunities to enhance situational awareness, improve response times, and mitigate emerging threats in a rapidly evolving security environment.

European defence industry consortia have played a leading role in influencing EU initiatives in developing capabilities and shaping the parameters of the EU's research-and-development policy in the field of security and defence.¹⁹ This is not surprising, as states have long viewed the existence of strong and competitive defence technological and industrial bases as a strategic and military advantage in both peacetime and wartime. The challenge for the EU, and especially the European Commission, has been the Europeanisation of defence research and innovation, as well as regulation of the European defence industry market and technological base.²⁰ In particular, it would have to deal with the costs of defence "outside of Europe"—that is, the costs of operating at the national level rather than the European level.²¹ It is estimated that the cost of "lack of Europe" in defence ranges from €130 billion (almost \$148 billion) at the upper end to at least €26 billion (over \$29 billion) in more conservative calculations.²² Another challenge for EU member states is accepting the constraints of national industrial bases amid decreasing budgets for research, development, and public procurement, as well as ensuring global competitiveness through regional cooperation and cross-border armament collaboration.

With specialised knowledge, resources, and experience in close collaboration with EU member states and national supply chains, as well as a long history of European defence programmes such as the Eurofighter combat aircraft and A400M military transport aircraft, the European defence industry has recognised opportunities through cooperation. It is well-

¹⁹ Akkerman, 2018, pp. 254; Karampekios, Oikonomou, and Carayannis, pp. 343.

²⁰ Renaud Bellais, 2018, pp. 104-107.

²¹ See Ballester, 2013, pp. 117-121.

²² *Ibid.*

prepared to translate security and defence goals and interests into policy outcomes in research and technological development at the EU level. This functional relationship is most evident in the work of the European Commission and major branches of the defence industry and arms manufacturers towards the establishment of European research programmes in the field of security and defence. One key structural issue for the European defence industry is that it currently does not invest enough in research and development in relative terms: aerospace and defence companies spend less on research and development as a percentage of revenue compared to software or technology firms. In 2017, Amazon became the global leader in research-and-development spending, surpassing Alphabet (Google's parent company) and Intel.²³ Alongside Apple and Microsoft, these companies spend billions of dollars on research and development. Amazon alone spends more on research and development than the entire global aerospace and defence industry. Over time, these changes could weaken the market position of the defence industry.

The workforce in the industry also poses a challenge for the future, as a significant portion of the defence contract workforce consists of older employees nearing retirement. This phenomenon, known as "segment reversal," is a common pitfall for mature industries where market leaders opt not to compete with new entrants in non-core segments.²⁴ The defence industry faces the risk of falling behind in new and emerging technologies and losing future market share. Young talent in the information technology and engineering fields is also more attracted to the civilian sector and technology platform companies, which offer higher salaries and a more stimulating work environment.

Overall, European Commission President Ursula von der Leyen has called for the establishment of a 'geopolitical commission'.²⁵ High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the European Commission Josep Borrell stated that the EU must 'learn the language of power' and create more strategic autonomy in defence to ensure industrial, technological, digital, and economic independence.²⁶

²³ See Fox, 2021.

²⁴ See Gons et al., 2018.

²⁵ See European Commission, 2020.

²⁶ See Borrell, no date.

Moreover, as Europe grapples with diverse security challenges ranging from terrorism and organised crime to hybrid warfare and cyberattacks, the role of technological innovations becomes increasingly indispensable in safeguarding the continent's security interests. However, technological advancements also present ethical, legal, and societal implications that must be considered carefully to ensure responsible and effective security practices.

This discussion aims to explore the multifaceted impact of technological innovations on European security activities, examining both their potential benefits and challenges. By understanding the nexus between technology and security, policymakers, law enforcement agencies, and defence organisations can harness the power of innovation to bolster Europe's security resilience and uphold its commitment to peace, stability, and prosperity.

The exploration of successes resulting from new technologies in the field of defence provides invaluable insights into the transformative impact of innovation on military capabilities and strategic outcomes. In this discussion, we delve into notable examples of how technological advancements have yielded significant successes and advancements in defence operations and capabilities. From precision-guided munitions and unmanned aerial vehicles to advanced surveillance systems and cybersecurity solutions, new technologies have revolutionised the modern battlefield, offering enhanced precision, efficiency, and adaptability to military forces. These successes not only underscore the potency of innovation in enhancing defence capabilities but also highlight the imperative for continuous investment and integration of cutting-edge technologies into military strategies and operations.

By examining concrete examples of successes stemming from new technologies in defence, we aim to elucidate the tangible benefits and strategic advantages afforded by innovation in the military domain. From improved situational awareness and decision-making to enhanced deterrence and operational effectiveness, these successes serve as compelling illustrations of the transformative power of technology in shaping the future of defence.

This discussion seeks to shed light on the profound impact of technological advancements on defence capabilities and outcomes, inspiring further exploration and investment in innovation to meet the evolving security challenges of the 21st century.

13. Conclusions and Future Prospects

The study delves into the EU's overarching objectives concerning the advancement of its defence capabilities, particularly within the realms of technology and industrial development. Central to these ambitions is the recognition that a robust defence infrastructure is vital for ensuring the security and sovereignty of EU member states. This entails reducing dependency on external sources for defence technology and equipment, thereby fostering greater autonomy and resilience in the face of emerging threats and geopolitical uncertainties. The primary focus is on fostering technological innovation within the EU's defence sector. Recognising the pivotal role of cutting-edge technology in modern warfare, there is a concerted effort to invest in research-and-development initiatives. By nurturing indigenous capabilities in defence technology, the EU aims to stay at the forefront of innovation, thereby bolstering its overall defence posture. Moreover, the study underscores the importance of fostering industrial cooperation among EU member states. Collaborative ventures offer a pathway to pooling resources, expertise, and infrastructure, thereby enhancing efficiency and cost-effectiveness in defence production processes. This cooperation not only strengthens the industrial base but also contributes to fostering a sense of solidarity and mutual trust among EU nations.

Integral to achieving these objectives is the imperative of integration and coordination among EU member states. Standardisation, interoperability, and harmonisation of defence procurement processes are essential elements in this regard. By aligning their defence strategies and capabilities, EU nations can maximise synergies, streamline operations, and optimise resource allocation.

However, the study also acknowledges the challenges inherent in pursuing such ambitious defence ambitions. Budgetary constraints, varying national priorities, and divergent strategic interests among member states pose significant hurdles. Overcoming these challenges necessitates political will, compromise, and a long-term commitment to the collective defence agenda. Nevertheless, amidst these challenges lie ample opportunities for the EU to bolster its defence capabilities. Collaborative ventures offer economies of scale, enabling cost savings and resource optimisation. Furthermore, collective security arrangements provide a framework for

mutual defence and solidarity, thereby enhancing overall security of the region.

Looking ahead, this study envisions a dynamic landscape characterised by continued evolution in defence technology and strategy. Geopolitical developments, emerging threats, and technological advancements will shape the trajectory of the EU's defence agenda. Consequently, close collaboration, strategic foresight, and adaptability will be paramount in navigating these complexities and safeguarding European security in an ever-changing global environment.

In conclusion, as we look towards the future, there are several potential directions for the development of the defence industry within the EU. First, continued investment in research and development will be paramount to ensure that the EU remains at the forefront of technological innovation in defence. This includes advancing areas such as artificial intelligence, cyber-defence, and unmanned systems, which are likely to play increasingly significant roles in modern warfare. Furthermore, enhancing industrial cooperation and integration among EU member states will remain crucial. Collaborative ventures not only offer economies of scale but also foster a sense of unity and solidarity among European nations. This can be achieved through initiatives such as joint procurement programmes, shared defence projects, and standardised interoperability frameworks.

Moreover, the EU should prioritise efforts to address strategic challenges such as hybrid warfare, terrorism, and cyberthreats. This may involve strengthening intelligence-sharing mechanisms, enhancing resilience against cyber-attacks, and investing in capabilities for rapid response and crisis management. Additionally, the EU should continue to explore opportunities for international collaboration and partnerships in defence. Engaging with key allies and partners around the world can facilitate knowledge exchange, interoperability, and burden-sharing, thereby enhancing collective security.

Ultimately, future development of the defence industry within the EU will be shaped by a combination of technological advancements, geopolitical dynamics, and strategic imperatives. By embracing innovation, fostering cooperation, and adapting to emerging threats, the EU can position itself as a leading force in ensuring the security and stability of the region in the years to come.

Bibliography

- [1] Akkerman, M. (2016) *Border Wars: The Arms Dealers Profiting from Europe's Refugee Tragedy*. Stop Wapenhandel and Transnational Institute.
- [2] Akkerman, M. (2018) ' Militarization of European Border Security' in Karampekios, N., Oikonomou, I., Carayannis, E. (eds.) *The Emergence of EU Defense Research Policy*, pp. 337-355; https://doi.org/10.1007/978-3-319-68807-7_18.
- [3] Ballester, B. (2013) *The Cost of Non-Europe in Common Security and Defence Policy*. Brussels: European Parliamentary Research Service [Online]. Available at: [https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/494466/IPOL-JOIN_ET\(2013\)494466_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/494466/IPOL-JOIN_ET(2013)494466_EN.pdf) (Accessed: 03 March 2025).
- [4] Bellais, R. (2018) 'The Economic Imperative of Europeanizing Defense Innovation' in Karampekios, N., Oikonomou, I., Carayannis, E. (eds.) *The Emergence of EU Defense Research Policy*, pp. 93–109; https://doi.org/10.1007/978-3-319-68807-7_6.
- [5] Besch, S. (2019) *Can the European Commission Develop Europe's Defense Industry?*, Center for European Reform [Online]. Available at: https://www.cer.eu/sites/default/files/insight_SB.18.11.19.pdf (Accessed: 03 March 2025).
- [6] Béraud-Sudreau, L., Alice Pannier, A. (2020) 'An 'Improbable Paris-Berlin Commission Triangle': Usages of Europe and the Revival of EU Defense Cooperation After 2016', *Journal of European Integration*, 43(3), pp. 295–310; <https://doi.org/10.1080/07036337.2020.1740215>.
- [7] Bigo, D., Jeandesboz, J. (2010) *The EU and the European Security Industry: Questioning the 'Public Private Dialogue,'* Centre for European Policy Studies, Brussels, February 26, 2010.

-
- [8] Bigo, D., Jeandesboz, J., Martin-Maze, M., Ragazzi F. (2014) *Review of Security Measures in the 7th Research Framework Programme FP7 2007–2013*, European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs. [Online]. Available at: [https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509979/IPOL-LIBE_ET\(2014\)509979_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/509979/IPOL-LIBE_ET(2014)509979_EN.pdf) (Accessed: 03 March 2025).
- [9] Borrell, J. (no date) *A window on the world* [Online]. Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/77199/window-world-personal-blog-hrvp-josep-borrell_en (Accessed: 03 March 2025).
- [10] Calcara, A. (2017) 'State-Defence Industry Relations in the European Context: French and UK Interactions with the European Defence Agency', *European Security*, 26(4), pp. 527–551.
- [11] Calcara, A. (2020) 'The European Defence Agency and the Subcommittee on Security and Defence: A 'Discursive Coalition' for EU Defence Research' in Calcara, A., Csernatoni, R., Lavallée, *Emerging Security Technologies and EU Governance*, pp. 23–42; <https://doi.org/10.4324/9780429351846-2>.
- [12] Calcara, A. (2020) *This Franco-Italian Naval Deal Is a Litmus Test for European Strategic Autonomy*, War on the Rocks.
- [13] Chappell, L., Exadaktylos, T., Petrov, P. (2020) 'A More Capable EU? Assessing the Role of the EU's Institutions in Defense Capability Development', *Journal of European Integration*, 42(4), pp. 583–600.
- [14] Citi, M., (2014) 'Revisiting Creeping Competences in the EU: The Case of Security R&D Policy', *Journal of European Integration*, 36(2), pp. 135–151.

- [15] Csernatoni, R. (2019) 'Between Rhetoric and Practice', *Critical Military Studies*, 7(3), pp. 1-25; <https://doi.org/10.1080/23337486.2019.1585652>.
- [16] Csernatoni, R. (2018) 'Constructing the EU's High-Tech Borders', *European Security*, 27(2), pp. 175-200; <https://doi.org/10.1080/09662839.2018.1481396>.
- [17] Hoijtink, M. (2014) 'Capitalizing on Emergence: The 'New' Civil Security Market in Europe', *Security Dialogue*, 45(5), pp. 458-475; <https://doi.org/10.1177/0967010614544312>.
- [18] Csernatoni, R. (2016) 'Defending Europe: Dual-Use Technologies and Drone Development in the European Union', *Focus Paper*, No. 25 (Brussels: Centre for Security and Defence Studies, Royal Higher Institute for Defence).
- [19] Csernatoni, R. (2016) *Defending Europe: Dual-Use Technologies and Drone Development in the European Union*. Brussels: Centre for Security and Defence Studies, Royal Higher Institute for Defence [Online]. Available at: <https://www.defence-institute.be/wp-content/uploads/2020/04/fp-35.pdf> (Accessed: 03 March 2025).
- [20] Csernatoni, R., Laïci, T. (2019) *Empowering the European Parliament: Toward More Accountability on Security and Defense*. Carnegie Endowment for International Peace [Online]. Available at: <https://carnegieendowment.org/research/2020/07/empowering-the-european-parliament-toward-more-accountability-on-security-and-defense?lang=en¢er=europe> (Accessed: 03 March 2025).
- [21] Csernatoni, R., Martins, B. O. (2019) *The European Defence Fund: Key Issues and Controversies*, PRIO Policy Brief 3, Oslo: PRIO.

- [22] Csernatoni, R. (2019) *The Democratic Challenge of EU Defense Policy*, Strategic Europe blog, Carnegie Endowment for International Peace [Online]. Available at: <https://carnegieendowment.org/europe/strategic-europe/2019/11/the-democratic-challenge-of-eu-defense-policy?lang=en> (Accessed: 03 March 2025).
- [23] Csernatoni, R. (2019) 'Between Rhetoric and Practice: Technological Efficiency and Defence Cooperation in the European Drone Sector', *Critical Military Studies*, 7(3), pp. 1-25; <https://doi.org/10.1080/23337486.2019.1585652>.
- [24] Csernatoni, R., (2020) EU Security and Defense Challenges: Toward a European Defense Winter? Carnegie Europe [Online]. Available at: <https://carnegieendowment.org/research/2020/06/eu-security-and-defense-challenges-toward-a-european-defense-winter?lang=en¢er=europe> (Accessed: 03 March 2025).
- [25] Csernatoni, R. (2021) 'Constructing the EU's High-Tech Borders: FRONTEX and Dual-Use Drones for Border Management', *European Security*, 27(2), pp. 175–200.
- [26] Csernatoni, R. (2021) *The EU's Rise as a Defense Technological Power: From Strategic Autonomy to Technological Sovereignty* Carnegie Endowment for International Peace. [Online]. Available at: <https://carnegieendowment.org/research/2021/08/the-eus-rise-as-a-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty?lang=en¢er=europe> (Accessed: 03 March 2025).
- [27] Csernatoni, R. (2021) *The EU's rise as a defense technological power: From strategic autonomy to technological sovereignty* [Online]. Available at: <https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134> (Accessed: 03 March 2025).

- [28] Edler, J., James, A. D. (2015) 'Understanding the Emergence of New Science and Technology Policies: Policy Entrepreneurship, Agenda Setting and the Development of the European Framework Programme', *Research Policy*, 44(6), pp. 1252–1265.
- [29] Fiott, D. (2015) 'Technopolitik': Europe, Power and Technology', *European Geostrategy*, 7(53).
- [30] Fiott, D. (2015) 'Interview with Jorge Domecq, Former Chief Executive of the European Defence Agency', *European Geostrategy*. [Online]. Available at: <https://researchportal.vub.be/nl/publications/interview-with-jorge-domecq> (Accessed: 03 March 2025).
- [31] Fiott, D., Bellais, R. (2016) *A 'Game Changer'? The EU's Preparatory Action on Defence Research*, ARES Policy Paper, Paris: Institut de Relations Internationales et Stratégiques.
- [32] Fiott, D. (2015) 'The European Commission and the European Defence Agency: A Case of Rivalry?', *JCMS: Journal of Common Market Studies*, 53(3), pp. 542–557.
- [33] Fiott, D. (2019) *The Scrutiny of the European Defence Fund by the European Parliament and National Parliaments* – Study Requested by the European Parliament's Security and Defence Subcommittee, Directorate General for External Policies Policy Department," European Parliament.
- [34] Fiott, D. (2020) 'Financing Rhetoric? The European Defence Fund and Dual-Use Technologies' in Calcara, A., Csernatoni, R., Lavallée, C. (eds.) *Emerging Security Technologies and EU Governance: Actors, Practices and Processes*, London: Routledge.
- [35] Fontelles, J., B. (2020) *Why European Strategic Autonomy Matters*. [Online]. Available at: https://www.eeas.europa.eu/eeas/why-european-strategic-autonomy-matters_en (Accessed: 03 March 2025).

- [36] Fox, J. (2021) *Amazon spends millions on R&D. Just don't call it that*. Bloomberg [Online]. Available at: <https://www.bloomberg.com/opinion/articles/2021-02-11/amazon-spends-billions-on-r-d-just-don-t-call-it-that> (Accessed: 03 March 2025).
- [37] Gons, E., Ketzner, L., Carson, B., Peddicord, T., Mallory, G. (2018) *How AI and robotics will disrupt the defense industry* [Online]. Available at: <https://www.bcg.com/en-be/publications/2018/how-ai-robotics-will-disrupt-defense-industry> (Accessed: 03 March 2025).
- [38] Hayes, B. (2005) *NeoConOpticon: The EU Security-Industrial Complex*, Statewatch and the Transnational Institute. [Online]. Available at: <https://www.statewatch.org/media/documents/analyses/neoconopticon-report.pdf> (Accessed: 03 March 2025).
- [39] Haroche, P. (2020) 'Supranationalism Strikes Back: A Neofunctionalist Account of the European Defence Fund', *Journal of European Public Policy*, 27(6), pp. 853–872.
- [40] Håkansson, C. (2021) 'The European Commission's New Role in EU Security and Defense Cooperation: The Case of the European Defence Fund', *European Security*, 30(4), pp. 589–608; <https://doi.org/10.1080/09662839.2021.1906229>
- [41] Hill, C. (1992) 'The Capability-Expectations Gap, or Conceptualizing Europe's International Role', *JCMS: Journal of Common Market Studies*, 31(3), pp. 305–328.
- [42] James, A. D. (2004) 'European Defence Research and Technology (R&T) Cooperation: A Work in Progress', in Bialos, J. P., Koehl, S. (eds.) *European Defence Research and Development: New Visions and Prospects for Cooperative Engagement*, Baltimore: Johns Hopkins University Press, pp. 123–145.

-
- [43] James, A., D. (2006) 'The Transatlantic Defence R&D Gap: Causes, Consequences and Controversies', *Defence and Peace Economics*, 17(3), pp. 223–238.
- [44] James, A. D. (2017) 'Policy Entrepreneurship and Agenda Setting: Comparing and Contrasting the Origins of the European Research Programmes for Security and Defense' in Karampekios, N., Oikonomou, I., Carayannis, E. G. (eds.) *The Emergence of EU Defense Research Policy*, pp. 15-43; https://doi.org/10.1007/978-3-319-68807-7_2.
- [45] Jehin, O. (2010) *European Defence Economy Affected by the Crisis*, IFRI Bulletin.
- [46] Jones, C. (2009) *Market Forces: The Development of the EU Security-Industrial Complex*, Statewatch and the Transnational Institute.
- [47] Karampekios, N., Oikonomou, I. (2003) *The European Arms Industry, the European Commission and the Preparatory Action for Security Research: Business as Usual?* in Karampekios, N., Oikonomou, I., Carayannis, E. G. (eds.) *The Emergence of EU Defense Research Policy*, pp. 181-204; https://doi.org/10.1007/978-3-319-68807-7_10.
- [48] Karampekios, N., Oikonomou, I., Carayannis, E. G., (2018) 'Conclusion', in Karampekios, N., Oikonomou, I., Carayannis, E. G. (eds.) *The Emergence of EU Defense Research Policy*.
- [49] Klepsch, E., A., Normanton, T. (1979) *Two-way Street– Klepsch Report: Europe–United States Arms Procurement*, London: Brassey's.
- [50] Lemberg-Pedersen, M. (2013) 'Private Security Companies and the European Borderscapes' in Gammeltoft-Hansen, T., Nyberg Sørensen, N. (eds.) *The Migration Industry and the Commercialization of International Migration*, London: Routledge, pp. 152–172.
- [51] Martins, B., O., Küsters, C. (2019) 'Hidden Security: EU Public Research Funds and the Development of European Drones', *JCMS: Journal of Common Market Studies*, 57(2), pp. 278–297.

-
- [52] Martins, B. O., Mawdsley, J. (2021) 'Sociotechnical Imaginaries of EU Defence: The Past and the Future in the European Defence Fund', *JCMS: Journal of Common Market Studies*, 59(6), pp. 1458-1474; <https://doi.org/10.1111/jcms.13197>.
- [53] Martins, B., O., Ahmad, N. (2020) 'The Security Politics of Innovation: Dual-use Technology in the EU's Security Research Programme', in Calcara, A., Csernaton, R., Lavallée, C. *Emerging Security Technologies and EU Governance*, pp. 58-74.
- [54] Mawdsley, J. (2017) 'The Emergence of the European Defence Research Programme', in Karampekios, N., Oikonomou, I., Carayannis, E. G. (eds.) *The Emergence of EU Defense Research Policy*, pp. 205-217; https://doi.org/10.1007/978-3-319-68807-7_11.
- [55] Mörth, U., Britz, M. (2004) 'European Integration as Organizing: The Case of Armaments', *JCMS: Journal of Common Market Studies*, 42(15), pp. 957-973.
- [56] Morth, U. (2000) 'Competing Frames in the European Commission - The Case of the Defence Industry and Equipment Issue', *Journal of European Public Policy*, 7(2), pp. 173-189.
- [57] Oikonomou, I. (2009) 'Protect European Citizens and the European Economy: The European Security Research Programme', *Studia Diplomatica: The Brussels Journal of International Relations*, 62(1), pp. 3-16.
- [58] Oikonomou, I. (2012) 'A Historical Materialist Approach to CSDP' in Xymena Kurowsla, X., Bereuer, F. (eds.) *Explaining the EU's Common Security and Defence Policy: Theory in Action*, London: Palgrave, pp. 179-181.
- [59] Oikonomou, I. (2023) "A Historical Materialist Approach to CSDP".
- [60] Rosen S. J. (1973) *Testing the Theory of the Military-Industrial Complex*, Lanham, MD: Lexington Books.

- [61] Schmitt, B. (2023) *Armaments: New Opportunities, New Challenges*, Newsletter 8, European Union Institute for Security Studies.
- [62] Slijper, F. (2005) 'The Emerging EU Military-Industrial Complex: Arms Industry Lobbying in Brussels', *TNI Briefing Series*, No 2005/1, Transnational Institute and Campagne tegen Wapenhandel.
- [63] Ballester B. (2013) *The Cost of Non-Europe in Common Security and Defence Policy*. Brussels, European Parliamentary Research Service [Online]. Available at: [europarl.europa.eu/RegData/etudes/etudes/join/2013/494466/IPOL-JOIN_ET\(2013\)494466_EN.pdf](https://europarl.europa.eu/RegData/etudes/etudes/join/2013/494466/IPOL-JOIN_ET(2013)494466_EN.pdf) (Accessed: 14 April 2024).
- [64] European Parliament, *Review of Security Measures in the Research Framework Programme*, Directorate General for Internal Policies; and Hayes, 'NeoConOpticon'. [Online]. Available at: *Review of Security Measures in the 7th Research Framework Programme FP7 2007-2013*.
- [65] EOS 'White Paper' Towards Holistic European Security and a Competitive European Security Industry: EOS Support to the Comprehensive Assessment of the EU's Security Policies (2017) [Online]. Available at: <https://www.eos-eu.com/Files/Homepage-docs/EOS%20White%20Paper%20on%20EU%20Security%20Union%20June%202017.pdf> (Accessed: 03 March 2025).
- [66] ESRAB (2006) *Meeting the Challenge: The European Security Research Agenda*, Kooperationsstelle EU der Wissenschaftsorganisationen. [Online]. Available at: [am608418Int.indd](#) (Accessed: 03 March 2025)
- [67] Fontelles, J., B. A *Window on the World* blog [Online]. Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/77199/window-world-personal-blog-hrvp-josep-borrell_en (Accessed: 22 April 2024).

- [68] SPIDER project, *Sensor Platform & Network for Indoor Deployment and Exterior-based Radiofrequency (SPIDER)* [Online]. Available at: https://eda.europa.eu/docs/default-source/documents/pp-spider-projectweb_v4.pdf (Accessed: 03 March 2025).
- [69] Tindemans L. (1996) *European Union*. Report by Mr. Leo Tindemans, Prime Minister of Belgium, to the European Council,” Bulletin of the European Communities, Supplement 1/76. [Online]. Available at: http://aei.pitt.edu/942/1/political_tindemans_report.pdf (Accessed: 28 March 2024).

IZTOK PREZELJ*

Challenges in the Use of Artificial Intelligence-enabled Systems in Modern Armed Forces**

ABSTRACT: The application of Artificial Intelligence (AI) in the armed forces brings about a number of new possibilities and also new risks. In this paper, we have identified and analysed a wide range of risks associated with uncontrolled and unstoppable development of general AI, as well as several ethical and legal, operational and strategic risks. We have shown how and why these risks are dangerous and some even pose a threat to human security, values, norms, democracy, human rights, etc. These risks need to be carefully examined in order to improve the military use of AI and regulation in this area. The wide range of risks identified and their extremely diverse nature show that regulating the military use of AI will be difficult and complex, requiring all disciplines of law, and that regulatory rules need to be applied at national, regional and global level. The rapid development of military AI suggests that some risks are likely to be considered and regulated before any malicious military use of AI occurs, while unfortunately some others will only be regulated after the first instances of its malicious and illegal use by some armed forces.

KEYWORDS: artificial intelligence, risks, military, ethics, legal, strategic, operational, technology.

* Dean of the Faculty of Social Sciences, University of Ljubljana, Slovenia.
iztok.prezelj@fdv.uni-lj.si.

** The research and preparation of this study was supported by the Central European Academy.

Introduction

Artificial intelligence (AI) is a relatively new computer technology that attempts to emulate complex human behaviour in some or all aspects, such as understanding or discovering meaning, linking information from different sources, recognising patterns, generalising, drawing conclusions, learning from experience, predicting, and adapting to changing circumstances. AI has become a technological source of the ongoing Revolution in Military Affairs¹ and a great hope for improving military capabilities or even redistributing the balance of military power on a global scale. The defence industries of richer, technologically more developed and more ambitious states are increasingly investing many resources in the development of new AI-enabled military capabilities in the areas of intelligence and surveillance, data-driven decision making or command and control, targeting, manoeuvring and other actions of military autonomous systems, cyber warfare and cyber security, logistics, training and exercises, etc. The application of AI in the armed forces brings with it a wide range of new opportunities on the one hand and many new risks and challenges on the other.

The aim of this paper is to identify and analyse some key challenges of the (potential) use of AI in modern armed forces. We argue that a responsible authorisation for the use of AI in armed forces and security services requires a thorough knowledge and investigation of the main application challenges in order to prevent various negative scenarios. Specifically, we argue that the main AI-related risks in this area are risks associated with the uncontrolled and unstoppable development of general AI, various ethical and legal risks, operational and strategic risks. The range of these risks is so wide that it will be difficult to address them

¹ The concept of the Revolution in Military Affairs refers to technological, organisational, structural, doctrinal, and operational profound, radical, discontinuous, non-incremental, and possibly disruptive changes. Four RMAs have been broadly discussed in the literature (see Thiele, 2021a: 65-69), such as RMA I (emerging from the second half of WWI in the form of combat vehicles), RMA II (based on the insurgent way of war in Asia), RMA III (focused around the use of nuclear weapons and other long-range means of delivery in the Cold War), and RMA IV (focusing on the digitalisation capabilities, including computers, precision-guided munitions, active and passive sensors, cyberspace, C4 and robotics. RMA V is the next RMA that will be brought by new technologies.

comprehensively. In the process of research, we used comprehensive literature review, case analysis, risk identification and synthesis.

The discussion about the use of AI usually narrows down to a debate between the proponents of AI, who emphasise the positive benefits, such as faster operations, reduction of own casualties, risk of errors, etc., and the opponents of AI, who emphasise the disadvantages, such as possible unintended consequences, the risk of violating existing laws and norms or even the supremacy of AI over humans. Any warnings from opponents or “doomers” should be carefully considered and used to better regulate the use of AI by armed and security forces.

1. General challenges of the difficult implementation of artificial intelligence in armed forces

The implementation of AI in the armed forces will be slower than expected, but still relatively fast. The implementation of previous RMAs has encountered some reality tests, and we foresee a similar outcome for the AI aspect. According to Horowitz, current progress in integrating AI into military systems has been only incremental, and organisations are struggling to make the leap from development to operational implementation. Debates about the development of AI technology reveal a high degree of uncertainty about the potential pace of progress in AI. Modern armed forces face technological and organisational obstacles to the effective use of AI. The technological challenges can be divided into two broad categories: internal reliability problems and external exploitation problems. On the one hand, internal problems relate to the enormous complexity of the modern battlefield, to which AI narrow systems cannot adapt, which can lead to accidents and errors. Reliability and trust will play a crucial role in opening up the armed forces to the use of AI. Practice has shown that AI systems can sometimes exhibit uncertain behaviour and this might not be tolerated by most armed forces. On the other hand, external problems could be the adversarial data problem or the problem of attempts of the enemy to poison the data. Before being introduced to operational use, armed forces will want AI systems to be noticeably better than existing systems. The armed forces will also have to weigh up capabilities and reliability against the risks It

seems that forces facing defeat will be more willing to take the risks of using AI and vice versa.²

Another implementation problem is that AI will not be integrated into military systems and platforms at the same time or with the same effectiveness or efficiency. The idea that AI will automatically supplement existing dysfunctional security systems and bring a new form of objectivity is wishful thinking. In military operations, the dependence on AI must be carefully calibrated. Armed forces will have to decide to what extent and how quickly historically evolved organisational structures and doctrines should be replaced by new, technology-centric concepts.³

Human absorption barriers will also play an important role. Studies on the use of AI in the civilian environment show that personal values and attitudes strongly affect readiness to use AI and trust in AI. They show that extroverted people often have negative feelings towards AI, agreeable people see it as positive and useful, neurotic people experience negative emotions but perceive AI as socially friendly, conscientious people as useful but less socially friendly, while open-minded people as very useful.⁴ Other studies have shown that more trusting people (within other people) tend to trust AI more than less trusting people⁵ and that geographical location and even religious orientation influence the trust in or fear of AI (e.g. respondents from East Asia are less afraid of AI than Europeans, Muslims and Buddhists are more afraid of AI).⁶

An example of implementation problems can be found in the US, where the National Security Commission on Artificial Intelligence expressed frustration with the level of AI-readiness in the US security administration, acknowledging that the integration of AI in all sectors is difficult due to some unique challenges. One of the most significant challenges and impediments for AI development is the holy grail of rare talent that will enable AI breakthroughs. Accordingly, there is a deficit of human talent in the U.S. government. New talent pipelines need to be built, such as the new Digital Service Academy and the civilian National Reserve, to grow talent with the same seriousness as military officers. The US has

² Horowitz, 2018, pp. 5-6.

³ Mashur, 2019, p. 4.

⁴ Park and Woo, 2022.

⁵ Schepman and Rodway, 2023.

⁶ Mantello et al., 2023. The authors of this study published in the journal *AI & Society* reached this conclusion based on the survey of 1.015 responses of future job-seekers from 48 countries.

also noted that some of its agencies have made great strides in adopting AI, putting them ahead of other agencies. The commission's report also stressed that in this situation, it is not time for incremental changes, such as increasing budgets and creating a few new positions at the Pentagon and Silicon Valley, but that it is time to fundamentally change the mindset.⁷

Finally, the armed forces and defence institutions still do not have sufficient amount of big data to adequately train AI models. At the 'NATO in the Nordics' conference, it was highlighted that in one exercise, 26 platoons were monitored by numerous sensors (locations, communications, etc.) continually and this was only a fraction of the data necessary. There is a great need to collect more data from existing military exercises. AI is currently more of a training object and not a serious tool.⁸

As with all promising game changing technologies in RMAs, AI will be slowly introduced in the armed forces, but also much faster than other new technologies in the past. An evolutionary approach with some leaps is to be expected instead of a real revolution.

2. A broad spectrum of challenges in the use of artificial intelligence by the armed forces

The existing literature increasingly addresses a wide range of risks and concerns about the use of AI. For example, Encyclopedia Britannica lists the following ethical and socio-economic risks of AI: increased unemployment for certain job profiles (although AI will create certain new jobs), ingrained social biases (gender bias, racial bias, etc.), privacy risks (large amounts of data can be accessed by unauthorised organisations and people), and the risk of manipulation of images, creation of fake profiles, etc.⁹ In this paper, we are interested in the risks posed by the use of AI in the defence and military sectors.

Various categories of observers have warned against the use of AI in general and in the military sphere. Firstly, in an open letter in 2015 groups of scientists and technologists, for example, warned against the AI arms race and the potential spread of lethal AI to terrorists and dictators. The letter also called for a ban on offensive autonomous weapons beyond meaningful human control. Secondly, groups of employees at technological companies

⁷ Final Report, 2021, p. 3, 8, 110.

⁸ Schuller, 2023.

⁹ Artificial Intelligence, 2023.

called against the production of weaponised robots and similar warfare technology. Google¹⁰ consequently published its AI guiding principles, in which it pledged not to design or deploy weapons that cause injury to people, technologies that gather or use information for surveillance violating internationally accepted norms, and not to develop technologies that violate generally accepted international law and human rights, despite its continued cooperation with the US government. International campaigns such as the International Campaign for Robot Arms Control and the Campaign to Stop Killer Robots were launched in 2009 and 2013 to mobilise nation states, the public and the industry. Several faith and interfaith declarations against autonomous weapons have been adopted, including one by the Catholic Church stating that it is fundamentally immoral to use a weapon that we cannot fully control. Finally, a discussion was initiated on a possible new formal protocol to the UN Convention on Certain Conventional Weapons to improve the regulation of fully autonomous weapons, but the US, Russia and the UK objected.¹¹ Some observers labelled AI as a new weapon of mass destruction, as they saw similarities with the development phase of the atomic bomb. Some actors, such as the Austrian and Swedish governments, the Belgian Parliament and the European Parliament, also called for a ban on autonomous weapons.¹²

The above discussion on the difficult implementation of AI in the armed forces shows that the potential premature introduction of AI systems and technology in military practice is a matter of concern. Many of the risks associated with the use of this technology stem from this problem. These risks and concerns need to be taken seriously and regulated as much as possible to avoid undesirable consequences in any way. We categorised several clusters of risks from the existing literature (see Table 1).

¹⁰ Google cooperated with the Pentagon in project Maven aiming to use special computer vision technology for analysing an increasing number of drone footage and identify and track objects. Google employees protested against this in 2018 and the contract was not continued (Canca, 2023, p. 60).

¹¹ Forrest et al., 2020, pp. 24-28.

¹² Soare, 2023, pp. 100-102.

Table 1 *Categorisation of risks of AI use by armed and defence forces.*¹³

General categories of risks:	Specific categories of risks:
1. Uncontrolled and unstoppable development of general AI	Exceeding human performance
	Self-directed, self-replicating and self-improving beyond human control
	Pursuing objectives that are not consistent with human interests
2. Ethical and legal risks	Limited AI capacity to understand the law of armed conflict, humanitarian law and other legal basis
	Accountability gap between the operators and AI systems
	Limited ability to make moral judgements
	Tendency to violate human rights and privacy (threat to privacy and human rights)
3. Operational risks	The issue of overconfidence in AI systems and the problem of surprising and incomprehensible decisions
	Problematic validity of AI-based recommendations or decisions
	AI outcomes and decisions based on narrow training experience
	The risk of accidental use and conflict escalation
	Vulnerabilities of AI systems
	Lower use and violence thresholds

¹³ The base for this categorisation was the classification by Forrest et al., which was then supplemented with other debated risks and published sources. The original categorisation by Forrest et al. (2020, p. 30) includes:

- Ethical and legal risks: law of armed conflicts, accountability and moral responsibility, human dignity, and human rights and privacy;
- Operational risks: trust and reliability, hacking, data poisoning and adversarial attacks, accidents and emergent risks;
- Strategic risks: thresholds, escalation management, proliferation, and strategic stability.

4. Strategic risks	The risk of easy proliferation to other malicious states, criminal and terrorist actors
	Risky and difficult to control the dual-use potential of AI technology
	The risk of global AI arms race and competition
	AI capability-related distrust among countries
	Risk of system mispositioning of AI-based decision-making
	The risk of increased police and intelligence states

2.1 Uncontrolled and unstoppable development of general artificial intelligence

The first concern relates to the worst-case scenario in terms of the potentially uncontrolled and unstoppable development of general AI. AI can usually be divided into artificial general intelligence (AGI) or strong AI and applied AI. The ultimate goal of AGI is to build machines that think and whose general intellectual abilities are indistinguishable from those of humans. After great optimism in the 1950s and 1960s, science has realised that this involves extreme difficulties. Applied AI, on the other hand, is about advanced information processing aimed at developing commercially viable and more targeted ‘smart’ systems. The application of such ‘expert systems’ has been much more successful in practice. Such systems are based on a knowledge base and an inference engine. The latter processes information on the basis of production rules (if-then rules, etc.). Good expert systems are often better than a single human expert, and their scope of application can be very broad.¹⁴ At present, our society is at the level of a weak or narrow AI, where the systems can only perform very specific tasks.¹⁵ However, the risk associated with AGI remains, as it is uncertain at what point AGI will be able to exceed human performance for a given task. There is also a risk that AGI could become self-directed, self-replicating and self-improving and escape human control. In addition, such AI systems will become larger, better, cheaper and more ubiquitous. They will be capable of quasi-autonomy and potentially self-improvement. Each of these features

¹⁴ Artificial Intelligence, 2023.

¹⁵ Luberisse, 2023a, p.3.

will challenge traditional governance models.¹⁶ At some point, these systems will be weaponised by nations and their armed forces, and defending against them will be the task of the armed forces of the conflicting countries. Furthermore, the fictional scenario is that human-made system surpasses human intelligence and pursues goals that do not coincide with human interests, thus posing an existential threat to all humans. The worst-case scenario in this direction would be the dominance of AI systems and some kind of conflict between human society and AI systems or even a new AI civilisation or human slavery. Such scenarios have been clearly simulated by the movie industry in some widely known movies, such as *The Matrix*. This was about a human society enslaved by AI, where people were bred in fields as batteries for technical systems and platforms. *The Matrix* was actually a special AR environment where people performed specific social roles, all for the purpose of keeping their minds happy so that the batteries (their bodies) in the real physical world grew at the right pace and could be harvested for consumption. Another such scenario is the case of *Skynet*, an artificial consciousness that controls the Terminator robots in the movie *Terminator*. The AI system in one of the Terminator movies asserted: 'I am not a machine, I am not a man, I am more'.¹⁷

Juliano further developed the possible negative scenario referred to above. The defining characteristic of a strong AI is the capacity to generalise, i.e. the ability to adapt to and act in new environments without being programmed to do so. Generalising intelligence will need to develop the ability to feel and understand consciousness. Juliano believes that we will ultimately be powerless to stop the release and future misuse of strong AI, and that it is unlikely that we will change enough to deal responsibly with strong AI. In his view, it is dangerous to believe that we, as a species, will not lose control after the first strong AI is liberated and distributed.¹⁸ Accordingly, we do not have a choice because not everyone will agree to limiting research, research can be conducted secretly regardless of legality, strong AI is algorithmic by nature and does not require significant resources or infrastructure to research it, and overlapping fields of research are converging in this direction (research in linguistics, mathematics, computer science, cognitive science, neuroscience, philosophy of mind, etc.). The

¹⁶ Bremmer and Suleyman, 2023, pp. 6-7.

¹⁷ Terminator Genesis, 2015.

¹⁸ Juliano, 2016, pp. 7-13.

threat will initially be coming from those individuals or groups who are the first to use strong AI, rather than from the AI itself, but later on ordinary people, including criminals and terrorists, will also gain access to strong AI with even the most basic computers. The threat will mainly come from force multiplication effects.¹⁹

In their RAND study, Forrest et al.²⁰ called for a deeper examination of the risks associated with AI and conducted an expert opinion survey on the risks associated with military AI applications. The top 5 AI risks of military AI applications were as follows: decisions might be made too fast, they could result in increased escalation, they could be less accurate/precise than humans, it is difficult to differentiate combatants from non-combatants, and it is difficult to differentiate anomaly from threats.

2.2 Ethical and legal risks

Limited AI capacity to understand the law of armed conflict, international humanitarian law and other legal basis. The law of armed conflict and international humanitarian law are based on the four Geneva Conventions and their protocols.²¹ Accordingly, belligerents must comply with the three most important principles: distinction (between civilians and combatants, operations must be directed at military objectives and attacks against civilian targets must be omitted), proportionality (no excessive harm disproportionate to the military objective) and precaution or military necessity (use of only necessary force to achieve a legitimate military objective).

The main criticism of fully autonomous weapon systems focuses on their alleged inability to comply with the principles of distinction and proportionality. They argue that these systems are unable to understand and assess subtle differences between combatants and non-combatants, especially in urban settings where combatants do not always wear uniforms. They are also unable to comply with the principle of proportionality, as this requires a case-by-case assessment of possible collateral damage weighed against the importance of the military objective.²² If these systems are able to distinguish between military and civilian targets, the question arises as to

¹⁹ Juliano, 2016 pp. 163-209.

²⁰ Forrest et al., 2020, p. 21.

²¹ See The Geneva Conventions of 12 August 1949, 1949; Protocols Additional to the Geneva Conventions of 12 August 1949, 1977.

²² Forrest et al., 2020, pp. 30-31.

how accurate they can be, whether they can assess the proportionality of the use of force and comply with international law.²³

Despite the fact that humans proved themselves as extremely efficient in ways of slaughter, there is a growing concern (it is even a key concern) about how deadly these AI systems could be and whether they can run amok and cause humans to lose control. It is unlikely that AI systems with a very narrow view of the world would be able to navigate and fight on their own in a very challenging urban combat environment. The laws of armed conflict could be integrated into the software, but the question is whether these 'killer robots' would be able to understand and apply them. This means that there is a risk that AI systems could be used to carry out illegal and unethical actions.²⁴

Accountability gap between the operators and AI systems. The ethical risk is that the use of autonomous weapon systems will create an accountability gap or moral buffer between human operators and the actions of the systems. Accountability is an important moral concept that designates moral responsibility for actions and the associated moral emotions, such as shame or guilt. This concept is an important deterrent in war and in general. Critics claim that fully autonomous weapons will make decisions without proper accountability and that systems cannot be held morally responsible for their actions. This brings us to a specific problem of attribution, where it is not clear who is responsible for the use of the system.²⁵ The issue of accountability is one of the most important ethical considerations in relation to autonomous weapons. The question is who is accountable if an autonomous weapon malfunctions or makes a decision that causes civilian casualties, and is it ethical to hold the programmers, the military or the government accountable.²⁶

Limited ability to make moral judgements. Arguments from the perspective of human dignity claim that only humans are capable of making moral judgments about the taking of human life, and that only humans have emotions and a sense of compassion and respect for human life. Technical systems do not have sufficient moral qualities to justify their actions in a way that respects the victims and therefore should not make such

²³ Luberisse, 2023b, p. 60.

²⁴ Luberisse, 2023a, pp. 19-20.

²⁵ Forrest et al., 2020, pp. 32-33.

²⁶ Luberisse, 2023b, p. 61.

decisions.²⁷ The question is whether the use of autonomous weapons is consistent with the principles of a just war.²⁸

Tendency to violate human rights and privacy (threat to privacy and human rights). AI brings threats and risks to human rights and the privacy of individuals. AI systems require vast amounts of data, leading to concerns that this data could be used to violate individual rights. For example, the massive use of AI data in facial recognition raises concerns about possible misuse by governments and other organisations.²⁹ Autocratic surveillance of one's own population can be made possible by systems such as extensive data analysis, persistent ISR, facial recognition, the Internet of Things, etc.³⁰ Information operations that spread false information and create social and cognitive bias lead to the diminished importance of objective facts (e.g. Truth Decay). Military systems can produce outputs that discriminate against minorities or other groups due to unrepresentative and biased training data.³¹ For example, algorithms trained on biased data can perpetuate discrimination against marginalised groups, leading to further marginalisation and human rights violations. This way, AI can perpetuate and exacerbate prejudices and inequalities.³² This susceptibility to bias in the data actually means that even machine learning cannot guarantee the absence of bias or analytical error.³³

The use of AI, especially in lethal autonomous weapons and decision support tools in active combat, may lead to ignoring the complexity of the given situation and the value of human life. The greatest risk is the potential incorporation of an ethical error in AI system because its widespread use can lead to mass damage to individuals and communities, behind the veil of computational objectivity.³⁴

²⁷ Forrest et al., 2020, p. 34.

²⁸ Luberisse, 2023b, p. 61.

²⁹ Luberisse, 2023a, pp. 38-40.

³⁰ Frequently, the use of AI by China indicates excessive monitoring of own citizens and suppressing dissent. However, such approaches were also used in more Western societies against own population as indicated for example by the Snowden case.

³¹ Forrest et al., 2020, p. 35.

³² Luberisse, 2023a, pp. 38-40.

³³ Mashur, 2019, p. 2; see also Rickli and Mantellassi, 2023, p.18.

³⁴ Canca, 2023, p. 59.

2.3 Operational risks

The issue of overconfidence in AI systems and the problem of surprising and incomprehensible decisions. The black box problem of AI refers to the inability to explain the reasoning that led to a particular outcome. Such situations would lead to an increasing ‘unawareness’ of what is happening on the battlefield³⁵ and to the problem of trust and reliability (mainly expressed in the issue of not trusting or overtrusting AI systems). The black box problem refers to the situation in which an AI system might produce outputs in ways not comprehensible or explainable to humans. Different performances of the AI system outside the laboratory can also lead to an additional lack of trust. On the other hand, operators or commanders might have excessive trust in AI systems because they are overconfident, do not look for contradictory information, etc. Such tendencies were observed in Operation Iraqi Freedom, where some operators trusted the systems without questioning.³⁶ The victory of the AI programme AlphaGo over the human world champion and grandmaster in 2016 was achieved through occasionally surprisingly bold moves that ultimately led to a shocking defeat of the human opponent.³⁷ If AI systems function in unpredictable ways that can have serious negative consequences, responsible leaders will not adopt them, and operators will not have confidence in their use and will not deploy them. There is also a risk that autonomous AI systems would be used for human rights violations and war crimes.³⁸

Problematic validity of AI-based recommendations or decisions. Occasionally, it will be impossible to verify the validity of AI-based recommendations. It is difficult to judge from an external point of view how accurate or trustworthy an AI-generated assessment really is. More complex AI may be able to predict or at least pre-define scenarios without necessarily understanding the underlying logic, reasoning and prioritisation. This means that it is very important how AI is embedded in a political and institutional context to minimise serious risks.³⁹

AI outcomes and decisions based on narrow training experience. AI systems must first be trained in an artificial environment with different data sets. The system processes the data, performs the tasks and hopefully learns.

³⁵ Rickli and Mantellassi, 2023, p.63.

³⁶ Forrest et al., 2020, p. 36.

³⁷ Gatopoulos, 2021, p. 5.

³⁸ Luberisse, 2023b, p. 61.

³⁹ Mashur, 2019, p. 2.

The catch is a lengthy accumulation of experience based on a large number of interactions and repetitions with different data sets. Training with one data set leads to certain results, while training with another data set leads to different results. Mashur emphasised that AI systems trained in different ways might come to conflicting conclusions. This means that AI systems are not able to achieve results based on perfect rationality.⁴⁰

The risk of accidental use and conflict escalation. The risk of accidental deployment and use with unintended consequences is real. AI-enabled autonomous weapons, if deployed globally in an uncontrolled manner, could increase the risk of unintended conflict escalation and crisis instability.⁴¹ The programmers of AI are not so much worried about the Terminator scenario, but rather about flash wars (wars that are triggered without control, similar to the collapse of the stock market, where many algorithms are trading and suddenly, due to an unforeseen event, the algorithms crash the stock market).⁴² These concerns are particularly present in the area of autonomous nuclear defence systems. The risks of accidental use in this area or potential use by malicious actors (who would hack into the system or feed false data) can be globally deadly. The speed of AI-powered decision making could even lead to an escalation of conflict, resulting in a rapid and unintended escalation in the use of nuclear weapons. AI can accelerate the decision-making process in crises to a machine AI level.⁴³ Future Cuban missile type crises might emerge, but the problem is that this acceleration could contribute to escalating the crisis rather than de-escalating it, as the actors would see their window of opportunity shrinking.⁴⁴ The existence of the Russian Perimeter nuclear defence system has also raised concerns about the ethical implications of granting decision making capabilities to machines and the risk of accidental use.⁴⁵

⁴⁰ Mashur, 2019, p. 2.

⁴¹ Final Report, 2021, p. 10.

⁴² Flash Wars: Autonomous Weapons, AI and the Future of Armed Conflict, 2023.

⁴³ Director of the US AI Center stated that that we are going to be shocked by the speed, chaos and bloodiness in the future wars, it is going to be algorithm against algorithm (Rickli and Mantellassi, 2023, p. 20).

⁴⁴ Mashur, 2019, p. 2.

⁴⁵ An AI-enabled example is the Russian nuclear automated defence system Perimeter, which can detect a nuclear strike against Russia and launch a retaliatory nuclear strike even if the lines of communication with Strategic Missile Forces are destroyed. The system adopts a decision to launch a retaliatory strike after approval by the human commander, but in case of a missing communication with the command centre it can launch such a strike alone. Additionally, it can launch a command rocket in the air over Russia and retaliatory

Due to the associated combination of massive damage and lack of controllability, there have been calls to consider an international ban on lethal autonomous weapon systems and to classify intelligent AI-supported drone swarms as weapons of mass destruction.⁴⁶

Vulnerabilities of AI systems. AI systems are also vulnerable to hacking, data poisoning and adversarial attacks. AI systems can be hacked and their training data manipulated or spoofed in order to influence the intended functioning of the system. Attacks by adversaries might also trick algorithms into making a mistake. AI software can also escape seemingly unintentionally, such as the Stuxnet worm and other cases of self-replicating malware (WannaCry, NotPetya). Finally, AI systems could become so advanced that they could undermine the 'second strike' capabilities that are essential for responding after an initial nuclear attack. AI could be used to locate enemy nuclear launchers, disable them during the attack and prevent a retaliatory strike.⁴⁷

Since AI-powered organisations will store large amounts of sensitive data, the risk of data breaches and information theft in AI-powered organisations is real.⁴⁸ The adversarial AI will aim also to deceive the AI with deceptive data.⁴⁹ The possibility that one's entire army of AI systems can suddenly turn against their owners is also terrifying for military planners.⁵⁰ In addition, even high-performance algorithms are not immune to being misled by more traditional means of espionage and deception. AI might mistakenly assess certain patterns of behaviour as harmless if they occur often enough without any feared consequences.⁵¹

2.4 Strategic risks

Lower use and violence thresholds. It is likely that the use of AI will shift the balance between offence and defence towards offence: AI will largely be

strike activation from all available platforms (silos, aircraft, submarines and mobile ground units) is done from there in case of missing link with strategic missile control centre. Perimeter checks this link all the time, but it can act autonomously in case of need. Another example is the Russian fully automated nuclear submarine Poseidon, which can also autonomously generate a nuclear attack. (Luberisse, 2023a, pp.21-23).

⁴⁶ Hambling cited in Nurkin, 2023, p. 52.

⁴⁷ Forrest et al., 2020, pp. 37-38.

⁴⁸ Luberisse, 2023a, p.18.

⁴⁹ Rickli and Mantellassi, 2023, p. 16.

⁵⁰ Gatopoulos, 2021, p. 10.

⁵¹ Mashur, 2019, p. 2.

used offensively.⁵² There is also a risk that the threshold for the use of autonomous armed systems is lower than the threshold for the use of conventional weapons. This faster use could also cause more civilian casualties during operations.⁵³ Schmidt et al. even fear that all AI tools will be among the weapons of first choice in future conflicts.⁵⁴

The risk of easy proliferation to other malicious states, criminal and terrorist individual or collective actors. AI systems are not only much easier to develop, steal and copy than nuclear weapons, they are also controlled by private companies and not by governments.⁵⁵ Egel emphasised that AI-enabled weapons are relatively easy and inexpensive to procure and will therefore be accessible to non-state actors and proxies. Some states could even deliberately provide such actors with these capabilities, as has happened in the past.⁵⁶ Thiele concluded that AI technologies will sooner or later be available to any opponent.⁵⁷

Risky and difficult to control dual-use potential of AI technology. As a rule, non-combat AI systems (used in the areas of predictive maintenance, logistics, personnel management, communication, etc.) are not ethically problematic. However, the literature warns that existing AI systems can be reprogrammed for use on the battlefield.⁵⁸ This leads us to the typical area of dual-use technology. For example, an AI algorithm for driving cars can easily be adapted to an algorithm for driving tanks and so on. This means that the boundaries between the safely civilian domain and the destructive military domain are inherently blurred.⁵⁹

The risk of global AI arms race and competition. The AI empowerment is a very attractive option in the global power struggle. Authors who have studied the geopolitical aspects of the use of AI emphasise that the race to adopt AI is leading to a power struggle between great powers with implications for the global balance of power.⁶⁰ Bremmer and Suleyman also emphasised that AI supremacy, or competition for AI supremacy, will be a strategic objective of every government that has the

⁵² Rickli and Mantellassi, 2023, p. 25.

⁵³ Forrest et al., 2020, p. 39.

⁵⁴ Schmidt et al, 2021, cited in Thiele, 2021b, p. 76.

⁵⁵ Bremmer and Suleyman, 2023, p. 10.

⁵⁶ Egel et al., 2019, cited in Thiele, 2021a, p. 77.

⁵⁷ Thiele, 2021b, p. 190.

⁵⁸ Canca, 2023, p. 60.

⁵⁹ Bremmer and Suleyman, 2023, p. 6.

⁶⁰ Luberisse, 2023a, p. 18.

resources. Two major players, the US and China, view AI development as a zero-sum game that will give the winner a decisive strategic edge in the future.⁶¹ Nations and organisations that are best to anticipate and exploit technological opportunities are likely to have a decisive advantage in future competitions, crises and conflicts. AI will also be the linchpin in achieving military superiority through the use of data, i.e. turning it into relevant information, usable knowledge and ultimately into decision-making advantages.⁶²

AI capability-related distrust among countries. The lesson from the classic confidence- and security-building measures is that distrust leads to conflicts and that distrust can be based on a lack of information about the capabilities of the opponent.⁶³ We argue that AI development and use in modern armed forces will lead to the typical distrust among states that has already been observed in the past in delicate geostrategic situations with a lack of information about the capabilities of the opponent. Horowitz also emphasised that the state's armament in the AI-related capabilities can hardly be measured precisely by other states. It will be difficult to assess the degree of automation, the quality of the code, the efficiency of autonomous weapons and their capabilities. This uncertainty will lead states to overestimate the capabilities of other states.⁶⁴

The risk of system mispositioning of AI-based decision-making. A very important question for society is who exactly has access to AI and who is in the position to contextualise and interpret the results. In democracies, the armed forces' sole access to analytical AI that recommends certain military options for action may be problematic. Especially at the highest strategic levels, where other defence and political actors should also be involved. It is important how and where AI is embedded in the existing institutional decision-making process,⁶⁵ otherwise AI could be used strategically based on a narrow military perception of the situation.

The risk of increased police and intelligence state through the use of AI. AI surveillance systems can be used for systematic, excessive surveillance of one's own or other people's populations. The exposure of widespread illegal HUMINT or TECHINT collection operations typically

⁶¹ Bremmer and Suleyman, 2023, pp. 7-8.

⁶² Thiele, 2021a, p. 59, 77.

⁶³ See Prezelj and Harangozo, 2018.

⁶⁴ Horowitz, 2018, cited in Rickli and Mantellassi, 2023, p. 25.

⁶⁵ Mashur, 2019, p. 2.

led to the so-called intelligence collection scandals.⁶⁶ The application of AI in this area will improve operational capabilities and give legal or rogue actors more opportunities to infringe the human rights of a large part of the population. The classic concept of a police or intelligence state can transform itself into an AI police and intelligence state. This risk is also recognised in the policy world, but much more in case of foreign states than for the domestic state. For example, according to US sources,⁶⁷ the U.S. is very concerned about China's use of AI as a tool of repression and surveillance both internally and gradually internationally. Accordingly, AI should reinforce democracy rather than erode it. AI future should be democratic, AI must be developed based on its values and work with democracies and the private sector is essential in building privacy-protecting standards into AI technologies and advancing democratic norms to guide AI use so that democracies can use AI for national security purposes.⁶⁸ Luberisse stressed that China has been investing heavily in AI, with a particular focus on surveillance systems to enhance its ability to monitor and control its population. The nationwide deployment of AI-powered cameras and facial recognition systems has raised significant privacy and human rights concerns and fuelled debates about the appropriate use of AI.⁶⁹ However, we should also be wary of similar intentions in democratic states. Several public intelligence scandals teach us to think along these lines too.

3. Conclusion

The application of AI in the armed forces brings with it a range of new opportunities as well as many new risks and challenges. In this paper, we have identified and analysed a wide range of risks associated with an uncontrolled and unstoppable development of general AI, along with several ethical and legal, operational and strategic risks. We have shown how and why these risks are dangerous and some even pose a threat to human security, values, norms, democracy, human rights, etc. These risks need to be carefully examined in order to improve the military use of AI and regulation in this area.

⁶⁶ Prezelj and Ristevska, 2023.

⁶⁷ Final Report, 2021, pp. 2-6.

⁶⁸ Final Report, 2021, pp. 2-6.

⁶⁹ Luberisse, 2023a, pp. 10-11.

The introduction of AI in modern armed forces will be complicated and slower than expected, but still faster than the introduction of previous new technologies. The armed forces will have to carefully weigh reliability and controllability, on the one hand, against the related risks on the other. They will have to deal with several technological and organisational barriers to reach an effective AI, as AI will be implemented asymmetrically in different weapon systems, and human absorption barriers have not yet been sufficiently addressed. The latter will be an important factor in the adoption of this technology, as there are already scientifically verified patterns of potential negative feelings, anxiety and distrust towards the new technology. The armed forces will also have to deal with the problem of the deficit of personnel specialising in AI who are willing to work for them. The introduction of AI in the armed forces will also require some legal, ethical, organisational, doctrinal, strategic and policy changes in the military and defence systems and beyond.

Several categories of actors from the international community have warned about the risks of development and use of AI. Particular attention has been paid to general AI and military autonomous weapons systems. The warnings have come from groups of scientists, technologists, technology company employees, activists and even the Catholic Church. Some have even labelled AI as a future weapon of mass destruction, as there are some similarities in the early stages of development of both technologies (nuclear and AI).

The most serious, but still very hypothetical and potentially existential risk comes from the unstoppable and uncontrolled development of general AI in a direction that is not consistent with the general human interest. We do not know when this may happen. Some authors are of the opinion that it will be inevitable, and when it happens, it will be too late. Existing movies offer several imaginary scenarios for such a possible future. The ethical and legal risk category includes the risk of the limited understanding of the law by the AI systems and the related concepts of proportionality, distinction and military necessity, the risk that the autonomous systems will not be able to take accountability for military actions, the limited ability to make moral judgments, and the tendency to violate human rights and privacy. The category of operational risks includes the risk of excessive trust in AI systems and the problem of occasionally surprising and incomprehensible AI decisions, the problematic validity of AI-based recommendations and decisions, the relatively limited training experience that determines the

results of AI systems, the risk of accidental use and conflict escalation and, finally, the vulnerability of the AI systems themselves. The category of strategic risks includes the risk of lower use and violence thresholds, the ease of dissemination to other malicious states and criminal and terrorist actors, the risk of the dual-use of AI, the risk of a global AI arms race and competition, the risk of distrust among states regarding actual AI capabilities, the risk of incorrect positioning of AI-based decision making in the system, and the risk of creating a police and intelligence state.

These risks need to be carefully examined and incorporated into future regulatory systems at national, regional and global level. The range of risks mentioned above is so wide that regulation will be very difficult. It is likely that some risks will be taken into consideration and clearly regulated before there is any malicious military use of AI. However, there will certainly be some uses of AI for military purposes where regulation will only follow after the malicious use of the technology. Unfortunately, this will not happen for the first time in human history.

Finally, the question arises as to what more concrete countermeasure strategies and practical guidelines should be applied to manage the risks associated with the use of artificial intelligence in the armed forces. We recommend the following countermeasures to address the identified risks:

1. Control the development of general AI by monitoring at what point it will be able to outperform humans, when it will become self-directed, self-replicating and self-improving, and when it will escape human control in the wrong direction by pursuing goals against humankind. Furthermore, the research process, even open coded, must somehow be limited.
2. The ability of AI to 'understand' the law of armed conflict, international humanitarian law and other legal frameworks must be constantly improved.
3. The accountability of operators and AI systems must be regulated. It should be made clear that the actions of AI systems are legally attributable to their operators and creators.
4. Due to the limited ability of AI systems to make moral judgments, moral responsibility should be assigned to their human AI operators.
5. Understand that autonomous AI systems deployed in all security domains are prone to violate human rights and privacy and prepare appropriate barriers to do so.

6. Educate AI operators about the problem of overconfidence and the 'black box' in order to maintain a certain critical distance from AI systems.
7. Stop the operation of AI systems in cases where they make completely surprising and incomprehensible decisions and try to understand them.
8. Try to verify the validity of AI-based recommendations or decisions.
9. Since AI results and decisions are based on narrow training experiences, AI should not be used in situations for which it has not been prepared.
10. Be aware that one of the main risks is the danger of accidental use and conflict escalation; try to simulate and predict such situations and use blockers for such a development.
11. Recognise vulnerabilities of AI systems and try to mitigate them.
12. Try to monitor violence thresholds when using AI systems.
13. Seek to create a non-proliferation regime for AI weapons that includes state and non-state actors.
14. Understand AI as a dual-use technology and seek to regulate it like other such technologies.
15. Create a confidence- and security-building regime that controls existing AI weapons capabilities in all states based on self-reporting, monitoring and verification.
16. Learn at which level which AI-based decisions should be made.
17. Mitigate the risks of a growing police and intelligence state through the use of AI by controlling AI operators, masters and related structures by means of democratic oversight.

Bibliography

- [1] Bremmer, I., Suleyman, M. (2023) 'The AI Power Paradox: Can States learn to Govern Artificial Intelligence – Before It's Too Late?', *Foreign Affairs*, 2023/September/October.
- [2] Canca, C. (2023) 'AI Ethics and Governance in Defence Innovation: Implementing AI Ethics Framework' in Raska, M., Bitzinger, R. A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*. New York: Routledge, pp. 1–11; <https://doi.org/10.4324/9781003218326-4>.
- [3] Forrest, E. M., Boudreaux, B., Lohn, A.J., Ashby, M., Curriden, C., Klima, K., Grossman, D. (2020) *Military Application of Artificial Intelligence: Ethical Concerns in an Uncertain World*. Santa Monica: RAND Research Report.
- [4] Gatopoulos, A. (2021) 'Project Force: AI and the Military – a Friend or Foe?', *Aljazeera* [Online]. Available at: <https://www.aljazeera.com/features/2021/3/28/friend-or-foe-artificial-intelligence-and-the-military> (Accessed: 09 August 2024).
- [5] Horowitz, M. C. (2018) 'The Promise and Peril of Military Applications of Artificial Intelligence', *Bulletin of the Atomic Scientists* [Online]. Available at: <https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/> (Accessed: 06 August 2024).
- [6] Juliano, D. (2016) *AI Security*. Fort Myers: Undine.
- [7] Kruger, A. (2024) 'Alternative ni, prilagoditi se bomo morali svetu z AI', Interview, Executive Director of DFKI, *Delo*, 22 February, p. 13.
- [8] Levy, A., Uri, M. (1986) *Organisational Transformation: Approaches, Strategies, Theories*. New York: Praeger. <https://doi.org/10.5040/9798400693960>.

-
- [9] Luberisse, J. (2023a) *The Geopolitics of Artificial Intelligence: Strategic Implications of AI for Global Security*. Wroclaw: Fortis Novum Mundum.
- [10] Luberise, J. (2023b) *Algorithmic Warfare: The Rise of Autonomous Weapons*. Wroclaw: Fortis Novum Mundum.
- [11] Mantello, P., Manh-Tung H., Minh-Hoang N., Quan-Hoang V. (2023) Bosses without a heart: Socio-demographic and cross-cultural determinants of attitude toward Emotional AI in the workplace. *AI & Society*, 38, pp. 97–119; <https://doi.org/10.1007/s00146-021-01290-1>.
- [12] Mashur, N. (2019) ‘AI in Military Enabling Applications’, *CSS Analyses in Security policy*, 2019/251, pp. 1–4. [Online]. Available at: <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/367663/CSSAnalyse251-EN.pdf?sequence=2> (Accessed: 09 August 2024).
- [13] Nurkin, T. (2023) ‘AI and Technological Convergence: Catalysts for Abounding National Security Risks in the Post-COVID World’, in Bitzinger, A. R., Raska, M. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*. New York: Routledge, pp. 37-58; <https://doi.org/10.4324/9781003218326-3>.
- [14] Park, J., Sang Eun W. (2022) ‘Who Likes Artificial Intelligence? Personality Predictors of Attitudes toward Artificial Intelligence’. *The Journal of Psychology* 156, pp. 68–94; <https://doi.org/10.1080/00223980.2021.2012109>.
- [15] Prezelj, I., Harangozo, D. (2018) *Confidence and Security-Building Measures in Europe at a Crossroads*. Baden-Baden: NOMOS. <https://doi.org/10.5771/9783845288970>.
- [16] Prezelj, I., Ristevska, T. T. (2022) ‘Intelligence Scandals: A Comparative Analytical Model and Lessons Learned from the Test Case of North Macedonia’, *Intelligence and National Security*, 38(1), pp. 143-170; <https://doi.org/10.1080/02684527.2022.2065616>.

- [17] Raska, M., Bitzinger, R. A. (2023) 'Introduction: The AI Wave in Defence Innovation', in Raska, M., Bitzinger, R. A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*. New York: Routledge, pp. 1–11; <https://doi.org/10.4324/9781003218326-1>.
- [18] Rickli, J.-M., Mantellassi, F. (2023) 'Artificial Intelligence in Warfare', in Raska, M., Bitzinger, R. A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*. New York: Routledge, pp. 12–36; <https://doi.org/10.4324/9781003218326-2>.
- [19] Schepman, A., Rodway, P. (2023) 'The General Attitudes towards Artificial Intelligence Scale (GAAIS): Confirmatory Validation and Associations with Personality, Corporate Distrust, and General Trust'. *International Journal of Human–Computer Interaction* 39, pp. 2724–2741; <https://doi.org/10.1080/10447318.2022.2085400>.
- [20] Schuller, M. (2023) Human and Machine Learning, Paper presented at a conference NATO in the Nordics, August 30–31st 2023, Stockholm.
- [21] Soare, S. (2023) 'European Military AI: Why Regional Approaches are Lagging Behind', in Raska, M., Bitzinger, R. A. (eds.) *The AI Wave in Defence Innovation: Assessing Military Artificial Intelligence Strategies, Capabilities and Trajectories*. New York: Routledge. <https://doi.org/10.4324/9781003218326-5>.
- [22] Thiele, R. (2021a) 'Nineteen Technologies in Focus', in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 71–124; https://doi.org/10.1007/978-3-658-35109-0_5.
- [23] Thiele, R. (2021b) 'Annex 2 – Artificial Intelligence', in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 187–196; <https://doi.org/10.1007/978-3-658-35109-0>.

-
- [24] Thiele, R. (2021c) ‘Technology as a Driver’, in Thiele, R. (ed.) *Hybrid Warfare: Future and Technologies*. Wiesbaden: Springer VS, pp. 59-70; https://doi.org/10.1007/978-3-658-35109-0_4.
- [25] Artificial Intelligence (2023) Encyclopaedia Britannica [Online]. Available at: <https://www.britannica.com/technology/artificial-intelligence> (Accessed: 09 August 2024).
- [26] Artificial Intelligence Act, Briefing, EU Legislation in Progress, European Parliamentary Research Service, June, 2023.
- [27] Artificial Intelligence Act: Council and Parliament Strike a Deal on the First Rules for AI in the World, Council of the EU, Press Release 986/23, 9.12, 2023.
- [28] Flash Wars: Autonomous Weapons, AI and the Future of Armed Conflict, documentary movie, Director Daniel Andrew Wunderer, Blue + Green Communications, 2023.
- [29] Geneva Conventions of 12 August 1949 (1949) ICRC [Online]. Available at: <https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0173.pdf#:~:text=the%20ICRC%20is%20at%20the%20origin%20of%20the%20Geneva%20Conventions> (Accessed: 07 August 2024).
- [30] Protocols Additional to the Geneva Conventions of 12 August 1949 (1977) [Online]. Available at: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc_002_0321.pdf#:~:text=Geneva%20Conventions%20of%2012%20August%201949,%20and%20relating%20to%20the (Accessed: 09 August 2024).
- [31] Final Report (2021) Washington, D.C.: National Security Commission on Artificial Intelligence. [Online]. Available at: <https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf> (Accessed: 09 August 2024).

- [32] Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development, UN General Assembly Resolution, A/78/L.49, 11 March 2024.
- [33] Summary of the NATO Artificial Intelligence Strategy (2021) Meeting of Defence Ministers, 22 October, Brussels.
- [34] Terminator Genesis, Director: Alan Taylor, IMDbPro, 2015.

MIHA ŠEPEC* - MAŠA KOČIVNIK**

Combatting Cyberwarfare Crimes in the European Union***

ABSTRACT: Cyberwarfare crimes constitute a major threat to the security of the European countries. The effects of such attacks could be devastating for the European economy, stability and national security. The question therefore remains, whether the European Union (EU) has effective security measures and strategies against cyberwarfare attacks, and whether it has appropriate legal definitions of such phenomena. Furthermore, does the EU have cooperation measures and institutions for combatting such crimes? In this article we will first present the practical and legal definition of cyberwarfare and its impact on the security of the EU Member States. Then we will analyse the main security measures and strategies of the EU for preventing cyberwarfare attacks, the primary among which are the EU Cybersecurity Act, Directive on the security of network and information systems (NIS) and its second revised version (NIS 2 Directive), and the European Network and Information Security Agency (ENISA). We will continue with substantive legal documents, where the main role is still played by the Directive EU 2013/40/EU on attacks against information systems, which is now almost 11 years old and dated in some aspects. On the procedural level we will analyse the EU cooperation in combatting cyberwarfare attacks through two perspectives (cooperation measures and EU institutions). In the first perspective, we will exam the European Arrest Warrant, the European Evidence Warrant, the European Freezing and Confiscation Order, the European Investigation Order, the European Judicial

* Associate Professor, Head of Department of Criminal Law, Faculty of Law, University of Maribor, Slovenia. miha.sepec@um.si.

** Master of Law Student, Faculty of Law, University of Maribor, Slovenia. masa.kocivnik@student.um.si.

*** The research and preparation of this study was supported by the Central European Academy.

Network (EJN), and the Schengen Information System (SIS). And in the second, we will present Europol and its European Cyber Crime Centre, Eurojust, and the European Network and Information Security Agency (ENISA). Although the EU has mechanisms in place to combat and prevent cyberwarfare crimes, the legal situation is still far from ideal. The main problem remains the lack of clear legal definition of cyberwarfare crimes and no focused legislation in regard to criminal prosecution of such crimes.

KEYWORDS: Cyberwarfare, Cyberattack, Defence Policy, Cooperation in criminal matters, Criminal Law, European Union.

1. Introduction

It is hard to imagine today's world without digital technology, which has revolutionised our lives. Electric cars, mobile phones and computers are all part of our way of living and reflect our overall dependence on digital technology. Although new technology has improved our lives to a considerable extent, it also has its drawback. One is the appearance of new forms of crimes connected with information systems and digital technology that is called cybercrime. With the introduction of the Council of Europe's Convention on Cybercrime in 2001,¹ the term cybercrime was established internationally for all forms of criminal acts committed in the cyberspace and is used today in established literature.²

The other, even newer phenomenon, which has the potential to be even more dangerous, is the rise of cyberwarfare. As long as human race existed, we have known war. War is a part of human history, and historically it was often the first or even the only way to resolve intercultural, interracial or interstate conflicts. The military industry has always developed new methods of warfare using the latest technology and means. Digital-information technologies are no exception, on the contrary, their accelerated development is often a reflection of the development of the war industry. This has led to countries attacking or sabotaging each other not with direct military operations, but with cyberwarfare attacks, that mimic military operations, but are performed in a digital world with computer technology, however often produce effects comparable to those of traditional armed attacks.

¹ Council of Europe, 2001, CETS No. 185.

² Clough, 2010, p. 9.

Digital warfare can be carried out between states, paramilitary units, or when states only participate indirectly (by providing financial or legal/moral support to perpetrators who attack the basic infrastructure of a rival state).³ States can also finance cyberterrorism of extremist groups. Cyberterrorism involves the use of information networks to damage or destroy critical state infrastructures (such as energy structures, transportation systems, state leadership establishments).⁴ All this is implemented for political, religious or ideological reasons and with the aim of instilling fear in the public and influencing the actions of the state authorities.⁵ Although, cybercrime and cyberterrorism are not synonymous, the terms are possibly connected when cyberterrorism is being coordinated or financed by the state directly or indirectly through intermediate companies or groups.

Cyberwarfare has no single definition. At its core, it means the misuse of computer technologies (such as hacking, using computer viruses, and other forms of malware) to disrupt, damage or destroy an adversary's information systems and networks. These are actions in cyberspace that threaten key state infrastructure systems in the form of armed conflicts with destructive effects. It often involves the exploitation of vulnerabilities in computer systems and networks⁶ to achieve strategic objectives, such as espionage, sabotage, or coercion.⁷ Cyberwarfare can target a wide range of assets, including military, governmental, critical infrastructure, and commercial systems, and it can have significant consequences for national security, economic stability, and public safety.⁸

For the purpose of this article the term cyberwarfare will be used to describe cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack.⁹ An armed attack intentionally causes destructive effects (i.e. death and/or physical injury to living beings and/or destruction of property). Only governments, organs of the state, or state-directed or state-sponsored individuals or groups can engage in

³ See also Bussolati, 2015, pp. 102-126.

⁴ See also Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, *OJ L 88*, 31.3.2017.

⁵ Clough, 2010, p. 12.

⁶ Snider, Shandler, Zandani and Canetti, 2021, pp. 1-11.

⁷ See also Bernik, 2014.

⁸ Digmelashvili, 2023, pp. 12-19.

⁹ Maras, 2016, pp. 10-20.

cyberwarfare.¹⁰

Types of cyberwarfare attacks also vary in different definitions. For the purpose of this article we will categorise the following cyberwarfare attacks: espionage (monitoring other countries to steal secrets), sabotage (harming state organisations or institutions), denial-of-service (DoS) attacks to disrupt critical operations and systems, attacks that disable critical systems and infrastructure, economic disruption by targeting economic establishments, surprise attacks in the context of hybrid warfare.¹¹

Today, cyberwarfare is present in practically every military operation, where classic military operations overlap with digital technology. Enemy infrastructure can be destroyed with conventional weapons, but it can also be crippled or even destroyed by a cyberattack. Considering that technology is constantly developing and that an ever-increasing part of the world depends on modern technologies, the potential for cyberwarfare is extreme. In the future, the countries of the European Union will have to invest in information technology, in addition to standard military equipment, and traditional soldiers will begin to be supplemented by information-aware soldiers. The changing global environment necessitates a corresponding evolution in warfare. The law will have to follow these changes and legally define these new forms of warfare.

The purpose of this article is to evaluate the European Union's capacity to combat against cyberwarfare attacks. We will assess whether the EU has the necessary substantial legislation to define cyberwarfare attacks. Furthermore, does the EU have legal measures of cooperation when an attack on one of its members is performed? And finally, which EU institutions are instrumental in combatting cyberwarfare crimes?

2. EU security measures and strategies against cyberwarfare

The European Union is tackling the problem of cyberwarfare in two ways. The first one involves adopting security strategies and protection mechanisms, while the second entails the legal approach (which will be presented in the next chapter). In December 2020, the European Commission and the European External Action Service (EEAS) presented a

¹⁰ Ibid., pp. 10-20.

¹¹ Cyber Warfare, Imperva [Online]. Available at: <https://www.imperva.com/learn/application-security/cyber-warfare/> (Accessed: 25 August 2023).

new EU cybersecurity strategy. The aim of this strategy is to strengthen Europe's resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The new strategy contains proposals for deploying regulatory, investment and policy instruments.¹² In June 2019 the EU Cybersecurity Act was adopted. The goal of the Act was to give ENISA (European Network and Information Security Agency) a permanent mandate, and to establish a European cyber security certification framework for information and communications technology products, services and processes. Thereby to create a new and stronger mandate for the EU agency for cybersecurity.¹³

Even before the new EU cybersecurity strategy and ENISA, in 2016 there was the Directive on the security of network and information systems (NIS),¹⁴ as the first ever EU-wide legislative measure with the purpose of increasing cooperation between Member States on the vital issue of cybersecurity. It laid down security obligations for operators of essential services and for digital service providers. In 2022 the EU adopted a revised NIS Directive (NIS2) to replace the 2016 Directive.¹⁵

NIS 2 Directive¹⁶ is aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society.¹⁷ The EU emphasises that during the war in Ukraine, cyberattacks go hand in hand with conventional military tactics, with the main purpose of destroying and disrupting the functioning of government agencies and organisations that manage critical infrastructure, as well as undermining confidence in the

¹² Cybersecurity: how the EU tackles cyber threats [Online]. Available at: <https://www.consilium.europa.eu/en/policies/cybersecurity/> (Accessed: 10 February 2024).

¹³ Available at: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act> (Accessed: 10 February 2024).

¹⁴ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *OJ L 194*, 19.7.2016.

¹⁵ Cybersecurity: how the EU tackles cyber threats [Online]. Available at: <https://www.consilium.europa.eu/en/policies/cybersecurity/> (Accessed: 10 February 2024).

¹⁶ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, *OJ L 333*, 27. 12. 2022.

¹⁷ Preamble to the Directive, 2022, p. 1.

country's leadership. Basic services, i.e. transport, healthcare and finance, are increasingly dependent on digital technologies and therefore extremely susceptible to cyberattacks.¹⁸ This is the main reason the new Directive was adopted on the EU level – in order to ensure the greatest possible information and cyber security in the EU.

According to NIS 2 Directive Member States must adopt national cybersecurity strategies and designate or establish competent cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs). The whole III chapter of the NIS 2 Directive is dedicated to the cooperation at Union and international level. The Directive establishes the Cooperation Group composed of representatives of Member States, the Commission and ENISA (Article 14). Furthermore, it establishes a network of national CSIRTs to promote swift and effective operational cooperation among Member States (Article 15), and European cyber crisis liaison organisation network (EU-CyCLONe) to support the coordinated management of large-scale cybersecurity incidents at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies (Article 16). Chapter IV of the Directive deals with cybersecurity risk-management measures and reporting obligations, while Chapter II deals with coordinated cybersecurity frameworks, which include national cybersecurity strategy (Article 7), competent authorities and single points of contact (Article 8), national cyber crisis management frameworks (Article 9), and computer security incident response teams (CSIRTs) (Article 10).

Although the new NIS 2 Directive does not include new definitions of criminal offences and therefore does not directly address definitions of cyberwarfare crimes, the whole goal of the Directive is to prepare strategy of defence against such attacks on information systems of the EU Member States. The new Directive brings stricter requirements and obligations for Member States regarding cyber security, especially in terms of supervision. The Directive improves the enforcement of these obligations, which will also be facilitated by the harmonisation of sanctions across all Member States, since the purpose of the Directive is precisely to improve

¹⁸ Cybersecurity: why reducing the cost of cyberattacks matters, European Parliament [Online]. Available at: <https://www.europarl.europa.eu/news/en/headlines/society/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters>. (Accessed: 10 October 2023).

cooperation between Member States, especially in the event of major incidents. The Directive does not define criminal acts under which individual forms of behaviour in the context of cybercrime could be placed, nor does it specifically refer to cyberwarfare, but applies generally to all cyberattacks and cybercrimes.

3. Cyberwarfare crimes in the EU law

The second approach of the European Union to combat cyberwarfare is the legal approach, namely through criminal law, as an attack on a state's information systems with profound consequences will always constitute a criminal offence. In this article we will not be dealing with military scenarios and jurisdiction of the Common Security and Defence Policy - European Defence Union, although an in-depth analysis will be required to ascertain the future role of the European Defence Union in the event of a cyberwarfare attack against an EU Member State.

As the European Union took over the legislative initiative in Europe, the most substantial shift was made by the Treaty of Lisbon (i.e. the Treaty on European Union and the Treaty on the Functioning of the European Union) from 2009, which gave the European Union a legal basis for the adoption of criminal law directives in order to ensure the effective implementation of the European Union policies. Before the adoption of the Treaty of Lisbon, the European Union also intervened in the field of criminal law, mainly through framework decisions and conventions.¹⁹ Interventions were mainly focused on the area of financial interests of the Union, but they also spread to other criminal areas (e.g. child pornography²⁰). According to the Treaty of Lisbon, in the field of criminal law, instead of framework decisions and conventions, the European Union can adopt normal community instruments (regulations, directives and decisions) with direct effect on the territory of the Member States.

However, this does not imply that the EU acts in a similar way as a sovereign state by formulating criminal legislation and carrying out criminal

¹⁹ The 1995 Convention on the Protection of the EU's Financial Interests and its Protocols, Council Regulation (EC, Euratom) no. 2988/95 of 18 December 1995 on the protection of the financial interests of the European Communities in relation to administrative sanctions, *OJ L 312*, 23.12.1995.

²⁰ Council Framework Decision 2004/68/PNZ of 22 December 2003 on combatting the sexual exploitation of children and child pornography, *OJ L 13*, 20.1.2004.

prosecution of criminal offences. The EU only protects its financial interests through legislation that is enforced on its members. This means that the Union still depends on the Member States to enforce its regulations, as in itself the EU has no means of physical coercion of individuals. As Ambos writes: “the designation European criminal law is a kind of umbrella term covering all those norms and practices of criminal and criminal procedural law based on the law and activities of EU and the Council of Europe and leading to widespread harmonisation of national criminal law.”²¹ Therefore, there is no comprehensive, self-contained European criminal law or justice system on its own, but more of an umbrella-like system that connects different entities, organs and EU legislations with the goal to investigate and prosecute transnational crimes²² – mainly connected to the financial interests of the EU.

As defined in Article 83(1) TFEU, the European Parliament and the Council may adopt directives to combat cross-border crimes that threaten the (economic) interests of the EU. The areas of crime eligible for this form of unification are also specified in 83(1) TFEU. These areas are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime. The EU therefore has some powers to harmonise criminal law of the Member States. This harmonisation takes place through an assimilation obligation on the part of the Member States and through the harmonisation of substantive criminal law by means of the EU’s competence to approximate and annex criminal law pursuant to Article 83(1) and (2) TFEU. Based on these competences the EU has issued several directives²³ aiming at harmonising national criminal law.²⁴

The list also includes computer-related crimes. The latter is probably one of the vaguest definitions on the entire list. As computers and information systems have become an essential tool for functioning of modern society, they are also commonly used when committing criminal offences. Therefore, the term ‘computer related crimes’ could include a vast

²¹ Ambos, 2018, p. 14.

²² Ibid., p. 15.

²³ For example, Directive (EU) of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU, *OJ L 156*, 19.6.2018.

²⁴ Šepec and Schalk-Unger, 2023, pp. 203-224.

list of different offences, which opposes the principle of legality, as it is not clear which offences are really meant with the term. This dilemma was at least partly solved with the Directive 2013/40/EU,²⁵ which includes five different offences that can be covered by the category “computer-related crime”. This means that cyberwarfare attacks that are included in the Directive 2013/40/EU are included in the lists of EU crimes after the Article 83(1) TFEU. Cyberwarfare attacks are therefore treated by the EU as crimes with a cross-border dimension of such nature and impact that they need a special treatment – meaning a harmonising legislation on the EU level to prosecute such crimes more efficiently. The already cited Directive 2013/40/EU on attacks against information systems demonstrates it.

It should be emphasised that cyberwarfare has neither a single definition nor a clearly established legal definition. In fact, in most cases, these are already known forms of cyberattacks, which most EU Member States already define as criminal acts. The specific of cyberwarfare is that it is firstly connected with the army of an individual country - i.e. it is a military operation, and secondly that the range and scope of the offence is significantly wider, as it attacks more important targets with significantly more repulsive motives - paralysing the country’s national security via attacks on its infrastructure, technological centres etc.

There is no law in the EU that would directly address cyberwarfare. However, Directive EU 2013/40/EU indirectly addresses the topic of cyberwarfare and cyberwarfare attacks, mainly through more classical cybercrimes.

3.1. Directive 2013/40/EU on attacks against information systems

Directive EU 2013/40/EU on attacks against information systems²⁶ is an upgrade of the unifying work of the Convention on Cybercrime.²⁷ As the Convention before, the Directive contains a list of crimes that Member States must adopt in their national legislation. At the time of the adoption of the Directive in 2013, this list was considered to be extremely advanced and

²⁵ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing council framework decision (2005/222/JHA), *OJ L 218*, 14.8.2013.

²⁶ Directive EU 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, *OJ L 218*, 14.8.2013.

²⁷ Convention of Cybercrime (2001), Council of Europe, CETS No. 185.

contained the most important forms of criminal acts in information systems. However, in the eleven years since its adoption, new forms of cybercrime acts have appeared, so today the Directive represents a minimum standard that should be followed by every serious criminal legislation.

The main objective of the Directive is to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and relevant sanctions. Furthermore, the Directive aims to improve cooperation between competent authorities, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, the European Network and Information Security Agency (ENISA).²⁸

From the substantive aspect the Directive proposes legal definitions of cybercrimes with the aim of their unification between Member States. These definitions include: illegal access to information systems (Article 3), illegal system interference (Article 4), illegal data interference (Article 5), illegal interception (Article 6), tools used for committing offences (Article 7), and incitement, aiding, abetting and attempt (Article 8). The Directive demands penalties for the listed offences, which vary from at least two years of imprisonment for less serious offences, up to at least five years of imprisonment for more serious offences. The Directive also adds the criminal liability of legal persons and the sanctions for legal persons that must be implemented into the national law of EU Member States.

From the procedural perspective, the Directive defines the jurisdiction for prosecution of cyberattacks (Article 12), and also demands exchange of information relating to the offences described in the Directive (Article 13). The EU Member States must also monitor and prepare statistics regarding cybercrimes (Article 14).

In regard to cyberwarfare attacks, the following articles of the Directive are the most relevant. Data interference under Article 5 and system interference under Article 4 are the two main articles for cyberwarfare attacks. They are present in any kind of attack on information system as the target – whether it be denial-of-service attacks, attacks to disrupt critical operations and systems, attacks that disable critical systems and infrastructure, economic disruption by targeting economic establishments, surprise attacks in the context of hybrid warfare, and even

²⁸ Preamble of the Directive, 2013, p. 1.

sabotage. The difference between the two offences is that data interference consists of damaging, deletion, deterioration, alteration or suppression of only computer data, while system interference disrupts the functioning of an information system as a whole (but is performed by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data). Illegal interception of non-public transmissions of computer data under Article 6 could be used in the case of cyber spying and espionage. Last but not least there is Article 7, criminalising the tools used for committing offences. This article could be connected to all types of cyberwarfare attacks because it criminalises any kind of production, sale, procurement, import or distribution of devices, programs or codes that enable the perpetrator to perform one of the criminal offences listed in the Directive. This means that all those who aid the perpetrators of cyberwarfare attacks by providing software or hardware to the attackers will be criminally liable together with the perpetrators. The Directive also covers aiding, abetting and even attempting one of the crimes in the Directive with imposed criminalisation in the Member States (article 8). Meaning that any cooperation in cyber offences, even if not successfully completed will be deemed as criminal offence in the territories of the Member States.

The Directive generally covers all offences related to cyberwarfare attacks by sanctioning illegal interception, data interference, system interference, and aiding and abetting these offences. However, we have to point out that the goal of the Directive was always combatting ordinary cyber offences committed by ordinary perpetrators or hackers, and not cyberwarfare attacks committed by a foreign military or hacker organisation backed by foreign state. This is further evident by the fact that in 2013 when the Directive was adopted, cyberwarfare attacks on Member States was clearly not a major concern. We know that today cyberwarfare attacks pose a much graver threat to the EU security and national security of the Member States than any classic cyberattack committed by ordinary individuals or hacker groups. It is therefore up to the Member States to implement stricter legislation for cyberwarfare offences, or up to the EU to present new legislation that would be more adept to legally combatting cyberwarfare attacks. If the EU wishes to develop a system of joint military defence, a legislation that will provide further protection of the Member States against cyberwarfare attacks would be a viable option in the future.

4. EU cooperation measures and institutions for combatting cyberwarfare crimes

The EU cooperation in combatting cyberwarfare attacks can also be analysed through two perspectives. One is procedural criminal law cooperation where EU Member States combine their efforts in combatting international crimes. The other is cooperation within the EU institutions.

4.1. Procedural criminal law cooperation in the EU

Procedural cooperation measures in criminal matters within the EU are vital for maintaining security, combatting cross-border crimes, and ensuring justice across the EU Member States. Cooperation is executed with the approximation of criminal procedural law of the Member States and with EU legal assistance. The approximation of procedural law is possible in accordance with Article 82(2) TFEU if it is necessary to facilitate mutual recognition of judgments, judicial decisions, and police and judicial cooperation in criminal matters having a cross-border dimension. Minimum rules can be established by means of directives adopted in accordance with the ordinary legislative procedure.²⁹ Legal assistance is based on the approximation of legislation and includes the area of extradition, other mutual assistance in criminal matters (gathering of evidence, searches and confiscations, interrogations of witnesses and suspects), and enforcement assistance³⁰ (execution of judgements and decisions of other Member States's courts).³¹

Given this premise the EU has adopted numerous conventions, directives and framework decisions that all facilitate the mutual cooperation and recognition between Member States. Meaning that the Member State is never alone in gathering of evidence or prosecution of a criminal offence, when the offence was committed internationally, or in the territory of other Member States. For the purposes of prosecuting cyberwarfare crimes, the most relevant procedural measures of the EU are the European Arrest Warrant, the European Evidence Warrant, the European Freezing and Confiscation Order, the European Investigation Order, the European Judicial Network (EJN), and the Schengen Information System (SIS).

²⁹ Ambos, 2018, p. 414. See also Mitsilegas, 2021 and Klip, 2021.

³⁰ For example Council Framework Decision of 13 June 2002 on joint investigation teams, *OJ L 162*, 20.6.2002.

³¹ Ambos, 2018, p. 415. See also Mitsilegas, 2021 and Klip, 2021.

The European Arrest Warrant (EAW)³² allows for the swift extradition of suspects between the EU Member States. It replaces traditional extradition procedures with a simplified and fast-tracked process, aiming to ensure that suspects cannot evade justice by fleeing to another EU country. The European Evidence Warrant³³ enabled Member States to have objects, documents and data confiscated in other Member States. However, it was later replaced with the European Investigation Order (EIO).³⁴ The EIO-Directive established a single comprehensive framework based on the principle of mutual recognition that allows the Member States to obtain evidence from the other Member States. It soon became the leading legal instrument for gathering of evidence in the EU and a useful tool for legal practitioners dealing with offences with a cross-border element.³⁵ With the use of EIO the issuing authority of the Member State can demand certain investigative measures to be executed by the executing authority of another Member State. This enables gathering of evidence on international level as never seen before and is a crucial procedural measure for combatting cyberwarfare attacks on international level.³⁶

The European Freezing and Confiscation Order³⁷ enhances the cooperation among Member States in the area of asset freezing and confiscation in criminal matters. It aims to streamline the process of freezing and confiscating assets across borders within the EU, particularly in cases involving organised crime, terrorism, and other serious offenses, such as cyberattacks, although the latter will probably not be the main target of this order as illegal assets are not a necessity, not the consequence of cyberwarfare attacks.

The European Judicial Network facilitates cooperation and information exchange between judicial authorities in the EU Member States. It helps streamline legal processes, such as mutual legal assistance and

³² Council Framework Decision 2002/584/JHA, *OJ L 190*, 18.7.2002.

³³ Council Framework Decision 2008/978/JHA, *OJ L 350*, 30. 12. 2008.

³⁴ Directive 2014/41/EU, *OJ L 130*, 1.5.2014.

³⁵ See also Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, *OJ L 191*, 28.7.2023.

³⁶ See also Digitalisation of justice in the European Union A toolbox of opportunities, COM/2020/710 final. Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52020DC0710> (Accessed: 10 August 2024).

³⁷ Regulation (EU) 2018/1805, *OJ L 303*, 28.11.2018.

extradition requests, by providing a platform for direct communication and coordination. EJN Contact Points function as active intermediaries and assist with establishing direct contacts between competent authorities and by providing legal and practical information necessary to prepare an effective request for judicial cooperation or to improve judicial cooperation in general.³⁸

The Schengen Information System (SIS) is a centralised database used by Schengen Area countries to exchange information on individuals and objects of interest, such as missing persons, stolen vehicles, and wanted criminals. It helps enhance border security and law enforcement cooperation within the Schengen Zone. From March 2023, SIS contains different types of biometrics (photographs, palm prints, fingerprints, fingermarks, palmmarks) to confirm and verify the identity of people registered in the system.³⁹ Meaning it could provide a useful tool in combatting international cyberwar crimes when searching the perpetrators in the territory of the EU Member States.

Overall, these cooperation measures, based on the principle of mutual recognition, demonstrate the EU's commitment to enhancing security, promoting the rule of law, and combatting crime through cross-border collaboration among its Member States. The EU has legal basis for implementation of procedural measures that can be used to prosecute cyberwarfare crimes on the international level. This cooperation is not of political but of a legal nature - meaning that the Member State does not decide on cooperation politically but is legally bound by EU legislation. Thereby, making this kind of cooperation much more effective.

When it comes to cyberwarfare attacks the procedural mechanisms should suffice for effective criminal prosecution. However, the lack of clear legal definition of cyberwarfare attacks could pose a problem in practice as such attacks will have to be defined only as cyberattacks, although the danger of cyberwarfare attacks is much higher.

³⁸ European Judicial Network [Online]. Available at: <https://www.ejn-crimjust.europa.eu/ejn2021/ContentDetail/EN/2/63>. (Accessed: 10 March 2024).

³⁹ Schengen Information System [Online]. Available at: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en (Accessed: 10 March 2024).

4.2. EU institutions for combatting cyberwarfare crimes in the EU

The European Union has numerous institutions for international cooperation in criminal matters. The most relevant are: Europol, Eurojust, Court of Justice of the European Union (CJEU), European Anti-Fraud Office – OLAF and European Public Prosecutor’s Office (EPPO). However, not all are relevant for combatting cyberwarfare crimes. OLAF deals mainly with financial frauds against the interests of the EU and plays no role in combatting cyberwarfare crimes. Similar can be said for the European Public Prosecutor’s Office (EPPO), which has the power to investigate, prosecute and bring to judgment crimes against the EU budget, such as fraud, corruption or serious cross-border VAT fraud,⁴⁰ but again has practically no jurisdiction on cyberwarfare crimes. Finally, one of the CJEU’s main tasks is to interpret the EU legislation. In this regard the Directive 2013/40/EU on attacks against information systems and other directives that provide cybersecurity protection can be interpreted. However, the CJEU cannot conduct a criminal trial or pass judgement against perpetrators of cyberwarfare attacks and offences. This task falls to the national courts of Member States. In case of misunderstanding the legal regulations of the Union, the CJEU could only be involved in the interpretation of the EU law. Therefore, its role is not as significant as it could have been.

On the other hand, the EU institutions that have a significant role in combatting cyberwarfare crimes are: Europol and its European Cyber Crime Centre, Eurojust, and the European Network and Information Security Agency (ENISA).

The European Union Agency for Law Enforcement (Europol) is the European Union’s most important agency for police cooperation. Its main goal is to support and strengthen the law enforcement agencies of the Member States – especially police.⁴¹ Europol does not have executive powers; it cannot arrest people or conduct investigations on its own. This is clearly evident from Article 88 of the Treaty on the Functioning of the European Union, which states that the application of coercive measures shall be the exclusive responsibility of the competent national authorities.

⁴⁰ European Public Prosecutor’s Office [Online]. Available at: https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/european-public-prosecutors-office_en (Accessed: 20 December 2023).

⁴¹ Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol), *OJ L 135*, 24.5.2016.

Europol facilitates the exchange of information and intelligence, provides analytical support, and offers specialised training and expertise. Some of Europol's principal areas of attention as listed in the Annex I to the Europol Regulation, include drug trafficking, trafficking in human beings, cybercrime, money laundering, and terrorism. The list is quite similar to that of crimes for which the Council Framework Decision 2002/584/JHA on the European Arrest Warrant and the other EU instruments of mutual recognition do not require the double criminality standard.⁴²

In regard to cyberwarfare attacks, Europol has important data processing tasks that include gathering and processing information, incorporating criminal intelligence, and performing strategic and operational analysis. Although, Europol does not have coercive powers, the institution's information gathering generates knowledge and can lead to data evidence that can be used in a national court procedure.⁴³ Europol is therefore an essential partner of national authorities when discovering cybercrime offences with international element. This is especially evident when Europol co-ordinates organisation and execution of investigations together with the Member States or within the framework of joint investigative teams. For this purpose, Article 4(1) of Europol Regulation (EU) 2016/794 stipulates that Europol shall develop Union centres of specialised expertise for combatting certain types of crime falling within the scope of Europol's objectives. The foremost consideration being the European Cybercrime Centre.

Europol's European Cybercrime Centre (EC3) is a specialised unit within Europol, dedicated to combatting cybercrime at the EU level. It serves as a central hub for coordinating and supporting law enforcement efforts across the EU Member States in addressing cyber threats and cyber-enabled crimes. The main objectives of the European Cybercrime Centre include:

1. Facilitating information sharing and collaboration among the EU Member States' law enforcement agencies regarding cyber threats and incidents.
2. Providing operational support and expertise to assist in investigations related to cybercrime.
3. Conducting strategic analysis and threat assessments to identify emerging trends and threats in the cybercrime landscape.

⁴² Ligeti and Giuffrida, 2023, p. 367.

⁴³ Ibid., p. 385.

4. Enhancing capacity-building initiatives to improve the capabilities of EU Member States' law enforcement agencies in combatting cybercrime.
5. Cooperating with international partners, such as other law enforcement agencies, private sector entities, and academia, to strengthen global cybersecurity efforts.⁴⁴

Overall, the European Cybercrime Centre plays a crucial role in enhancing cybersecurity and combatting cybercrime within the European Union and beyond.

Eurojust is the European Union Agency for Criminal Justice Cooperation. The main goal of the agency is to enhance collaborative efforts in criminal investigations and prosecutions of serious cross-border and organised crimes in the EU.⁴⁵ Eurojust was established out of need for a centrally coordinating cross-border prosecution of the most serious crimes in the EU. This can only be done by decentralised network of national contact points. Therefore, it was necessary to create an additional central body in which the representatives of the judicial authorities of all Member States are located.⁴⁶

Eurojust's primary functions include the initiation and coordination of criminal investigations and prosecutions across Member States, and strengthening judicial cooperation of Member States.⁴⁷ Eurojust lacks any real formal investigative powers, as the decision to investigate or prosecute a crime in a Member State falls to the national authorities.⁴⁸

Eurojust's jurisdiction covers crimes listed in Annex 1 of the Regulation (EU) 2018/1727, which includes the familiar list of EU crimes also including "computer crime". Therefore, according to the principle of legality, Eurojust has jurisdiction over computer crimes listed in the Directive 2013/40/EU which includes five different offences: illegal access to information systems, illegal system interference, illegal data interference, illegal interception, and tools used for committing offences. This means that Eurojust has competencies over cybercrime and cyberwarfare offences when

⁴⁴ European Cybercrime Centre – EC3 [Online]. Available at: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>. (Accessed: 20 January 2024).

⁴⁵ Regulation (EU) 2018/1727 on the European Union Agency for Criminal Justice Cooperation (Eurojust), *OJ L* 295, 21.11.2018.

⁴⁶ Ambos, 2018, p. 569.

⁴⁷ *Ibid.*, p. 570.

⁴⁸ *Ibid.*, p. 570.

committed against or in EU Member States (Denmark being the exception because of the special regime foreseen in the Protocol no. 22 of the Lisbon Treaty).

Finally, there is the European Network and Information Security Agency (ENISA). The agency is tasked with enhancing cybersecurity across Europe. ENISA endeavours to optimise cybersecurity capability, awareness, and cooperation among EU Member States, as well as with private sector organisations and international partners. It provides expertise, advice, and recommendations to support the development and implementation of EU cybersecurity policies and strategies. ENISA also conducts research, organises training and awareness-raising activities, and facilitates information sharing and collaboration to strengthen Europe's cyber resilience.

The main functions of ENISA include its advisory role (it provides expert advice and guidance to EU institutions, Member States, and private sector stakeholders on cybersecurity issues); capacity building role (enhancing the cybersecurity capabilities of EU Member States and organisations, organising training programs, workshops, and exercises to improve cybersecurity skills, knowledge, and best practices); risk assessment and management in order to mitigate cybersecurity risks at both national and EU level (this also helps in identifying vulnerabilities and threats and developing appropriate risk management strategies); incident response support to cybersecurity incidents and crisis; promoting the development and implementation of cybersecurity standards and certification schemes that helps in harmonising cybersecurity practices and ensuring a common level of security; research of cybersecurity technologies, methodologies, and solutions; and finally awareness raising about cybersecurity threats, risks, and best practices.⁴⁹

Regarding cyberwarfare attacks the three main institutions (Europol, Eurojust, ENISA) do have the necessary jurisdiction for involvement in the criminal prosecution of such crimes. However, their lack of any real formal investigative powers remains a persistent problem, as they are practically useless without formal authorisation of the national authorities of a Member State that has experienced a cyberwarfare attack.

⁴⁹ European Cybercrime Centre – EC3 [Online]. Available at: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>. (Accessed: 20 March 2024).

5. Conclusion

Cyberwarfare crimes constitute a major threat to the security of the European countries. The effects of such attacks could be devastating for European economy, stability and national security. Therefore, sensible legal definitions, immediate criminal prosecution and effective cooperation between EU Member States is of crucial significance. A collective action by EU Member States is essential to identify the perpetrators of such attacks, gather evidence of criminal offences and protect its borders and citizens from this new type of external or even internal threats.

Unfortunately, no legal instrument is available in the EU that would directly address cyberwarfare, given the absence of a precise legal definition for the term. The main substantive legal document that addresses cybercrimes is the Directive 2013/40/EU. Although the Directive generally covers all offences related to cyberwarfare attacks, its goal was consistently combatting ordinary cyber offences committed by ordinary perpetrators or hackers, and not cyberwarfare attacks committed by a foreign military or hacker organisation backed by foreign states. It is therefore up to the Member States to implement stricter legislation for cyberwarfare offences, or up to the EU to present new legislation that would be more adept to legally combatting cyberwarfare attacks.

On the procedural level the EU cooperation in combatting cyberwarfare attacks can be analysed through two perspectives. One is procedural criminal law cooperation where the EU Member States combine their efforts in combatting international crimes. The other is cooperation within the EU institutions.

The EU has adopted numerous conventions, directives and framework decisions that all facilitate mutual cooperation in criminal issues and recognition between the Member States. These cooperation measures, based on the principle of mutual recognition, demonstrate the EU's commitment to enhancing security, promoting the rule of law, and combatting crime through cross-border collaboration among its Member States. The EU therefore has strong legal basis for implementation of procedural measures that can be used to prosecute cyber warfare crimes on the international level. This cooperation is not of political but of a legal nature - meaning that the Member State does not decide on cooperation politically but is legally bound by EU legislation. Thereby, making this kind of cooperation much more effective.

The European Union also has several institutions for international cooperation in criminal issues. Although EU's three main institutions (Europol, Eurojust, ENISA) do have the necessary jurisdiction for involvement in the criminal prosecution of such crimes, they still lack any kind of investigative powers. These lie solely in the hands of the national authorities of a Member State that has experienced a cyberwarfare attack.

Although Europe has mechanisms in place to combat and prevent cyberwarfare crimes, the legal situation is still far from ideal. The main problem remains the lack of clear legal definition of cyberwarfare crimes and the absence of targeted legislation in regard to criminal prosecution of such crimes. Cyberwarfare attacks therefore remain in the domain of classical cyberattacks, which have a much smaller scope and meaning than cyberwarfare attacks. It is therefore up to the Member States to implement stricter legislation for cyberwarfare offences, or up to the EU to present new legislation that would be more adept to legally combatting cyberwarfare attacks. If the EU wishes to develop a system of joint military defence, a legislation that will provide further protection of the Member States against cyberwarfare attacks would be a viable option in the future.

Bibliography

- [1] Ambos, K. (2018) *European Criminal Law*. Cambridge: Cambridge University Press, <https://doi.org/10.1017/9781316348628>.
- [2] Bernik, I. (2014) *Cybercrime and cyber warfare*. London: John Wiley & Sons, <https://doi.org/10.1002/9781118898604>.
- [3] Bussolati (2015) 'The Rise of Non-State Actors in Cyberwarfare' in Ohlin, J. D., Govern, K., Finkelsterin, C. (eds.) *Cyber War: Law and Ethics for Virtual Conflicts*, Oxford: Oxford University Press, pp. 102-126; <https://doi.org/10.1093/acprof:oso/9780198717492.003.0007>.
- [4] 'Europol' in Ambos, K., Rackow, P. (eds.), *The Cambridge Companion to European Criminal Law*, Cambridge: Cambridge University Press, pp. 361-386.
- [5] Clough, J. (2010) *Principles of cybercrime*. Cambridge: Cambridge University Press, <https://doi.org/10.1017/CBO9780511845123>.
- [6] Digmelashvili, T. (2023) 'The Impact of Cyberwarfare on the National Security', *Future Human Image*, 19, pp. 12-19; <https://doi.org/10.29202/fhi/19/2>. <https://doi.org/10.29202/fhi/19/2>.
- [7] Klip, A. (2021) *European Criminal Law: An Integrative Approach*, 4th edition. Cambridge: Intersentia.
- [8] Ligeti, K., Giuffrida, F. (2023) 'Europol' in Ambos, K., Rackow, P. (eds.) *The Cambridge Companion to European Criminal Law*, Cambridge: Cambridge University Press, pp. 361-386.
- [9] Maras, M. H. (2016) *Cybercriminology*. Oxford: Oxford University Press.
- [10] Mitsilegas, V. (2021) *EU Criminal Law*, 2nd edition. Oxford: Hart Publishing, <https://doi.org/10.1017/9781108891875.021>.

-
- [11] Snider, K., Shandler, R., Zandani, S., Canetti, D. (2021), 'Cyberattacks, cyber threats, and attitudes toward cybersecurity policies', *Journal of Cybersecurity*, 7(1), pp. 1-11; <https://doi.org/10.1093/cybsec/tyab019>.
- [12] Šepec, M., Dugar, T., Stajniko, J. (2023) 'European Investigation Order – A Comparative Analysis of Practical and Legal Dilemmas' in Ambos, K., Heinze, A., Rackow, P., Šepec, M. (eds.) *The European investigation order: legal analysis and practical dilemmas of international cooperation*, Berlin: Duncker & Humblot, pp. 123-137.
- [13] Šepec, M., Schalk-Unger, L. (2023) 'Special part of EU criminal law: the level of harmonization of the categories of offences listed in annex D in EU legislation and across selected member states' in Ambos, K., Heinze, A., Rackow, P., Šepec, M. (eds.) *The European investigation order: legal analysis and practical dilemmas of international cooperation*, Berlin: Duncker and Humblot, pp. 203-224.
- [14] Consolidated version of the Treaty on the Functioning of the European Union PROTOCOLS - Protocol (No 22) on the position of Denmark, OJ C 326, 26.10.2012.
- [15] Convention of Cybercrime (2001), Council of Europe, CETS No. 185, Budapest, 23 Nov. 2001.
- [16] Convention on the Protection of the EU's Financial Interests and its Protocols, Council Regulation (EC, Euratom) no. 2988/95 of 18 December 1995 on the protection of the financial interests of the European Communities in relation to administrative sanctions, OJ L 312, 23 December 1995.
- [17] Council Framework Decision 2004/68/PNZ of 22 December 2003 on combating the sexual exploitation of children and child pornography, Official Journal L 013, 20/01/2004.

- [18] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, OJ L 350, 30. 12. 2008.
- [19] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002.
- [20] Council Framework Decision of 13 June 2002 on joint investigation teams, OJ L 162, 20.6.2002.
- [21] Cybersecurity: how the EU tackles cyber threats [Online]. Available at: <https://www.consilium.europa.eu/en/policies/cybersecurity/> (Accessed: 25 August 2023).
- [22] Cybersecurity: why reducing the cost of cyberattacks matters, European Parliament [Online]. Available at: <https://www.europarl.europa.eu/news/en/headlines/society/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters>. (Accessed: 10 October 2023).
- [23] Cyber Warfare, Imperva [Online]. Available at: <https://www.imperva.com/learn/application-security/cyber-warfare/> (Accessed: 25 August 2023).
- [24] Digitalisation of justice in the European Union A toolbox of opportunities, COM/2020/710 final. Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52020DC0710> (Accessed: 10 August 2024).
- [25] ENISA [Online]. Available at: <https://www.enisa.europa.eu/> (Accessed: 20 March 2024).
- [26] ENISA (2020) *A trusted and cyber secure Europe*. Brussels: European Agency for Cyber Security.

- [27] European Cybercrime Centre – EC3 [Online]. Available at: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (Accessed: 20 January 2024).
- [28] European Judicial Network [Online]. Available at: <https://www.ejn-crimjust.europa.eu/ejn2021/ContentDetail/EN/2/63> (Accessed: 30 March 2024).
- [29] European Public Prosecutor's Office [Online]. Available at: https://anti-fraud.ec.europa.eu/policy/policies-prevent-and-deter-fraud/european-public-prosecutors-office_en (Accessed: 20 December 2023).
- [30] Schengen Information System [Online]. Available at: https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en (Accessed: 10 March 2024).
- [31] The Cybersecurity Act, European Commission [Online]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>. (Accessed: 10 October 2023).
- [32] U.S. Army Cyber Command [Online]. Available at: <https://www.arcyber.army.mil/> (Accessed: 30 August 2023).

JÁNOS SZÉKELY*

Export Restrictions in the Field of Artificial Intelligence and Quantum Computing: Justification and Risks – The United States–China Rivalry from a European Union Perspective**

ABSTRACT: The study aims to elicit the problems posed under international law and, to a lesser extent, under European Union (EU) law by export controls imposed on foundational transformative technologies such as artificial intelligence and quantum information technology in the relations between United States and People's Republic of China. It examines the notion of export controls and its evaluation under international law, finding that such an evaluation of the legal nature of these measures remains unclear on not only whether these measures may constitute economic coercion but also whether such coercion is prohibited. Further uncertainty persists regarding whether other legal foundations may be identified, which would permit such measures when they affect critical technologies for future development. The study finds that, currently, export controls affecting artificial intelligence and quantum information technology are limited but expanding, thereby creating some urgency in finding legal solutions to counteract their effects. Updating of the EU legal infrastructure, which is not ready to counteract the unintended effects of export controls on the EU, is also found as necessary.

KEYWORDS: export controls, economic coercion, artificial intelligence, quantum information technology, United States, People's Republic of China, European Union.

* PhD, Senior University Lecturer, Sapientia Hungarian University of Transylvania, Cluj-Napoca Faculty, Department of Law, Cluj-Napoca, Romania. <https://orcid.org/0000-0003-4254-2054>, szekely.janos.jr@okt.kv.sapientia.ro.

** The research and preparation of this study was supported by the Central European Academy.

1. Introduction

Technological development, as well as societal resilience, are contingent in large part on unhindered, cross-border flow of information (e.g. scientific discoveries) and of other assets or goods (e.g. tangible assets including raw materials, manufacturing technologies, and various manufactured items such as advanced semiconductors and other computer hardware, as well as intangible assets such as specialised knowledge and manufacturing know-how) that integrate the latest advancements. Therefore, free flow of these assets—that is, freedom of trade in the widest possible sense—is significant to global, regional and national techno-economic development. Such free flow also provides exchanges that allow research, development, and marketing of new technologies for significant potential profit in the framework of a self-reinforcing virtuous cycle.¹

Therefore, any conditions that result in constraints on the freedom of trade must necessarily—and conversely—lead to serious economic consequences on the one hand and hinder technological development as a whole on the other. Erection of trade barriers, including in the form of export controls—regardless of the reason—constitutes such a type of constraint. When such measures are instituted regarding cutting-edge technologies, the stakes become even higher. Yet, this is exactly the situation in which the world economy now finds itself, after several waves of export controls instituted by the United States (US) against the People's Republic of China (PRC) and the counter-restrictions implemented by the same token.²

Restrictions of this type, however onerous on the parties directly at odds with each other, should be viewed from not two but rather three different perspectives: that of the “sender,” the supplier instituting the export restrictions having considerable leverage due to monopoly on the supply of the controlled assets; the “target” meant to be affected by the restrictions; and third parties suffering the consequences of the extraterritorial effects or the general economic consequences of export controls.

¹ See Grossman and Helpman, 1995; Garnsey, 1998; Goertzel, Goertzel and Goertzel, 2017; Markolf et al., 2018.

² See Hryniv, 2022; Köstner and Nonn, 2023; ‘The United States announces’, 2023.

In this study, I first aim to briefly elicit the notion of export controls and enumerate some of their negative effects; then, I introduce the related concepts of economic securitisation and economic coercion, by which trade exchanges and economic advantage become subjected to national security-oriented actions. Second, I delve into the international law implications of export controls as forms of economic coercion when they affect a vital resource. I refer to the example of the 1973–1974 oil embargo that resulted in differing views on the legality of such controls. These views are, in my opinion, now being overlooked, even though artificial intelligence (AI) and quantum information technology (QIT) are predicted to be more transformative to mankind's long-term development compared to oil (petroleum). The present study does not aim to thoroughly analyse the specifics of such dual-use technologies, the transformative nature of which is now taken as fact, focussing instead on the implications of the export regulations applicable to them.³ Third, I examine the export controls applied to AI and QIT instituted by the US against the PRC starting in 2019, which were later extended several times. I view this set of export controls from the technological and the international law perspective, considering their effects on the European Union and its member states as not only partners to the export controls but also affected third parties. Finally, I endeavour to speculate on some future developments and legislative necessities in the field of export controls aimed at restricting the export of AI- and QIT-related items.

2. Export Controls and Economic Securitisation

Export controls of what are considered sensitive technologies likely date back to time immemorial.⁴ However, the 20th century brought a never-before-seen widening in the scope of such measures⁵ when it comes to technologies considered vital to the national interest of, especially, major powers. Such controls exist in different forms, which include export prohibitions (export bans or embargos); licensing requirements for the export of certain assets; export quotas, export taxes, or minimum export

³ For a description of such technologies and the technological rationale for restricting their exports, see Székely, 2024.

⁴ For some historical examples, see Voetelink, 2022a, p. 70.

⁵ See Aubin and Idiart, 2016. For a comprehensive history of export controls in a wide sample of jurisdictions, including in Hungary, see Tamotsu, 2016.

prices; and even establishment of a state monopoly on the export of assets.⁶ In the course of this study, I shall focus mainly on the first two categories of export controls among those listed, as targeted export bans and onerous licensing requirements have been put into place in recent years, affecting technologies necessary for the deployment of AI and QIT.

The justification for instituting export controls may differ, with economic and strategic considerations often intertwined. Some controls may be instituted for pure economic advantage (preventing the adoption of technologies by competitors, enhancing domestic production or protecting strategic industries from competition, protecting intellectual and industrial property from being unlawfully acquired by others, etc.). Others may aim to defend—broadly, wholly, or at the very least partly—non-economic interests, such as maintaining a technological edge over perceived adversaries and preventing⁷ proliferation of some categories of weapons or technologies with possible dual uses (military and civilian, nefarious and beneficial, and moral and immoral).⁸

A specific reason for the institution of restrictive measures, regarding not only dual use but also single use of even (apparently) purely civilian technologies, is the increasing “securitisation” of economic interactions between various states. Securitisation denotes an approach by which economic and technological advantages, as well as maintenance of those advantages, are considered paramount to national security; this approach is not new but is experiencing renewed resurgence.⁹ While securitisation has historically been considered exceptional as a reason for restricting trade flows and instituting restrictions on exports, among other forms of trade, a new and worrying normalisation of such measures is now occurring.¹⁰ This has made the measures’ study all the more essential to predict the future risks posed by the fragmentation of trade in and development of advanced technologies.

Export restrictions evidently affect trade relations and result in the sub-optimal allocation of resources when viewed from the global economic

⁶ Bonarriva, Koscielski, and Wilson, 2009, p. 2.

⁷ See Lentzos and Silver, 2012; Hryniv, 2022.

⁸ For the varying notions collected under the term of “dual-use technology,” see Sanchez, 1987; Rath, Ischi, and Perkins, 2014.

⁹ Casarini, 2013, p. 182; Mawdsley, 2013, pp. 11–12; Mola, 2023.

¹⁰ See Floyd, 2007, 2019.

perspective. Some of their impacts have been summarised in the relevant literature:¹¹

1. Export controls lead to lost business for exporters from the jurisdiction that has instituted such controls, as well as from other jurisdictions, even those not involved in tensions that prompted the controls in the first place, if they are applied extraterritorially.
2. Such controls reconfigure economic and trade flows, thereby advantaging actors that can circumvent them at the expense of those that are compliant.
3. They hinder knowledge transfer and therefore technological and wider economic development, especially in a context where such development stems from international cooperation. This occurs even if the information or knowledge concerned is not strictly technology relevant (e.g. export controls instituted on certain items also prevent market research related to these items in countries to which they could not be exported). Export controls, especially in the category of so-called “deemed exports,” may even prevent *domestic* knowledge transfer, such as in academic settings, even if the information being disclosed is just export restricted and not classified.
4. Export controls reduce competitiveness by imposing onerous compliance requirements (e.g. internal and external compliance checks) on exporters, not only regarding items, knowledge, and technologies specifically subjected to control measures but also where it is questionable if such controls are even applicable. Transaction costs are also increased due to the discretionary nature of some export controls.
5. Re-exports or maintenance may also be prohibited by export controls. Moreover, even the transfer of non-controlled items is subject to export controls if they use other, controlled items. For example, if an assembly line manufactured in a jurisdiction, and in turn exported, is used to manufacture items in that second jurisdiction, which would then, in turn be exported to a third jurisdiction, it is subject to export controls.
6. Investment in capital-intensive export-related activities may be reduced if risks of export controls persist, as such situations constitute a disincentive to both producers and exporters.

¹¹ Seyoum, 2017, p. 55.

Along with import restrictions and other measures meant to impede free trade, regardless of the reason for their imposition, export controls may constitute a subcategory of conduct known as economic coercion¹² in international relations. According to this, outside other, preponderantly domestic economic purposes (e.g. raising government revenue, promoting domestic industries, diversification of exports, etc.),¹³ a state with control over the supply, markets, or distribution of a given tangible or intangible asset will seek to control the distribution of that asset. The aim is to modify the economic, political, or other conduct, or the posture of another state¹⁴ by, *inter alia*, discouraging it from a given policy, forcing the withdrawal or amendment of a given policy, or forcing compliance with the policy choices of the state initiating economic coercion.¹⁵

Economic coercion, at a significant cost to the “sender” (actor initiating the export controls) was found¹⁶ to be in correlation with a higher expectation of future conflict with the “target” (e.g. actor suffering the effects of export restrictions). Despite the apparent futility of such measures in some cases, there is ample evidence to show that economic coercion is efficient, specifically in shaping the conduct of the target state, in ways that are seldom made public.¹⁷

It is worthwhile to note that public discourse currently tends to differentiate between trade restrictions imposed by Western powers, which usually *are not* labelled as coercive but rather defensive (e.g. export controls and restrictions imposed on semiconductor exports to the PRC are usually set in the framework of mitigating national security threats), even if such measures clearly conform to the definition¹⁸ of economic coercion. However, similar measures imposed by non-Western powers, including the PRC (e.g. possible export control¹⁹ measures instituted against Taiwan) *are*

¹² See Chapman, 2013, p. 331; Hackenbroich, Medunic, and Zerka, 2022; OECD, 2024.

¹³ Bonarriva, Koscielski, and Wilson, 2009, pp. 2–5.

¹⁴ Olson, 1979; Drezner, 2003, p. 645; Uren, 2020.

¹⁵ Tanner, 2007, p. 13.

¹⁶ See Drezner, 1998.

¹⁷ Drezner, 2003, pp. 652–656.

¹⁸ A functional definition of economic coercion is given by Drezner, in the following form: ‘... the threat or act by a sender government or governments to disrupt economic exchange with the target state, unless the target acquiesces to an articulated demand’ Drezner, 2003, p. 643. For an expanded but essentially identical definition, as well as an analysis of various definitions, see Carter, 2009. For the intricacies of properly defining economic coercion, see Tzanakopoulos, 2015, pp. 618–623.

¹⁹ Tanner, 2007, pp. 16–17.

regularly labelled as being coercive.²⁰ Several measures²¹ taken by the PRC in fact differ little from similar measures exercised by other great powers, leaving room for perceived hypocrisy. The effect is the institution of a “siege mentality” in the target country, ultimately subverting the goals of the coercive measures themselves.²² This apparent double standard is not at all new. The most poignant examples constitute, on the one hand, the vehement Western (specifically US) reaction to the 1973–1974 oil embargo instituted by several OPEC members, initiated by what were deemed as “third-world” countries, and, on the other hand, the widespread use of economic coercion against states in the Global South throughout the Cold War and beyond for the advancement of Western economic or political agendas.²³

3. Evaluating Economic Coercion Through Export Controls in International Law: The Old Oil and the New

As evident from the above, the relationship of export controls with the written and unwritten rules of international order and international trade is of interest. This is all the truer in determining the possible actions taken by state participants for present and future conflicts with an economic and/or military component, especially since economic coercion, in the form of weaponised economic policies and sanctions, may constitute an act tantamount to economic warfare.

The prohibition of using economic or political coercion is apparently settled—in principle—in both binding and non-binding international instruments, even if international coercion itself is considered an indispensable part of what is deemed “diplomacy.”²⁴ As such coercion is usually an instrument most readily available to great powers or alliance systems, international raw material export cartels that have a monopoly over certain assets and states situated in geographic bottlenecks should also be noted. Some states will inevitably have significantly wider powers of coercion than others.

²⁰ See, for example, Piekos, 2023.

²¹ See Reynolds and Goodman, 2023. See also Nanopoulos, 2023.

²² Gueorguiev, McDowell, and Steinberg, 2020.

²³ See Olson, 1979; Zoller, 1984, p. 70; Subrahmanyam, 1993.

²⁴ Farer, 1985, pp. 405–407; ‘The use of nonviolent coercion’, 1974, pp. 990–991.

Article 2(4) of the United Nations (UN) Charter²⁵ provides for general prohibition of ‘the threat or use of force’. The cited text suffers from inadequacy in its construction (which may or may not be deliberate) by not defining the notion of “force,” thus allowing the co-existence of several competing interpretations regarding whether (1) the framers envisaged the prohibition of economic coercion as falling under the ambit of the rule and, (2) if they did, whether the prohibition is a rule of international *jus cogens* or simply a future or even unattainable desiderate in international relations.²⁶

Under this perspective, it remains questionable whether economic coercion in the form of export controls may constitute a prohibited use of force. The Preamble of the Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States, in accordance with the UN Charter, expands on the interpretation of the use of force:

No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organise, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State.²⁷

An identical text is included in the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty.²⁸

Both latter instruments are mere declarations and thus are non-binding; yet, their relation to the UN Charter permit them to spell out the principle of the prohibition of use of force as well as its constitutive elements. The juxtaposition of economic coercion with violent forms of

²⁵ According to the United Nations Charter, 1945, ‘All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations’.

²⁶ ‘The use of nonviolent coercion’, 1974, pp. 986–988.

²⁷ UN General Assembly, 1970.

²⁸ UN General Assembly, 1965.

force in the cited texts—in and of itself—shows that the two categories were meant to be evaluated as, at the very least, comparable by the framers of the declarations.²⁹ The UN declarations on friendly relations and non-intervention were intended to be authoritative sources for the interpretation of the UN Charter and were quasi-unanimously adopted as such.³⁰

The case has been made for a narrow interpretation of Article 2(4) of the UN Charter, arising specifically from the declaration on friendly relations.³¹ However, these declarations were at the time widely construed—including by the US—as prohibiting economic coercion in the context of the 1973–1974 oil embargo. This interpretation was later embraced in paragraph 4 of UN General Assembly Resolution 3171 (XXVIII) of 17 December 1973 – Permanent Sovereignty Over Natural Resources.³² Such wider interpretation also appears preferable because not only was it included in some later instruments but framers of Article 2(4) of the UN Charter also clearly did not envisage a restrictive interpretation of “force” (as evident from the lack of any further adjectives, or attributes associated with the notion, such as “armed force” as in Article 46 of the Charter). Furthermore, an expansive interpretation is compatible with the spirit of the charter and the initial intention of the framers to advance world peace and suppress aggression; this latter notion is itself broadened by early UN General Assembly resolutions to an extent that may include economic coercion, which is in a way compatible with the general direction of post-Second World War evolution of international law.³³

The inadequacy of the generally formulated prohibition of economic coercion was pointed out in the literature, with some authors arguing that such actions, as tools of international relations, are in reality often used and rarely complained about.³⁴ It was also stated that if economic coercion might be considered a use of force (aggression) under the UN Charter, for such measures to be permissible under international law, they would have to fall within the distinct categories of self-defence, UN-authorised reprisals

²⁹ As noted in the literature, legal scholars and states in the Global South from the outset advocated such an interpretation, equating economic coercion with threat or use of force, which was only adopted by the US during the 1973–1974 oil embargo. Lillich, 1975, pp. 360–361.

³⁰ Lillich, 1975, pp. 362–364.

³¹ See ‘The use of nonviolent coercion’, 1974, pp. 994–997.

³² UN General Assembly, 1973.

³³ ‘The use of nonviolent coercion’, 1974, pp. 997–1010.

³⁴ Farer, 1985, p. 406.

against actions incompatible with the UN Charter, or “countermeasures” involving the unilateral suspension of obligations assumed under international agreements (a category I shall briefly discuss below). Therefore, economic coercion in cases that do not fall within one of these categories might even warrant armed retaliation based on the aforementioned principles, especially the right to self-defence.

This last distinct possibility was in fact discussed as a justification in international law to a proposed military response by the US to end the 1973–1974 oil embargo.³⁵ The embargo, as a moment in history, is all the more significant. This is because it was in the context of this unprecedented measure of coercion that the doctrine of equal access to raw materials was proposed as a new *jus cogens* rule that was later codified into international public law. The embargo was in effect qualified as a form of use of force by economic coercion, contrary to Article 2(4) of the UN Charter, because it deprived industrialised Western powers, all of them oil importers, from a vital resource.³⁶ This doctrine was included in one form into Article 6³⁷ the Charter of Economic Rights and Duties of States.³⁸ While the language of Article 6 “particularly” refers to “commodities” (i.e. raw materials), the intention is clear: The international trade of goods should not be hindered by economic coercion (at last not when industrialised states would suffer a penury of raw materials imported from the Global South as a result). Any state that does so may run afoul of the provisions of Article 2(4) of the UN Charter.

One further problem raised in international public law must be examined when qualifying economic coercion as a possible form of the use

³⁵ Farer, 1985, pp. 411–413. In Farer’s opinion, economic coercion would only present sufficient gravity as to be considered aggression if it were directed against the territorial integrity or political independence of a state (in my opinion, ignoring the final provisions of Article 2(4) of the UN Charter).

³⁶ Lillich, 1975, p. 370.

³⁷ According to the UN General Assembly, 1974.

It is the duty of States to contribute to the development of international trade of goods, particularly by means of arrangements and by the conclusion of long-term multilateral commodity agreements, where appropriate, and taking into account the interests of producers and consumers. All States share the responsibility to promote the regular flow and access of all commercial goods traded at stable, remunerative and equitable prices, thus contributing to the equitable development of the world economy, taking into account, in particular, the interests of developing countries.

³⁸ Lillich, 1975, p. 371.

of force: While the UN Charter may be considered a primary and *jus cogens* norm when it comes to obligations set forth for states, and it seems to prohibit economic coercion—or at least it seemed so during the 1973–1974 oil embargo—this is not always the case with secondary international law. We have seen that the general prohibition of economic coercion is not universally accepted, as international relations are said to presuppose a given amount of coercion by their very nature.

A true tension therefore exists³⁹ between the primary rule of international law (prohibiting use of force) and the secondary rules, which seem to allow for coercion,⁴⁰ preventing the institution of the fundamental right of states to be entirely free of such coercion by other states. Coercion, taking the form of self-help, or “countermeasures” (as referred to in Articles 49–51 of the document titled Responsibility of States for Internationally Wrongful Acts⁴¹ [ARSIWA] submitted in the UN General Assembly by the UN International Law Commission), is thought to be inevitable in enforcing compliance with some rules of international conduct.⁴² Such countermeasures may be limited in scope and proportionality.

They may be enacted in the context of Article 49 of the ARSIWA, which provides as follows:

Object and limits of countermeasures

1. An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under part two.
2. Countermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State.
3. Countermeasures shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question.

It is clear from the norm that such countermeasures would not cover all possible forms of economic coercion, mainly allowing for material and

³⁹ Tzanakopoulos, 2015, p. 617.

⁴⁰ Zoller, 1984, pp. 70–73.

⁴¹ UN General Assembly, 2001.

⁴² Tzanakopoulos, 2015, pp. 624–627.

temporary non-performance of some international obligations (except those excluded by Article 50 of the ARSIWA). It is questionable if they would even cover all forms of export restrictions (although in my opinion, it is likely that the restriction of commodity exports as referred to above would be permitted as a countermeasure).

In any case, such countermeasures, as well as similar compliance-inducing instruments accepted in international practice because of the breadth of their effects—which may include intervention into the foreign affairs of other states (e.g. as seen during the Greek sovereign debt crisis) that may radically coerce a state to adhere to international agreements or adopt a behaviour favourable to other states—seem to exclude the existence of the fundamental right of states to be entirely free from coercion.⁴³ However, this does not mean that any wanton measure of coercion, regardless of its nature and magnitude, would be allowed. In fact, unjustified coercion seems as much excluded by the above norms of international law as the right to be free from coercion.

To this legal tension another one is added, due mainly to the political nature of economic coercion when it is utilised. As noted in the context of the 1973–1974 oil embargo, US protestations against what it deemed to be economic coercion stand in stark contrast with the fact that coercive economic measures were quite prevalent in US foreign policy in the same period.⁴⁴ Such measures remain prevalent today. Coercion by the US and other Western states was often complained about by others, especially in the region that today would be called the Global South.⁴⁵ Economic coercion, as evident, is best practiced by major powers.⁴⁶ Therefore, economic coercion seems to be a measure that, when proposed or implemented by some major powers, seems less contested than it is when implemented against the same powers. This elicits what can only be called a double standard, prejudicious to the conceptual unity of international law.

It is interesting to note that Article 52 of the Vienna Convention on the Law of Treaties of 1969 provides for rendering null and void any international convention reached under the ‘threat or use of force in violation of the principles of international law embodied in the Charter of

⁴³ Tzanakopoulos, 2015, pp. 630–633.

⁴⁴ Lillich, 1975, pp. 364–365.

⁴⁵ Olson, 1979.

⁴⁶ Farrell and Newman, 2019.

the United Nations’.⁴⁷ Even if this provision is generally considered⁴⁸ to not invalidate treaties reached as a result of economic coercion, the very existence of the text is significant, as it is still apt to undermine any settlement that may flow from such coercion.

It is also worthwhile to note that another sort of tension exists under international law concerning export restrictions and other means of coercion—the principle of freedom of trade (trade in weapons is not included here)—which is recorded in numerous instruments, even if this tension is apparently alleviated by clauses enshrined in such instruments. Examples of the instruments include Article XXI(b)(ii)—and also XXI(b)(iii)—of the General Agreement on Tariffs and Trade in its 1994 iteration and Article 346(1)(b) of the Treaty on the Functioning of the European Union.⁴⁹ Both texts, which mirror each other quite closely, refer to trade in arms, other implements of war, or—in the case of Article XXI(b)(iii) of the General Agreement on Tariffs and Trade—war or other international emergencies, while Article XXI(b) mentions ‘essential security interests’. Therefore, these instruments do not envisage permitting disruption to (global) free trade between their parties, based on any unspecified threats to national security, such as simply maintaining national economic supremacy. It has even been argued, that ‘essential security interests’ alone, in the absence of armed conflict, may not justify disruption of free trade at all.⁵⁰ Export restrictions not enacted within the rather strict confines of these texts may thus constitute a breach of the listed instruments.⁵¹

The scope of the application of economic coercion in the possible wider interpretation of Article 2(4) of the UN Charter, as outlined above, is mostly limited to trade in critical raw materials (such as oil). Nevertheless, there is an argument to be made for a possible analogy in cases of economic coercion by restricting trade in assets such as semiconductors or other information technology-related equipment should any such manufactured goods constitute a vital resource for a state’s economy. (This argument has been made, in effect, in the runup to the adoption of the EU’s Anti Coercion Instrument, which I shall present below.)

⁴⁷ Partridge, 1971, p. 755.

⁴⁸ Ibid., pp. 767–768.

⁴⁹ Voetelink, 2022a.

⁵⁰ ‘Article XXI. Security Exceptions’, 2012, pp. 600–602; Randazzo, 2014.

⁵¹ Rajput, 2022.

The problems of economic coercion, countermeasures, and resilience against them—just as economic interconnectedness itself—are strongly linked to technological development, as any factor that diminishes the free flow of ideas and technologies in the broadest sense will also slow or possibly deform technological development. If, for example, a ban on the export of advanced semiconductors and their manufacturing equipment by one global power is answered by an export ban on rare earth metals on which the same high technology relies,⁵² the effects on technological development as a whole are easy to predict.

Transformative foundational technologies such as AI and QIT will, by all appearances, be vastly more significant for the future of humanity than oil ever was, although the latter literally fuelled the economic and technological development of the 20th century.⁵³ Their use may last for millennia, possibly even throughout the future of humankind, whatever that future might be. The significance of export restrictions in an industrial society reliant on “old oil,” in its literal sense, may be outweighed many times over in the case of societies basing themselves on the “new oil” of transformative foundational technologies. Competition in developing, deploying, and obtaining such technologies in and of itself is conducive to economic coercion through the institution of export controls, which may then lead to “countermeasures” by similar means.⁵⁴ Importantly, an increasing tit-for-tat of measures such as export bans and export controls seems to not diminish to a possibility of conflict once they are adopted,⁵⁵ a finding that associates grave risks with such measures, which, instead of serving a de-escalation, may even contribute to a further rise in economic and political tensions.

This warrants a future study not only of economic coercion by the restriction of access to such technologies under the present and future rules of international law but also of the structure of such restrictions, something I now set out to do for the remainder of this study.

⁵² See Seyoum, 2017; Wilson, 2018; Yang, Wang, and Whang, 2024.

⁵³ See Jiang et al., 2022; Jones, 2023; Liu et al., 2018; Majot and Yampolskiy, 2015; Makridakis, 2017; Popkova and Gulzat, 2020; Perrier, 2022; West and Allen, 2018.

⁵⁴ Dalton et al., 2019.

⁵⁵ Drezner, 1998; Pape, 1997.

4. Export Controls in the Field AI and QIT

4.1. Raison d'être of Export Controls in the US–PRC Relationship and its Implications in International Law

That AI is a transformative technology, as we have seen, stands beyond any doubt. Its significance for economic and social development is predicted to be near-unparalleled and is, therefore, of strategic importance to all those possessing and desiring to harness this technology. The same may be said, perhaps in narrower terms, of QIT, as it may reshape telecommunications, cryptography, and cryptanalysis in ways that will be nothing short of fundamental.⁵⁶ It is therefore no surprise that AI, especially, has become the latest battleground between major powers, specifically the US and the PRC, as dominance of the field has become equated with global military and economic supremacy.

Technological development in the PRC has given birth to misgivings in the US for a long time, even after Cold War technology transfer rules were relaxed, with two competing lobbies developing in US law-making: Those advocating the so-called “run faster” model of development proposed technological cooperation and trade with the PRC as the guarantee of continued US technological supremacy, while the “control hawks” lobbied for restricting significant dual-use technologies from being exported to or accessed by companies in the PRC.⁵⁷ Eventually, beginning in 2019, on the backdrop of significant advances by Chinese companies such as Huawei, this second lobby prevailed, resulting in the institution of first targeted and then more general export controls by the US against the PRC. In the words of a US Congressional Research Service report, this came about,

... to address concerns about China's attempts to seek global civilian and military leadership in advanced and emerging technologies through coordinated industrial policies. Tightened controls respond to China's ambitious state-led industrial efforts, such as its Made in China 2025 (MIC 2025), that intend to create competitive advantages for China in strategic industries, in part by obtaining technology and expertise from U.S. and foreign firms. MIC 2025 aims to make China a leader

⁵⁶ Shagina, 2023.

⁵⁷ Meijer, 2016.

in emerging technologies important to future commercial, government, and military systems and capabilities.⁵⁸

It is quite unequivocal that the aim of current US export controls directed against the PRC in the field of emerging technologies is to prevent the latter power from effectively competing with the US or obtaining technological advantage over the US, including in purely civilian domains.⁵⁹ It may also be posited that, from the perspective of international law, export controls instituted in the US–PRC relationship (i.e. by both actors) are clearly coercive in nature. They are part of a geo-economic rivalry in which the US aims to prevent the PRC from attaining economic supremacy, and the PRC aims to resist such an attempt. The US strategy, which is the more significant one from the perspective of this study, calls for,⁶⁰ *inter alia*, insulating the PRC from access to advanced technologies.

Following historical precedent set by previous (First) Cold War technology controls,⁶¹ in the implementation of this strategy, the US legislative opted for an export control regime affecting so-called ‘emerging and foundational technologies’ that are ‘essential to the national security of the United States’⁶² (also called ‘critical technologies’), through the Export Control Reform Act of 2018 (ECRA),⁶³ in force as of 2019. Among the technologies slated for newly instituted export controls ‘AI and machine learning’ and ‘quantum information and sensing technology’ are prominently listed,⁶⁴ even if these are still hypothetical or of limited practical applications.⁶⁵ The authority for including various items thought to be linked to these technologies in the export restrictions lists currently lies with the president of the US, who may exercise it after consultations within the administration, making US export restrictions subject to administrative measures for added flexibility, based on a national security rationale.⁶⁶

⁵⁸ Congressional Research Service, 2021, p. 27.

⁵⁹ See Schmidt et al., 2021, pp. 223–240.

⁶⁰ Luttwak, 2012, pp. 266–269.

⁶¹ Jones, 2020a, pp. 33–36, 45.

⁶² ECRA, Section 1758.

⁶³ United States: Export Control Reform Act (ECRA), 2019.

⁶⁴ Jones, 2020a, p. 47.

⁶⁵ *Ibid.*, p. 44.

⁶⁶ *Ibid.*, pp. 55–57. When determining which technologies should be placed on export control lists, pursuant to Section 1758 of the ECRA, the contents of the Wassenaar

Restrictions of trade in these technologies are aimed at kerbing Chinese geopolitical great-power ambitions, including by preventing the PRC from attaining the goals stated in its Made in China 2025 programme, while also sealing the PRC off from access to foundational transformative technologies that may be crucial for its further economic development, beyond the 2025 horizon. The question arises as to what the international public law implications of such a coordinated set of measures should be, justified by securitisation of economic and technological advantage and aimed at hindering the economic development of a competing economy. Traditionally, export controls—notwithstanding those instituted during or related to the use of armed conflict—have been and remain based in international/sanctions law or human rights law, respectively,⁶⁷ which provide the two sets of principles that may justify such measures. Along with these legal bases, the right of individual self-defence of states⁶⁸ could also be considered. However, despite the lack of any form of aggression to defend against but considering the conditions of necessity, imminence, and proportionality,⁶⁹ this right may be ignored in the present case. This is because the stated aim of US measures is not to answer any use or threat of force directed against the US by the PRC but to ensure economic and military containment of the PRC to prevent it from reaching a state of technological and geo-political supremacy. As this objective clearly lies outside the bounds⁷⁰ of self-defence in international law, I shall not examine this possibility separately.

As we have seen, when discussing the international legality of economic coercion against the PRC, sanctions law as a fundament for such actions is problematic, as it would in theory require acquiescence by the UN, so as not to constitute potentially prohibited economic coercion, an

Arrangement's proscription lists are regularly considered and updated. Bureau of Industry and Security, 2022; The Wassenaar Arrangement Secretariat, 2023.

⁶⁷ Voetelink, 2022a, pp. 84–90.

⁶⁸ See Alexandrov, 1996, pp. 121–149.

⁶⁹ Akande and Liefänder, 2013.

⁷⁰ Anticipatory self-defence, or defence from the threat of the use of force might come to mind, despite the distinct lack of imminent aggression directed against the party defending itself by economic coercion. See Alexandrov, 1996, p. 149; Azubuike, 2011; Weightman, 1951. Some authors mention the national security decisions reached without the use of force or that were at least threatened as being possibly compatible with the objective of international self-defence. See Schachter, 1989. However, these ad-hoc measures are not compatible with the current state of international (UN) law.

authorisation that is clearly absent. Still, it is sanctions law that forms—at least at the declarative level—the foundation of current US-imposed export restrictions targeted at the PRC, with the various measures taken being based on supposed technology theft being committed against US interests, the decreasing lead of the US economy over that of the PRC, and increasing foreign trade deficits.⁷¹ Human rights law is sometimes also cited as a basis for some measures (especially directed against mass surveillance conducted by the PRC and the repression practiced against the Uyghur community).⁷²

When it comes to justifying export controls, one more problem must be addressed in international law, namely whether they are compatible with the General Agreement on Tariffs and Trade (GATT) signatory and World Trade Organisation (WTO) member status of both the initiating and target jurisdictions. This is done based primarily on the supposed national security exemption apparently allowed for in the GATT.⁷³ Such a position, as we have seen, is vulnerable as, under the GATT, national security seems not to constitute an autonomous exemption for instituting trade restrictions outside some manner of conflict. It is perhaps also worth to spare a moment and consider the justification of export restrictions instituted by the PRC against the US (as well as other states), adopted quasi-simultaneously with US measures. In this latter case, the measures might be considered retaliatory, bringing them closer to the categories of self-defence and “countermeasure” rationales.⁷⁴ This creates the appearance that, at least considering the ARSIWA rules outlined above, the Chinese export controls may find justification on the doctrine of legitimate countermeasures, while the US measures are outside any treaty-based regime and are, in fact, unilateral restrictions of trade not authorised by either the UN or WTO.

4.2. Meagre Substance of Export Controls in the Field of AI and QIT

The Bureau of Industry and Security (BIS) is the US federal agency overseeing the export control regime established under ECRA. This entity manages the export control lists for various transformative (foundational) technologies, which are identified by the president of the US after administrative consultations as being subject to such restrictions (the so-called Section 1758 list, as a reference to the ECRA provision permitting the

⁷¹ Hufbauer and Jung, 2020.

⁷² Congressional Research Service, 2021, p. 29.

⁷³ ‘The United States announces’, 2023.

⁷⁴ Rajput, 2022.

designation for control of such technologies).⁷⁵ These provisions use several approaches to instituting export controls, depending on the technology subject to control (classification-based controls) and the entity it is destined for (end-user based controls).⁷⁶

The following are technologies targeted for (mostly future) export controls in the field of AI:

- (i) Neural networks and deep learning (e.g., brain modelling, time series prediction, classification);
- (ii) Evolution and genetic computation (e.g., genetic algorithms, genetic programming);
- (iii) Reinforcement learning;
- (iv) Computer vision (e.g., object recognition, image understanding);
- (v) Expert systems (e.g., decision support systems, teaching systems);
- (vi) Speech and audio processing (e.g., speech recognition and production);
- (vii) Natural language processing (e.g., machine translation);
- (viii) Planning (e.g., scheduling, game playing);
- (ix) Audio and video manipulation technologies (e.g., voice cloning, deepfakes);
- (x) AI cloud technologies; or
- (xi) AI chipsets.⁷⁷

For QIT, the BIS envisages necessary restrictions regarding the following technologies: ‘(i) Quantum computing; (ii) Quantum encryption; or (iii) Quantum sensing’.⁷⁸

The list of such technologies is largely in line with those considered as “critical and emerging technologies” by the US administration, which enumerates the following technologies:

Artificial Intelligence (AI)

- Machine learning

⁷⁵ Tongele, 2022a, 2022b.

⁷⁶ Whenever applying export controls, several methods of regulation are possible. Such controls may be instituted depending on whom they target (“end-user” controls), what purpose of use they prohibit (“end-use” controls), what items they refer to (“classification” controls), or where the controlled item is headed (“destination” controls). Voetelink, 2022a, p. 72.

⁷⁷ Bureau of Industry and Security, Commerce, 2018.

⁷⁸ Ibid.

- Deep learning
- Reinforcement learning
- Sensory perception and recognition
- AI assurance and assessment techniques
- Foundation models
- Generative AI systems, multimodal and large language models
- Synthetic data approaches for training, tuning, and testing
- Planning, reasoning, and decision making
- Technologies for improving AI safety, trust, security, and responsible use Quantum Information and Enabling Technologies
- Quantum computing
- Materials, isotopes, and fabrication techniques for quantum devices
- Quantum sensing
- Quantum communications and networking
- Supporting systems.⁷⁹

As can be seen from the list of technologies proposed as subject to future export restrictions in 2018, the intended reach of the measures was exceedingly wide. The enumeration includes many, if not the most, current and predicted applications of the given technologies in imprecise general, non-technological terms. It apparently envisages a mostly end-user-based or a very wide classification-based regime, where entire technologies, especially those destined to be used by certain entities linked to the PRC, would have been entered into the BIS proscription lists.

However, the reach of the regulators seems to have largely exceeded their grasp. In effect, until now, all⁸⁰ measures aimed at limiting technological exports regarding AI have been quite targeted ones, with the BIS entity list—the list of end-users prohibited from obtaining technologies—being updated several times, and only semiconductor and semiconductor-manufacturing equipment export restrictions being imposed. In fact, the expansion of blanket measures against PRC-bound AI-related technology exports, adopted on 7 October 2022 and in effect from 16

⁷⁹ National Science and Technology Council, 2024, pp. 4, 6. See also ‘National Strategy for Critical and Emerging Technologies’, 2020.

⁸⁰ For the full list of BIS export controls on AI and QIT, see Bureau of Industry and Security, 2024b.

November 2023,⁸¹ which forms the material quasi-entirety of such measures only affects four distinct fields:⁸²

1. high-performance (more precisely high processing power) microchips, including ones which do not exceed the thresholds set, but contain technical solutions intentionally ‘dumbed down’ in order to comply with export controls, but which contain cutting-edge technology (so-called grey-zone chips);⁸³
2. expanding licensing agreement requirements for exports to several countries not directly targeted, based on the risk of transfer of prohibited technologies to the PRC (a destination-based restriction);⁸⁴
3. the restriction for the exports of semiconductor manufacturing equipment, and related goods and services (including maintenance) to the PRC, Macau, and the countries for which such restrictions have been expanded as per point 2 above;⁸⁵
4. an expansion of the entity-list (blacklist) of potential end-users.⁸⁶

The dual-use technology proscription lists drafted under the Wassenaar Arrangement, which mirror the US BIS restrictions on technology exports, show that most AI technologies that are currently restricted under this latter regime also comprise computer hardware such as integrated circuits used for the construction of neural networks, neural-network-based computers, high-performance semiconductors (computer chips), and production equipment for such semiconductors, as well as software for operating such systems (as software is usually not treated as a separate item).⁸⁷ The Wassenaar Arrangement comprises all EU member states, apart from Cyprus, and is also the basis for the rules of the EU Dual-

⁸¹ Bureau of Industry and Security, 2023a.

⁸² Benson, 2023.

⁸³ Bureau of Industry and Security, 2023d.

⁸⁴ Bureau of Industry and Security, 2024c.

⁸⁵ Bureau of Industry and Security, 2023b.

⁸⁶ Bureau of Industry and Security, 2023c. For the current full entity-list, see *Supplement No. 4 to Part 744, Title 15, Entity List*, 2024.

⁸⁷ Brockmann, 2022, pp. 196–197. The List of Dual-Use Goods and Technologies and Munitions List compiled under the Wassenaar Arrangement does not reference AI at all. The Wassenaar Arrangement Secretariat, 2023

Use Regulation,⁸⁸ so that the approach to export restrictions pioneered by the US has been effectively implemented by these states as well.

The review process of AI technologies to be appended to the restriction lists has not elicited any new emerging AI technologies that should be added, with the technological chokepoints of microprocessors, processor assemblies, and related manufacturing equipment mainly being targeted, even by the most recent measures, according to specialist recommendations.⁸⁹ As AI software and semiconductors are a sub-optimal target for export restrictions, mostly the manufacturing equipment for such advanced semiconductors is likely to constitute the future target of export controls.⁹⁰ Future proposed controls would extend current restrictions—which, as we have seen, now mainly target semiconductors—to entire AI systems as well as scientific collaborations on AI.⁹¹

In the field of QIT, a similar approach to end-use and classification-based controls as in the case of AI has been adopted: Both the BIS export restrictions and the Wassenaar Arrangement proscriptions lists⁹² contain controls for equipment that may be used in quantum cryptography,⁹³ as well as algorithms that permit encryption that is immune to quantum-technology based attacks (post-quantum encryption), without specifying further or specifying wider technologies as being restricted. Interestingly, and as a quite recent development, end-user controls have been strengthened, with numerous PRC entities involved in quantum technology development being blacklisted.⁹⁴ There are voices calling for blanket restrictions on quantum sensing technology (and perhaps even wider restrictions on possible future applications). However based on the most recent developments—and due to

⁸⁸ *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*, 2021. See also Vandenberghe, 2021.

⁸⁹ Eitel, 2023.

⁹⁰ See Flynn, 2020.

⁹¹ *Bipartisan Coalition Introduces Monumental Bill Giving Admin Authority to Export Control Advanced AI Systems*, 2024; *Enhancing National Frameworks for Overseas Restriction of Critical Exports Bill*, 2024.

⁹² The Wassenaar Arrangement Secretariat, 2023; e.g. category 5.A.2.c,

⁹³ This is defined as ‘A family of techniques for the establishment of a shared key for “cryptography” by measuring the quantum-mechanical properties of a physical system (including those physical properties explicitly governed by quantum optics, quantum field theory, or quantum electrodynamics).’ The Wassenaar Arrangement Secretariat, 2023, p. 231.

⁹⁴ Bureau of Industry and Security, 2024a.

the remote nature of practical implementations and the as-of-yet unknown and largely unpredictable characteristics of other quantum technologies—restricting these is considered futile for the time being.⁹⁵ Component-level restrictions are, for the time being, the norm in the field of QIT.⁹⁶

Both the approaches to AI and QIT show that the US is currently implementing the ‘small yard with a high fence’ policy.⁹⁷ This approach would subject key technologies and especially components to export controls while leaving most other technologies untouched. Very recent developments now cast doubt on how small the yard really is, as the substance of especially AI-related export restrictions has ballooned, and further enhancements are in the works.⁹⁸

4.3. US Export Controls and the EU

US export control law, including ECRA (and the Export Control Act, which it reformed) is constructed in a way so as to regularly apply to entities (i.e. legal and natural persons or groups of such persons) found outside the territorial jurisdiction of the US. This is the characteristic of extraterritorial application.⁹⁹ Extraterritorial application draws third parties into the US export control regime as stakeholders and may be prejudicial to the interests of such stakeholders. This is especially true for rules applying to “foreign-made” or “foreign-produced” assets, which gained great significance since the field of technology export controls was vastly expanded after the adoption of ECRA; such restrictions are attached to each US-made part (component) of assets or assets manufactured by the use of US-made equipment (so-called “foreign direct product” restrictions).¹⁰⁰ Extraterritorial application of export restriction may clearly impact EU businesses. The EU has, for this reason, historically opposed extraterritorial application of, *inter alia*, export restrictions and sanctions, based on considerations of international law, even if this stance has softened over time.¹⁰¹ An example of such opposition is the so-called Blocking Statute, to which I shall return to below. Such extraterritorial effects (and more

⁹⁵ Perrier, 2022; Parker, 2024.

⁹⁶ Parker, 2023, p. 16.

⁹⁷ *Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution*, 2023.

⁹⁸ Cavanagh, 2023; He, 2024.

⁹⁹ Voetelink, 2022b.

¹⁰⁰ Voetelink, 2023.

¹⁰¹ Bismuth, 2023.

specifically those of post-ECRA measures by the US) have recently been raised again as a cause for concern by the EU,¹⁰² but they have not yet been effectively acted upon, even if some tools are already available to the EU for counteracting them.

The question arises regarding whether incidental extraterritorial effects of export controls instituted by the US against the PRC, which in turn are prejudicial to EU trade, may be evaluated as forms of economic coercion, which would be contrary to international law and, if its effects are sufficiently grave, may be converted. This is especially important since there is economic competition¹⁰³ between the US and EU in the field of high technology; therefore, benign intentions in imposing extraterritorial export controls by the US with effects on EU exports should not be considered a forgone conclusion, even if they are presumed. An even more important question is whether the EU can resist economic coercion from actors such as the PRC. The two questions are in fact intertwined when applicable norms are concerned.

In the instrument titled The European Economic Security Strategy, adopted in 2023, the European Commission stated that the EU Economic Security Strategy's priority is to protect the bloc

... from commonly identified economic security risks, by better deploying the tools we already have in place, such as on trade defence, foreign subsidies, 5G/6G security, Foreign Direct Investment screening and export controls, as well as the new instrument to counter economic coercion.¹⁰⁴

The document also identifies 'weaponisation of economic dependencies or economic coercion' as risks identified by the European Commission and High Representative (albeit mostly regarding non-allied economies).

Resisting economic coercion or resilience in the face of such coercion is then clearly significant in enhancing technological sovereignty and strategic autonomy. In the case of the EU, this necessity has not just been recognised but also acted upon by the creation of the European Anti-

¹⁰² European Commission, 2024.

¹⁰³ OECD, 2023, pp. 66–68.

¹⁰⁴ European Commission, 2023.

Coercion Instrument (ACI),¹⁰⁵ which entered into force on 27 December 2023. The ACI at Recital (5) explicitly references the prohibition of economic coercion, as contained in the UN Charter and the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States as well as the ARSIWA, stating that ‘[t]hose rules are binding in the relations between third countries, on the one part, and the Union and its Member States, on the other’. Recital (15) is even clearer on the illegal nature of coercion, while at the same time, it allows for setting particular intensity thresholds for action to be deemed as coercive.¹⁰⁶ Therefore, from the perspective of the EU, economic coercion is considered prohibited, at least beyond certain thresholds.

The ACI at Recital (6) states that ‘[t]he modern interconnected world economy increases the risk of economic coercion, as it provides countries with enhanced means for such coercion, including hybrid mean’. Thus, the EU not only recognises some form of prohibition of economic coercion but also apparently posits its equivalence with the use of force. It refers to “hybrid means” and almost overtly cites the second sentence of the text in

¹⁰⁵ *Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the protection of the Union and its Member States from economic coercion by third countries*, 2023.

¹⁰⁶ Recital (15) reads as follows:

Coercion is prohibited and therefore a wrongful act under international law when a country deploys measures such as trade or investment restrictions in order to obtain from another country an action or inaction which that country is not obliged to perform under international law and which falls within its sovereignty, and when the coercion reaches a certain qualitative or quantitative threshold, depending both on the objectives pursued and the means used. The Commission and the Council should take into account qualitative and quantitative criteria that help in determining whether the third country interferes in the legitimate sovereign choices of the Union or a Member State and whether its action constitutes economic coercion which requires a Union response. Among those criteria, there should be elements that characterise, both qualitatively and quantitatively, notably the form, the effects and the aim of the measures which the third country is deploying. Applying those criteria would ensure that only economic coercion with a sufficiently serious impact or, where the economic coercion consists in a threat, that only a credible threat, falls under this Regulation. In addition, the Commission and the Council should examine closely whether the third country pursues a legitimate cause, because its objective is to uphold a concern that is internationally recognised, such as, among other things, the maintenance of international peace and security, the protection of human rights, the protection of the environment, or the fight against climate change.

See also Article 4 of the ACI.

the Preamble of the Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States, which prohibits the use of force in the form of interference in the affairs of another state. Finally, Recital (8) of the ACI firmly asserts that the ACI is a defensive instrument, meant to deter and counteract economic coercion.

While the ACI makes no mention of economic coercion by restricting access to certain vital technologies *per se*, the European Economic Security Strategy refers to this problem by name rather often and in quite broad terms, stating that regarding ‘key technologies’, ‘[p]rofound technological shifts are adding to the intensity of this competition and making the economic and security challenges more complex’. Most clearly the strategy states the

... need to rely on trade and on the Single Market to spur competition and ensure that we have access to the raw materials, technologies, and other inputs which are crucial for boosting our competitiveness, resilience and for sustaining current and future employment and growth.

It should be mentioned that, conversely, to ensure access, the document is also concerned with “technology leakage risks” in the fields of AI and QIT. These desiderates make for a complicated balancing act as the EU aims to prevent withholding of crucial technologies from it, while at the same time promoting their withholding from its competitors. This latter action itself a possible form of economic coercion, where access to vital technologies is restricted in return for political or economic concessions.

Therefore, while the ACI should be viewed primarily from the perspective of a desire to ensure the security of supply in the EU,¹⁰⁷ we should not ignore that some “response measures” taken under Article 8 and Annex I the ACI, such as export and trade restrictions undertaken by the EU, may in and of themselves be perceived as economic coercion be the “target” countries.

While the language of the ACI sometimes references the notion of “countermeasures” relevant under the ARSIWA, in both Article 8 and Annex I, it introduces the competing notion of “response measures.” This leaves the door open to applying measures other than those that are legal under the ARSIWA (this is quite apparent from the structuring of items 1–4

¹⁰⁷ See Theodosopoulos, 2020.

in Annex I to the ACI, where the classical meaning of “countermeasures” under the ARSIWA is only truly present in item 4). It seems that while the EU is clearly concerned about being cut off from vital technologies and other resources, it has few qualms about imposing export restrictions of its own, provided there is a sufficient, duly ascertained reason to do so and proportionality is respected. This EU approach is open to criticism, as it is somewhat reminiscent of the US position adopted during the 1973–1974 oil embargo and seems hypocritical. The ACI permits the bloc to be ‘running with the hare and hunting with the hounds’¹⁰⁸ at the same time.¹⁰⁹

Another problem posed by economic coercion, which may affect European interests, involves the collateral effects of coercion by other Western powers, specifically the US, directed at the latter power’s geopolitical opponents,¹¹⁰ especially in the case of the PRC, when such measures are instituted with extraterritorial effects. The ACI is silent on the issue, which falls within the scope of the EU Blocking Statute.¹¹¹ However the Annex of the Blocking Statute has not been updated, with the last version of the norm dating to 2018, thus predating the most prejudicious extraterritorial sanctions implemented by the US against the PRC, with effects on the EU.

5. Conclusions

In this study, I examined export controls from the perspectives of international law and foundational, transformative technologies such as AI and QIT. I found that these technologies, much like some important commodities during the 20th century, are likely to form the basis for continued economic development and may therefore be considered vital.

Withholding access to such technologies by way of export controls may, for this very reason, be considered a form of economic coercion. The same can be said of forcing export controls, through extraterritorial application, on third parties to the conflict that prompted them. Both international law and international custom seem unclear on whether

¹⁰⁸ Olsen and Schmucker, 2024.

¹⁰⁹ For some examples, see Packroff, 2023.

¹¹⁰ Hackenbroich et al., 2020, p. 4; Hackenbroich, Medunic, and Zerka, 2022, p. 9.

¹¹¹ *Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom*, 1996; Szép, 2024.

economic coercion is entirely, or at least partly, prohibited and, if yes, how thresholds for such a prohibition may be determined. The international law foundations for export controls unilaterally instituted in the past few years by the US against the PRC are somewhat unclear, even if such controls were then transferred into multilateral non-binding instruments such as the Wassenaar Arrangement, with effects on the EU. This is because neither the UN instruments nor the GATT/WTO infrastructure offer clear grounds for instituting such controls based on a pure national security rationale, particularly in the absence of an armed conflict.

It is perhaps evident from the above that export controls instituted regarding AI and QIT are not going to diminish anytime soon. If anything, the “small yard, high fence” approach seems, to be undermined by proposals for wider restrictions affecting entire technologies (an option seemingly supported by the US BIS list of foundational technologies) and not component-based restrictions, which may be the most likely of near-term outcomes, especially if the PRC manages to sidestep restrictions by enhancing domestic manufacturing capabilities.

In this context, the EU—more a bystander than an actor—is only now re-evaluating measures that should be taken to defend its strategic interests from (both) its competitors. I believe that it is necessary for the EU legislative to address the concerns posed by foreign export controls that, when applied extraterritorially, may have unintended negative effects on European strategic autonomy and technological sovereignty, by updating the Blocking Statute to discourage export controls by competing powers in the way envisaged but not yet acted on by the European Commission. A proposed amendment of this instrument,¹¹² perhaps by way of a regulation, has already been formulated but was apparently shelved during the incipient phase of its development. Some proposed measures it included read as follows:

[To] deter and counteract extra-territorial sanctions ... the proposed regulation could provide the Commission with powers to apply deterrent and counteracting measures against third countries unlawfully applying extra-territorial sanctions, or persons benefiting from their imposition; this could take the form of commercial or other measures in the field of judicial cooperation in civil matters, as well as exclusion/restrictions

¹¹² European Commission, 2021.

from access to the EU capital markets, EU public tenders, or even visa limitations for individuals. The Commission would exercise those powers through implementing acts. Further, the proposed regulation could envisage the award of financial or other types of support to EU operators willing to engage in trade that is prohibited by such extra-territorial sanctions of third countries but not prohibited by Union law.

[To] streamline the application of the Blocking Statute as well as reduce the administrative burden ... the proposed regulation could simplify compliance, as appropriate, through: streamlined processing for authorisation requests pursuant to Article 5, second paragraph, of the Blocking Statute, including a review of the information required to process the authorisation request; clarifications of the prohibition to comply with unlawful extra-territorial sanctions of third countries (Article 5, first paragraph of the Regulation), including a possible specific focus on strategic sectors.¹¹³

Such a proposal is more relevant than ever and should be acted upon in European interest.

The establishment of a fair, rules- (not just interests-) based global export regime could also be achieved by engaging in international cooperation to ensure the creation of a clear, unified, and legally sound basis for their imposition against the PRC to ensure global security. The Wassenaar Arrangement (while non-binding, but largely adhered to) may provide a template for such a multilateral regime entered into by Western powers, with the added value of allaying concerns raised by unilateral export restrictions based on economic self-interest and not collective security. Such a multilateral practice, while possibly viewed as a form of economic containment, would ensure that restrictions remain actionable and reasonable, without recourse to unilateralism on behalf of either the US or EU. This basis should include a clarification of the notion of economic coercion, as a set of thresholds, to avoid any appearance of a double standard.

¹¹³ Ibid.

Bibliography

- [1] Akande, D., Liefländer, T. (2013) 'Clarifying Necessity, Imminence, and Proportionality in the Law of Self-Defense', *The American Journal of International Law*, 107(3), pp. 563–570; <https://doi.org/10.5305/amerjintelaw.107.3.0563>.
- [2] Alexandrov, S. A. (1996) *Self-Defense Against the Use of Force in International Law*. The Hague, London, Boston: Kluwer Law International.
- [3] Aubin, Y., Idiart, A. (2016) *Export Control Law and Regulations Handbook, Third Edition*. Wolters Kluwer.
- [4] Azubuike, E. C. (2011) 'Probing the Scope of Self Defense in International Law', *Annual Survey of International and Comparative Law*, 17(1), pp. 129–183.
- [5] Benson, E. (2023) *Updated October 7 Semiconductor Export Controls*. Center for Strategic and International Studies (CSIS) [Online]. Available at: <https://www.csis.org/analysis/updated-october-7-semiconductor-export-controls> (Accessed: 03 April 2024).
- [6] Bismuth, R. (2023) 'Chapter 7: The European Union experience of extraterritoriality: when a (willing) victim has become a (soft) perpetrator', Cheltenham, UK: Edward Elgar Publishing, pp. 118–132; <https://doi.org/10.4337/9781800885592.00015>.
- [7] Brockmann, K. (2022) 'Applying Export Controls to AI: Current Coverage and Potential Future Controls', in Reinhold, T., Schörnig, N. (eds.) *Armament, Arms Control and Artificial Intelligence: The Janus-faced Nature of Machine Learning in the Military Realm*. Cham: Springer International Publishing, pp. 193–209; https://doi.org/10.1007/978-3-031-11043-6_14.

-
- [8] Carter, B. E. (2009) 'Economic Coercion', *Max Planck Encyclopedias of International Law*. Oxford: Oxford University Press (Oxford Public International Law) [Online]. Available at: <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1518> (Accessed: 07 April 2024).
- [9] Casarini, N. (2013) 'The Securitisation of EU-Asia Relations in the Post-Cold War Era', in Christiansen, T., Kirchner, E., Murray, P. (eds.) *The Palgrave Handbook of EU-Asia Relations*. London: Palgrave Macmillan UK, pp. 181–197; https://doi.org/10.1057/9780230378704_12.
- [10] Cavanagh, C. (2023) 'U.S. Economic Restrictions on China: Small Yard, High Fence?', *Georgetown Security Studies Review* [Preprint] [Online]. Available at: <https://georgetownsecuritystudiesreview.org/2023/12/26/u-s-economic-restrictions-on-china-small-yard-high-fence/> (Accessed: 07 April 2024).
- [11] Chapman, B. (2013) *Export Controls. A Contemporary History*. Lanham, New York, Oxford: University Press of America, Inc.
- [12] Dalton, M., Hicks, K.H., Donahoe, M., Sheppard, L., Friend, A.H., Matlaga, M., Federici, J., Conklin, M., Kiernan, J. (2019) *Political and Economic Coercion by Other Means. Part II: Adapting to Compete in the Grey Zone*. Center for Strategic and International Studies (CSIS), pp. 11–17 [Online]. Available at: <http://www.jstor.org/stable/resrep22608.7> (Accessed: 23 July 2024).
- [13] Drezner, D. W. (1998) 'Conflict Expectations and the Paradox of Economic Coercion', *International Studies Quarterly*, 42(4), pp. 709–731; <https://doi.org/10.1111/0020-8833.00103>.
- [14] Drezner, D. W. (2003) 'The Hidden Hand of Economic Coercion', *International Organization*, 57(3), pp. 643–659.

-
- [15] Eitel, M. (2023) 'The US Goes "All In" On China Chip Controls', *Center for European Policy Analysis* [Online]. Available at: <https://cepa.org/article/the-us-goes-all-in-on-china-chip-controls/> (Accessed: 15 March 2024).
- [16] Farer, T. J. (1985) 'Political and Economic Coercion in Contemporary International Law', *The American Journal of International Law*, 79(2), pp. 405–413; <https://doi.org/10.2307/2201710>.
- [17] Farrell, H., Newman, A.L. (2019) 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', *International Security*, 44(1), pp. 42–79; https://doi.org/10.1162/isec_a_00351.
- [18] Floyd, R. (2007) 'Towards a consequentialist evaluation of security: bringing together the Copenhagen and the Welsh Schools of security studies', *Review of International Studies*, 33(2), pp. 327–350; <https://doi.org/10.1017/S026021050700753X>.
- [19] Floyd, R. (2019) 'Evidence of securitisation in the economic sector of security in Europe? Russia's economic blackmail of Ukraine and the EU's conditional bailout of Cyprus', *European Security*, 28(2), pp. 173–192; <https://doi.org/10.1080/09662839.2019.1604509>.
- [20] Flynn, C. (2020) 'Recommendations on Export Controls for Artificial Intelligence', *CSET Issue Brief* [Preprint] [Online]. Available at: <https://pdfs.semanticscholar.org/cd59/5d03186fde7c8d5051809513cc0bae19b96c.pdf> (Accessed: 14 February 2024).
- [21] Garnsey, E. (1998) 'The Genesis of the High Technology Milieu: A Study in Complexity', *International Journal of Urban and Regional Research*, 22(3), pp. 361–377; <https://doi.org/10.1111/1468-2427.00146>.
- [22] Goertzel, B., Goertzel, T.; Goertzel, Z. (2017) 'The global brain and the emerging economy of abundance: Mutualism, open collaboration, exchange networks and the automated commons', *Technological Forecasting and Social Change*, 114, pp. 65–73; <https://doi.org/10.1016/j.techfore.2016.03.022>.

- [23] Grossman, G. M., Helpman, E. (1995) ‘Chapter 25 Technology and trade’, in *Handbook of International Economics*. Elsevier, pp. 1279–1337; [https://doi.org/10.1016/S1573-4404\(05\)80005-X](https://doi.org/10.1016/S1573-4404(05)80005-X).
- [24] Gueorguiev, D., McDowell, D., Steinberg, D.A. (2020) ‘The Impact of Economic Coercion on Public Opinion: The Case of US–China Currency Relations’, *Journal of Conflict Resolution*, 64(9), pp. 1555–1583; <https://doi.org/10.1177/0022002720912323>.
- [25] Hackenbroich, J., Medunic, F., Zerka, P. (2022) *Tough Trade: The Hidden Costs of Economic Coercion*. European Council on Foreign Relations [Online]. Available at: <http://www.jstor.org/stable/resrep39679> (Accessed: 14 July 2024).
- [26] Hackenbroich, J., Oertel, J., Sandner, P., Zerka, P. (2020) *Defending Europe’s Economic Sovereignty: New Ways to Resist Economic Coercion*. European Council on Foreign Relations [Online]. Available at: <http://www.jstor.org/stable/resrep26434> (Accessed: 15 April 2024).
- [27] He, J. (2024) ‘WorldFrom “Small Yard, High Fence” to “Large Yard, High Fence”’, *EUreporter* [Preprint] [Online]. Available at: <https://www.eureporter.co/world/2024/06/20/from-small-yard-high-fence-to-large-yard-high-fence/> (Accessed: 22 June 2024).
- [28] Hryniv, O. (2022) ‘Export Controls and Securitization of Economic Policy: Comparative Analysis of the Practice of the United States, the European Union, China, and Russia’, *Journal of World Trade*, 56(4), pp. 633–656; <https://doi.org/10.54648/trad2022026>.
- [29] Hufbauer, G. C., Jung, E. (2020) ‘What’s new in economic sanctions?’, *European Economic Review*, 130, p. 103572; <https://doi.org/10.1016/j.euroecorev.2020.103572>.
- [30] Liu, J., Kong, X., Xia, F., Bai, X., Wang, L., Qing, Q., Lee, I. (2018) ‘Artificial Intelligence in the 21st Century’, *IEEE Access*, 6, pp. 34403–34421; <https://doi.org/10.1109/ACCESS.2018.2819688>.

-
- [31] Jiang, Y., Li, X., Luo, H., Yin, S., Kaynak, O. (2022) ‘Quo vadis artificial intelligence?’, *Discover Artificial Intelligence*, 2(1); <https://doi.org/10.1007/s44163-022-00022-8>.
- [32] Jones, E. (2023) ‘Digital disruption: artificial intelligence and international trade policy’, *Oxford Review of Economic Policy*, 39(1), pp. 70–84; <https://doi.org/10.1093/oxrep/grac049>.
- [33] Jones, S. A. (2020a) ‘Disrupting Export Controls: “Emerging and Foundational Technologies” and Next Generation Controls’, *Strategic Trade Review*, 6(9), pp. 31–52.
- [34] Jones, S. A. (2020b) ‘Trading Emerging Technologies: Export Controls Meet Reality’, *Security and Human Rights*, 31, pp. 47–59.
- [35] Köstner, D., Nonn, M. (2023) ‘The 2020 Chinese export control law: a new compliance nightmare on the foreign trade law horizon?’, *China-EU Law Journal*, 8(3), pp. 81–95; <https://doi.org/10.1007/s12689-021-00092-4>.
- [36] Lentzos, F., Silver, P. (2012) ‘Innovation, Dual Use and Security’.
- [37] Lillich, R. B. (1975) ‘Economic Coercion and the International Legal Order’, *International Affairs (Royal Institute of International Affairs 1944-)*, 51(3), pp. 358–371; <https://doi.org/10.2307/2616620>.
- [38] Luttwak, E. N. (2012) *The Rise of China v. the Logic of Strategy*. Cambridge (Massachusetts), London: The Belknap Press of Harvard University Press.
- [39] Majot, A., Yampolskiy, R. (2015) ‘Global catastrophic risk and security implications of quantum computers’, *Confronting Future Catastrophic Threats To Humanity*, 72, pp. 17–26; <https://doi.org/10.1016/j.futures.2015.02.006>.
- [40] Makridakis, S. (2017) ‘The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms’, *Futures*, 90, pp. 46–60; <https://doi.org/10.1016/j.futures.2017.03.006>.

- [41] Markolf, S. A., Chester, M. V., Eisenberg, D. A., Iwaniec, D. M., Davidson, C. I., Zimmerman, R., Miller, T. R., Ruddell, B. L., Chang, H. (2018) 'Interdependent Infrastructure as Linked Social, Ecological, and Technological Systems (SETs) to Address Lock-in and Enhance Resilience', *Earth's Future*, 6(12), pp. 1638–1659; <https://doi.org/10.1029/2018EF000926>.
- [42] Mawdsley, J. (2013) *A European Agenda for Security Technology: From Innovation Policy to Export Controls*. Flemish Peace institute [Online]. Available at: https://vlaamsvredesinstituut.eu/wp-content/uploads/2013/02/a_european_agenda_for_security_technology_report_0-1.pdf (Accessed: 07 February 2024).
- [43] Meijer, H. (2016) 'Supercomputers, Telecommunications Equipment, and China's Military Modernization', in Meijer, H. (ed.) *Trading with the Enemy: The Making of US Export Control Policy toward the People's Republic of China*. Oxford University Press, pp. 165–197; <https://doi.org/10.1093/acprof:oso/9780190277697.003.0006>.
- [44] Mola, L. (2023) 'The securitisation of international economic law and "global security": an analysis of the EU law approach through the prism of the Common Commercial Policy', *Cambridge International Law Journal*, 12(1), pp. 105–128 [Online]. Available at: <https://doi.org/10.4337/cilj.2023.01.07>.
- [45] Nanopoulos, E. (2023) 'The Antinomies of "Peaceful" Economic Sanctions', in *Yale Journal of International Law. Symposium: Third World Approaches to International Law (TWAIL) & Economic Sanctions* [Online]. Available at: https://www.yjil.yale.edu/the_antimonies_of_peaceful_economic_sanctions/ (Accessed: 03 February 2024).
- [46] Olsen, K. B., Schmucker, C. (2024) 'The EU's New Anti-Coercion Instrument Will Be a Success if It Isn't Used', *Internationale Politik Quarterly* [Preprint] [Online]. Available at: <https://ip-quarterly.com/en/eus-new-anti-coercion-instrument-will-be-success-if-it-isnt-used> (Accessed: 17 April 2024).

-
- [47] Olson, R. S. (1979) 'Economic Coercion in World Politics: With a Focus on North-South Relations', *World Politics*, 31(4), pp. 471–494 [Online]. Available at: <https://doi.org/10.2307/2009906>.
- [48] Packroff, J. (2023) 'EU "united" against economic blackmail – despite facing claims of hypocrisy', *Euroactiv* [Preprint] [Online]. Available at: <https://www.euractiv.com/section/economy-jobs/news/eu-united-against-economic-blackmail-despite-facing-claims-of-hypocrisy/> (Accessed: 17 December 2023).
- [49] Pape, R. A. (1997) 'Why Economic Sanctions Do Not Work', *International Security*, 22(2), pp. 90–136 [Online]. Available at: <https://doi.org/10.2307/2539368>.
- [50] Parker, E. (2023) 'Promoting Strong International Collaboration in Quantum Technology Research and Development'. RAND Corporation [Online]. Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PEA1800/PEA1874-1/RAND_PEA1874-1.pdf (Accessed: 11 April 2024).
- [51] Parker, E. (2024) 'The Chinese Industrial Base and Military Development of Quantum Technology. Addendum to testimony before the U.S.-China Economic and Security Review Commission'. RAND Corporation [Online]. Available at: https://www.rand.org/content/dam/rand/pubs/testimonies/CTA3100/CTA3189-2/RAND_CTA3189-2.pdf (Accessed: 11 April 2024).
- [52] Partridge, C. E. Jr. (1971) 'Political and Economic Coercion: Within the Ambit of Article 52 of the Vienna Convention on the Law of Treaties?', *The International Lawyer*, 5(4), pp. 755–769.
- [53] Perrier, E. (2022) 'The Quantum Governance Stack: Models of Governance for Quantum Information Technologies', *Digital Society*, 1(3), p. 22 [Online]. Available at: <https://doi.org/10.1007/s44206-022-00019-x>.

-
- [54] Piekos, W. (2023) *Investigating China's economic coercion: The reach and role of Chinese corporate entities*. Atlantic Council [Online]. Available at: <https://www.atlanticcouncil.org/wp-content/uploads/2023/11/Role-and-Reach-of-Chinese-Econ-Statecraft-1.pdf> (Accessed: 19 January 2024).
- [55] Popkova, E. G., Gulzat, K. (2020) 'Technological Revolution in the 21st Century: Digital Society vs. Artificial Intelligence', in Popkova, E.G., Sergi, B.S. (eds.) *The 21st Century from the Positions of Modern Science: Intellectual, Digital and Innovative Aspects*. Cham: Springer International Publishing, pp. 339–345.
- [56] Rajput, T. (2022) 'Restricting International Trade through Export Control Laws: National Security in Perspective', Leiden, The Netherlands: Brill | Nijhoff, pp. 603–645 [Online]. Available at: https://doi.org/10.1163/9789004518681_022.
- [57] Randazzo, V. (2014) *Article 346 and the qualified application of EU law to defence*. European Union Institute for Security Studies [Online]. Available at: https://www.files.ethz.ch/isn/182625/Brief_22_Article_346.pdf (Accessed: 11 April 2024).
- [58] Rath, J., Ischi, M., Perkins, D. (2014) 'Evolution of Different Dual-use Concepts in International and National Law and Its Implications on Research Ethics and Governance', *Science and Engineering Ethics*, 20(3), pp. 769–790 [Online]. Available at: <https://doi.org/10.1007/s11948-014-9519-y>.
- [59] Reynolds, M., Goodman, M. P. (2023) *Economic Coercion with Chinese Characteristics*. Center for Strategic and International Studies (CSIS), pp. 7–27 [Online]. Available at: <http://www.jstor.org/stable/resrep48483.5> (Accessed: 21 July 2024).
- [60] Sanchez, M.B. (1987) 'The faces of Justice and State Authority', *Tulsa Law Review*, 23(2), pp. 309–314.

- [61] Schachter, O. (1989) 'Self-Defense and the Rule of Law', *American Journal of International Law*. 2017/02/27 edn, 83(2), pp. 259–277 [Online]. Available at: <https://doi.org/10.2307/2202738>.
- [62] Schmidt, E., Work, R., Catz, S., Horvitz, E., Chien, S., Jassy, A., Clyburn, M., Louie, G., Darby, C., Mark, W., Ford, K., Matheny, J., Griffiths, J.-M., McFarland, K., Moore, A. (2021) *Final Report*. National Security Commission on Artificial Intelligence [Online]. Available at: https://cybercemetery.unt.edu/nscai/20211005231038mp_/https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf (Accessed: 19 February 2024).
- [63] Seyoum, B. (2017) 'Export Controls and International Business: A Study with Special Emphasis on Dual-Use Export Controls and Their Impact on Firms in the US', *Journal of Economic Issues*, 51(1), pp. 45–72 [Online]. Available at: <https://doi.org/10.1080/00213624.2017.1287483>.
- [64] Shagina, M. (2023) 'The Role of Export Controls in Managing Emerging Technology', in Berghofer, J., Futter, A., Häusler, C., Hoell, M., Nosál, J. (eds.) *The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network*. Cham: Springer International Publishing, pp. 57–72 [Online]. Available at: https://doi.org/10.1007/978-3-031-24673-9_4.
- [65] Subrahmanyam, K. (1993) 'Export Controls and the North—South Controversy', *The Washington Quarterly*, 16(2), pp. 135–144 [Online]. Available at: <https://doi.org/10.1080/01636609309443400>.
- [66] Székely, J. (2024) 'Legal Aspects of Dual-Use Technologies: Emerging and Disruptive Technologies', in Szilágyi, J. E. (ed.) *Shielding Europe with the Common Security and Defence Policy*. Miskolc – Budapest: Central European Academic Publishing, pp. 303–353 [Online]. Available at: https://doi.org/10.54237/profnet.2024.zkjeszcodef_7.

- [67] Szép, V. (2024) ‘The legislative history of the EU’s anti-coercion instrument’, *ERA Forum*, 25(1), pp. 127–139 [Online]. Available at: <https://doi.org/10.1007/s12027-024-00784-x>.
- [68] Tamotsu, A. (2016) *Historical Background of Export Control Development in Selected Countries and Regions: U.S., EU, U.K., Germany, France, Hungary, Russia, Ukraine, Japan, South Korea, China, India and ASEAN*. Center for Information on Security Trade Controls [Japan] [Online]. Available at: https://www.cistec.or.jp/english/service/report/1605historical_background_export_control_development.pdf (Accessed: 10 March 2024).
- [69] Tanner, M. S. (2007) ‘Chapter Two. Economic Coercion: Factors Affecting Success and Failure’, in *Chinese Economic Coercion Against Taiwan*. 1st edn. RAND Corporation (A Tricky Weapon to Use), pp. 11–32 [Online]. Available at: <http://www.jstor.org/stable/10.7249/mg507osd.10> (Accessed: 15 July 2024).
- [70] Theodosopoulos, V. (2020) ‘The Geopolitics of Supply: towards a new EU approach to the security of supply of critical raw materials?’, *Institute for European Studies. Policy Brief*, (5), pp. 1–10.
- [71] Tongele, T. N. (2022a) ‘Emerging & Foundational Technology Controls: A General Overview’. *BIS 2022. Update Conference on Export Controls and Policy*, 29 June [Online]. Available at: <https://www.bis.doc.gov/index.php/documents/2022-update-conference/3073-rev3-emerging-tech-update-2022-section-1758-controls-tongele/file> (Accessed: 30 November 2023).
- [72] Tongele, T. N. (2022b) ‘Emerging and Foundational Technology Controls’. *AUECO - Export Controls and Research Security at Higher Education and Scientific Institutions*, 4 May [Online]. Available at: <https://researchservices.upenn.edu/wp-content/uploads/2022/04/Emerging-and-Foundational-tech.pdf> (Accessed: 30 November 2023).

-
- [73] Tzanakopoulos, A. (2015) 'The Right to be Free from Economic Coercion', *Cambridge International Law Journal*, 4(3), pp. 616–633 [Online]. Available at: <https://doi.org/10.7574/cjicl.04.03.616>.
- [74] Uren, D. (2020) *The Rise of Economic Coercion*. Australian Strategic Policy Institute, pp. 7–10 [Online]. Available at: <http://www.jstor.org/stable/resrep26896.5> (Accessed: 13 July 2024).
- [75] Vandenberghe, K. (2021) 'Dual-Use Regulation 2021/821: What's Old & What's New in EU Export Control', *Global Trade and Customs Journal*, pp. 479–488.
- [76] Voetelink, J. (2022a) 'International Export Control Law—Mapping the Field', in Beeres, R., Bertrand, R., Klomp, J., Timmermans, J., Voetelink, J. (eds.) *NL ARMS Netherlands Annual Review of Military Studies 2021: Compliance and Integrity in International Military Trade*. The Hague: T.M.C. Asser Press, pp. 69–94 [Online]. Available at: https://doi.org/10.1007/978-94-6265-471-6_5.
- [77] Voetelink, J. (2022b) 'Limits on the Extraterritoriality of United States Export Control and Sanctions Legislation', in Beeres, R., Bertrand, R., Klomp, J., Timmermans, J., Voetelink, J. (eds.) *NL ARMS Netherlands Annual Review of Military Studies 2021: Compliance and Integrity in International Military Trade*. The Hague: T.M.C. Asser Press, pp. 187–217 [Online]. Available at: https://doi.org/10.1007/978-94-6265-471-6_11.
- [78] Voetelink, J. (2023) 'The Extraterritorial Reach of US Export Control Law. The Foreign Direct Product Rules', *Journal of Strategic Trade Control*, 1(1), pp. 1–23 [Online]. Available at: <https://doi.org/10.25518/2952-7597.57>.
- [79] Weightman, M. A. (1951) 'Self-Defense in International Law', *Virginia Law Review*, 37(8), pp. 1095–1115 [Online]. Available at: <https://doi.org/10.2307/1069591>.

-
- [80] West, D. M., Allen, J. R. (2018) *How artificial intelligence is transforming the world*. The Brookings Institution [Online]. Available at: <https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/> (Accessed: 03 January 2024).
- [81] Wilson, J. D. (2018) 'Whatever happened to the rare earths weapon? Critical materials and international security in Asia', *Asian Security*, 14(3), pp. 358–373 [Online]. Available at: <https://doi.org/10.1080/14799855.2017.1397977>.
- [82] Yang, F., Wang, Y., Whang, U. (2024) 'Trade restrictions on digital services and the impact on manufacturing exports', *The Journal of International Trade & Economic Development*, 33(4), pp. 523–550 [Online]. Available at: <https://doi.org/10.1080/09638199.2023.2195958>.
- [83] Zoller, E. (1984) *Peacetime Unilateral Remedies: An Analysis of Countermeasures*. Dobbs Ferry, New York: Transnational Publishers, Inc.
- [84] 'Article XXI. Security Exceptions' (2012) in *The GATT Analytical Index – Guide to GATT Law and Practice* [Online]. Available at: <https://gatt-disputes.wto.org/sites/default/files/books/GATT%20Analytical%20Index.pdf> (Accessed: 12 March 2024).
- [85] *Bipartisan Coalition Introduces Monumental Bill Giving Admin Authority to Export Control Advanced AI Systems* (2024). Available at: <https://foreignaffairs.house.gov/press-release/bipartisan-coalition-introduces-monumental-bill-giving-admin-authority-to-export-control-advanced-ai-systems/> (Accessed: 14 May 2024).
- [86] Bonarriva, J., Koscielski, M., Wilson, E. (2009) 'Export Controls: An Overview of Their Use, Economic Effects, and Treatment in the Global Trading System'. Office of Industries U.S. International Trade Commission [Online]. Available at: <https://www.usitc.gov/publications/332/ID-23.pdf>.

-
- [87] Bureau of Industry and Security (2022) ‘Identification of Section 1758 Technologies’ [Online]. Available at: <https://www.bis.gov/articles/implementation-certain-2021-wassenaar-arrangement-decisions-four-section-1758-technologies> (Accessed: 9 February 2024).
- [88] Bureau of Industry and Security (2023a) *Commerce Strengthens Restrictions on Advanced Computing Semiconductors, Semiconductor Manufacturing Equipment, and Supercomputing Items to Countries of Concern*. Available at: <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3355-2023-10-17-bis-press-release-ac-and-sme-rules-final-js/file> (Accessed: 15 December 2023).
- [89] Bureau of Industry and Security (2023b) ‘Export Controls on Semiconductor Manufacturing Items’. Available at: <https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3352-10-16-23-semiconductor-equipment-controls/file> (Accessed: 14 April 2024).
- [90] Bureau of Industry and Security (2023c) ‘Export Controls on Semiconductor Manufacturing Items [Entity List]’. Available at: <https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3352-10-16-23-semiconductor-equipment-controls/file> (Accessed: 14 April 2024).
- [91] Bureau of Industry and Security (2023d) ‘Implementation of Additional Export Controls: Certain Advanced Computing Items; Supercomputer and Semiconductor End Use; Updates and Corrections’. Available at: <https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3353-2023-10-16-advanced-computing-supercomputing-ifr/file> (Accessed: 10 April 2024).

-
- [92] Bureau of Industry and Security (2024a) ‘Additions of Entities to the Entity List’. Available at: <https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3502-2024-10485/file> (Accessed: 17 April 2024).
- [93] Bureau of Industry and Security (2024b) *Rules Affecting the Export Administration Regulations*. Available at: <https://www.bis.doc.gov/index.php/federal-register-notices> (Accessed: 17 April 2024).
- [94] Bureau of Industry and Security (2024c) ‘Supplement No. 1 to Part 740’. Available at: <https://www.bis.doc.gov/index.php/documents/regulation-docs/2255-supplement-no-1-to-part-740-country-groups-1/file> (Accessed: 17 April 2024).
- [95] Bureau of Industry and Security, Commerce (2018) *Review of Controls for Certain Emerging Technologies*. Available at: <https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies> (Accessed: 15 November 2023).
- [96] Congressional Research Service (2021) *The U.S. Export Control System and the Export Control Reform Act of 2018*. R46814. Available at: <https://crsreports.congress.gov/product/pdf/R/R46814> (Accessed: 20 November 2023).
- [97] ‘Critical and Emerging Technologies List Update’ (2024). Available at: <https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf> (Accessed: 15 April 2024).
- [98] *Enhancing National Frameworks for Overseas Restriction of Critical Exports Bill* (2024). Available at: https://foreignaffairs.house.gov/wp-content/uploads/2024/05/MCCAUL_128_xml-ENFORCE-Act.pdf (Accessed: 14 May 2024).

- [99] European Commission (2021) ‘Combined Evaluation Roadmap/Inception Impact Assessment’. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13129-Unlawful-extra-territorial-sanctions-a-stronger-EU-response-amendment-of-the-Blocking-Statute-_en (Accessed: 17 October 2023).
- [100] European Commission (2023) ‘Joint Communication to the European Parliament, the European Council and the Council on “European Economic Security Strategy”’. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0020> (Accessed: 13 October 2023).
- [101] European Commission (2024) *White Paper on Export Controls, COM(2024) 25 final*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0025> (Accessed: 1 March 2024).
- [102] ‘National Strategy for Critical and Emerging Technologies’ (2020). Available at: <https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf> (Accessed: 15 April 2024).
- [103] OECD (2023) *Science, technology and innovation policy in times of strategic competition*. Available at: <https://doi.org/10.1787/f3c247fc-en>.
- [104] *Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution* (2023). Available at: <https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution/> (Accessed: 14 February 2024).

-
- [105] *Supplement No. 4 to Part 744, Title 15. Entity List* (2024). Available at: [https://www.ecfr.gov/current/title-15/part-744/appendix-Supplement No. 4 to Part 744](https://www.ecfr.gov/current/title-15/part-744/appendix-Supplement+No.+4+to+Part+744) (Accessed: 21 March 2024).
- [106] ‘The United States Announces Export Controls to Restrict China’s Ability to Purchase and Manufacture High-End Chips [Editorial]’ (2023) *The American Journal of International Law*, 117(1), pp. 144–150 [Online]. Available at: <https://doi.org/10.1017/ajil.2022.89>.
- [107] ‘The Use of Nonviolent Coercion: A Study in Legality under Article 2(4) of the Charter of the United Nations [Editorial]’ (1974) *University of Pennsylvania Law Review*, 122(4), pp. 983–1011 [Online]. Available at: <https://doi.org/10.2307/3311418>.
- [108] The Wassenaar Arrangement Secretariat (2023) *List of Dual-Use Goods and Technologies and Munitions List*. Available at: <https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf> (Accessed: 29 February 2024).
- [109] *Trade Impacts of Economic Coercion* (2024). OECD Trade and Agriculture Directorate. Available at: https://beta.oecd.org/content/dam/oecd/en/publications/reports/2024/05/trade-impacts-of-economic-coercion_044bdb0a/d4ab39b9-en.pdf (Accessed: 31 May 2024).
- [110] UN General Assembly (1965) *Resolution 2131 (XX). Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty General Assembly*. Available at: https://legal.un.org/avl/ha/ga_2131-xx/ga_2131-xx.html (Accessed: 31 May 2024).

- [111] UN General Assembly (1970) *Resolution 26/25 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*. Available at: <https://www.refworld.org/legal/resolution/unga/1970/en/19494> (Accessed: 31 May 2024).
- [112] UN General Assembly (1973) *Resolution 3171 (XXVIII). Permanent sovereignty over natural resources*. Available at: <https://www.refworld.org/legal/resolution/unga/1973/en/9902> (Accessed: 31 May 2024).
- [113] UN General Assembly (1974) *Resolution 3281 (XXIX). Charter of Economic Rights and Duties of States*.
- [114] UN General Assembly (2001) *General Assembly Resolution 56/83 of 12 December 2001. Annex. Responsibility of States for Internationally Wrongful Acts*. Available at: <https://www.ilsa.org/Jessup/Jessup11/basicmats/StateResponsibility.pdf>.
- [115] *United Nations Charter* (1945). Available at: <https://www.un.org/en/about-us/un-charter> (Accessed: 15 November 2023).
- [116] *United States: Export Control Reform Act (ECRA)* (2019). Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/644187/EPRS_BRI\(2019\)644187_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/644187/EPRS_BRI(2019)644187_EN.pdf).

ZVONKO TRZUN*

Artificial Intelligence and Human-out-of-the-Loop: Is It Time for Autonomous Military Systems?***

ABSTRACT: This paper systematically presents the disruptive technologies that have emerged on the battlefields in recent decades, as well as those that are yet to come. Special attention is given to current technical capabilities: the status of unmanned vehicle development is briefly outlined, focusing primarily on the most prevalent type, unmanned aerial vehicles (UAVs). Additionally, the paper discusses the most common and effective adversarial attack techniques specifically targeting unmanned vehicle technology. The concepts of artificial intelligence (AI), machine learning, deep learning, and convolutional neural networks (CNNs) are introduced. The paper illustrates how CNNs aim to tackle tasks that previously required human intelligence, as well as how the enemy attempts to disrupt the development of CNNs during the crucial training and pattern recognition phase, which is essential for later generalisation. The paper demonstrates the advantages of manned-unmanned teaming as a model that effectively utilises disruptive technologies while simultaneously counteracting the effects of the enemy's measures. Moreover, it analyses the introduction of fully autonomous, AI-driven military systems on the battlefield, outlining the advantages and disadvantages inherent to such a fundamental change. From the evident lack of interest among young people in joining the armed forces to the autonomous systems' potential to save the lives of soldiers and civilians, there are numerous reasons suggesting that this technology could alleviate the burden on human soldiers. However, concerns remain that

* Assist. Prof. Dr.sc., Dr. Franjo Tuđman University of Defense and Security, Croatia.
<https://orcid.org/0000-0003-3570-9063>, zvonko.trzun@sois-ft.hr.

** The research and preparation of this study was supported by the Central European Academy.

autonomous systems may malfunction, potentially reducing rather than increasing the safety of militaries. The paper concludes with recommendations for future steps in the introduction of new technologies, based on their current state of development and the robustness of the AI models they use.

KEYWORDS: Artificial Intelligence, Human-out-of-the-Loop, autonomous military systems, adversary attacks, manned-unmanned teaming.

1. Introduction

Unmanned Military Systems (UMSs) are becoming essential components of military arsenals. Driven by adverse demographic shifts, declining interest in military enlistment, and public aversion to domestic casualties resulting from armed conflicts, UMSs are increasingly deployed on modern battlefields¹. Once deployed, their outstanding efficiency and the benefits they offer typically justify their substantial initial procurement costs. In essence, unmanned systems are entering and remaining on battlefields around the world, underlining their status as more than just experimental endeavours. Numerous examples of such systems have emerged over the past few decades, to the extent that at present, modern armies cannot be envisioned without them. The groundbreaking moment came with the first actions of the unmanned aerial vehicle (UAV) Predator, recorded at the end of the 20th century. Initially designated as RQ-1 in accordance with the US Air Force's naming conventions, where the letter "Q" is reserved for unmanned aircraft and "R" for reconnaissance missions, this widely utilised UAV underwent a significant transformation in 2002. With the addition of the AGM-114 Hellfire air-to-ground missiles, it was re-designated as MQ-1, signifying its newfound multi-role capabilities.² The elegant silhouette, akin to a sailboat, combined with its low weight and large wingspan of 14.8 meters, allowed it to achieve a substantial operational range and endurance in the air for a commendable number of hours.

However, that was just the beginning: the Predator was soon followed by its more powerful successor, the MQ-9 Reaper, boasting a wider operational range and greater endurance (1900 km and 27 h vs. Predator's

¹ Krishnan, 2009, p. 7.

² Watts, 2013, p. 18.

1250 km and 24 h), a higher ceiling (50,000 ft. vs. 25,000), increased payload capacity (1750 kg vs. 200 kg) and superior armament (8 AGM-114 Hellfire Missiles, or a combination of Hellfire missiles, GBU-12 Paveway II laser-guided bombs, GBU-38 Joint Direct Attack Munitions, GBU-49 Enhanced Paveway II, or GBU-54 Laser Joint Direct Attack Munitions).³ The MQ-9 Reaper is also equipped with an enhanced Multi-Spectral Targeting System (MTS), featuring a robust suite of visual sensors for precise targeting. Its MTS-B integrates an infrared sensor, colour and monochrome daylight TV cameras, shortwave infrared camera, laser designator, and laser illuminator.⁴ Following the MQ-9 Predator, other sizeable UAVs followed, built on related or independent platforms (for example, the MQ-20 Avenger UAV with jet propulsion and a maximum speed of 720 km/h, the MQ-9B SkyGuardian with an increased 24-meter wingspan and an extended range of 2500 km, or the heavyweight Northrop Grumman's RQ-4 Global Hawk classified as the only HALE USAF unmanned aircraft).

2. Different Classes of Unmanned Vehicles

European industry has also ventured into the development of HALE and MALE UAVs⁵, although with less success thus far. However, this does not necessarily imply a negative outcome. Recent military conflicts, particularly the intense battles between Russia and Ukraine, have demonstrated the significant utility of tactical UAVs at a considerably lower cost. In this regard, the European industry has achieved greater success, partly due to reduced technical requirements and development costs, and partly because individual countries were able to develop their own systems instead of engaging in uncertain and often unsuccessful collaborations with other European nations. Notable examples include French Safran's development of the Patroller UAV, Spain's collaboration with Colombia in developing the SIRTAP tactical UAV, and Italy's Leonardo manufacturing the FALCO

³ US Air Force (2021) MQ-9 Reaper, [Online]. Available at: <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/> (Accessed: 18 October 2023).

⁴ General Atomics (2020) Lynx Multi-Mode Radar: Surveillance, Tracking, Targeting for Manned and Unmanned Missions, Lynx Datasheet, [Online]. Available at: <https://www.ga-asi.com/radars/lynx-multi-mode-radar> (Accessed: 5 November 2023).

⁵ HALE: High-Altitude Long Endurance UAVs; MALE: Medium-Altitude Long Endurance UAVs.

EVO, among others. These small UAVs feature an endurance exceeding 20 hours, a range of approximately 200 km, a payload capacity of around 200 kg, a ceiling of 6,000 m, and a maximum speed of about 200 km/h. However, there are notable drawbacks, including redundant research and expenditures, resulting in associated costs amounting to a significant 500 million EUR per country. As a result, European attempts to reduce dependence on foreign drone technology through costly capability development projects were unsuccessful.⁶ Tactical UAVs, suitable for a wide range of Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) missions,⁷ are still better solutions for a highly contested airspace, compared to expensive and still vulnerable large MALE and HALE UAVs.

This suggests that it would be beneficial for European nations to undertake joint projects on a more regular basis. However, this is not typical, as each country strives to bolster its technological autonomy, invest in its own manufacturing capabilities, and retain exclusive control over UAV development, including specific requirements. This is particularly evident in the case of the Eurodrone MALE UAV project, which is heavily influenced by conflicting demands from the initiating countries.⁸ For instance, Germany prioritised a twin-turboprop configuration for security reasons, whereas France opted for a lighter aircraft. Additionally, Germany has only recently shown interest in developing an armed UAV with attack capabilities, a request initially made by the other founding nations (France, Italy, and Spain).

It would appear that major EU countries are trailing behind in the global market competition, which is dominated by manufacturers from the USA, China, Turkey, and Russia. They have opted to concentrate on creating top-tier MALE UAVs, despite the lessons learned from the Russo-Ukrainian conflict suggesting that quantity often outweighs quality in today's landscape. By committing to developing a single large and costly UAV, which is likely to become outdated by the time of project completion, EU countries continue to fall behind in production and may struggle to set a foothold in the global UAV market. Historical experiences do not favour participation in large-scale EU initiatives either, which tend to result in delayed deliveries of expensive systems with subpar technical capabilities.

⁶ Kunertova, 2022, pp. 3-4.

⁷ Bartulović, Trzun and Hoić, 2023, p. 87.

⁸ Kunertova, 2021, p. 3.

Regrettably, grandiose projects persist while the benefits of miniaturisation, proven effective in recent military conflicts, are disregarded.

As for the unmanned ground, surface, and underwater vehicles (abbreviated UGVs, USVs, and UUVs respectively), their achievements thus far have been modest, primarily due to the challenges of navigating and operating in environments cluttered with obstacles.⁹ However, this does not mean that the development of such systems has been halted. For example, the Milrem THeMIS tracked UGV has been built in various iterations, spanning from logistical support vehicles to intelligence, surveillance, and reconnaissance (ISR) variants. Even armed versions of UGVs have been developed capable of carrying various armaments from a 12.7 mm machine gun to a 40 mm grenade launcher. For example, in early 2024, footage was released showing the destructive attack by the Ukrainian Ironclad wheeled UGV on a Russian position. Surface and underwater unmanned systems play an even more significant role in the Russo-Ukrainian war, with the most recent example being on 1 February 2024, when multiple Ukrainian GPS-guided MAGURA V5 USVs attacked and ultimately sank the Russian missile corvette ‘Ivanovets’ of the Tarantula-III class.

3. Signal Jamming: Obstruction to the Stronger Use of Unmanned Systems

The increasing capabilities of unmanned systems are evident, yet their susceptibility to signal interference cannot be overlooked. Electronic warfare (EW) encompasses the use of a set of powerful tools across three main categories: electronic support (ES), electronic self-protection (EP), and electronic attack (EA). This paper places particular emphasis on EA measures, which involves jamming or other offensive actions aimed at degrading the electromagnetic systems and communications of an adversary. Through EW measures, a less technologically advanced opponent can offset its disadvantage against a more advanced adversary by nullifying the capabilities of its modern systems. As for unmanned vehicles (regardless of their domain), after encountering unbeatable signal interference, they enter idle mode and subsequently circle aimlessly in an attempt to reconnect with the remote pilot.¹⁰

⁹ Zhou et al., 2021, p. 1576.

¹⁰ Smith, 2020, p. 4.

Faced with modern EW measures, unmanned systems actually become more vulnerable the more advanced they are. For example, inertial guidance has its limitations and depends on the accurate operation of accelerometers, so today it is often paired with or even replaced by GPS guidance. However, strong EW defence manages to replace the real GPS signal with a fake one, causing unmanned vehicles to make errors in assessing their location by tens or hundreds of kilometres. Russia was particularly successful in developing its EW capabilities after bad experiences during the 2008 Russo-Georgian War. Based on a sincere analysis and an acknowledgment of the shortcomings of the equipment used at the time, Russia launched its ambitious Armed Forces reform, aiming to have up to 70% new or modernised equipment in the military inventory. This particularly applied to strategic EW systems, which were recognised as an “asymmetric response to the network-centric system of combat operations” on the part of the US and NATO.¹¹ The Murmansk-BN, a powerful system with a reported range of 5,000 km, capable of the continuous monitoring of electromagnetic activity and intercepting enemy signals with a broad jamming capability, has been recognised as acknowledged the core part of the Russian EW capabilities.

The consequences of such uncompromising modernisation of EW capabilities can be observed today in the Russo-Ukrainian conflict. Regarding the abovementioned GPS spoofing attacks, there are indications that they are deployed across the entire battlefield with significant impact. It is alleged that Russian EW equipment can emit false GPS signals that are an astonishing 500 times stronger than genuine ones.¹²

Generally, the side deploying unmanned vehicles (UVs) seeks to evade the effects of jamming systems and other EW measures by employing more advanced tactics, such as utilising variable frequencies for unmanned vehicle communication with the base station (cognitive radio). Communication between the pilot and the UV is programmed to dynamically change and rapidly select new frequencies to avoid any interruption of data transfer. The algorithm for adjusting transmission parameters continuously analyses the received signal; if adversary interference is detected, changes in transmission parameters, such as

¹¹ McDermott, 2017, p. 15.

¹² Smith, 2020, p. 4.

frequency, power or modulation are applied. Simultaneously, an alternative frequency range is selected if the current range is deemed unsuitable.¹³

A conflict between two opposing sides where one seeks to disrupt the guidance signal for unmanned vehicles while the other endeavours to evade signal interference poses one of the primary challenges in the wider adoption of UVs. In contemporary conflicts varying in intensity, there is an obvious effort to overcome the defences of the opposing side by deploying a multitude of cheap and disposable robots/drones that attack otherwise well-defended objectives simultaneously. The guidance signal is attempted to be concealed within channels already congested with high data traffic, particularly in urban warfare scenarios. Even highly affordable commercial drones are utilised, with their MAC addresses altered to prevent the identification of the control station (the first six characters of a MAC address denote the manufacturer).¹⁴

Up to this time, the most prominent instances of employing multiple unmanned vehicles to overload defensive systems took place during the sinking of the cruiser 'Moskva' and the missile corvette 'Ivanovets'. In the case of the 'Moskva', it is alleged that one or two Bayraktar TB-2 UAVs prevented the defensive systems from detecting the incoming 'Neptune' missile. However, this seems less probable, as the ship's anti-drone and anti-missile defences were provided by two different systems: long-range S-300F (NATO designation: SA-N-6 Grumble) missiles against the Bayraktar and similar slow-moving UAVs, and multi-barrelled AK-630 cannons planned to engage the incoming missiles. On the other hand, during the sinking of the corvette 'Ivanovets', it appears that six MAGURA V5 USVs easily overwhelmed the relatively weak defence of the Russian ship.

4. Artificial Intelligence and Autonomous Systems

The most effective solution to evade the adversary's EW capabilities could be fully autonomous unmanned vehicles, i.e., vehicles that will advance on the battlefield guided by their own artificial intelligence. The use of autonomous weapon systems offers numerous advantages, ranging from economic and operational to security and humanitarian benefits.¹⁵ From an economic perspective, replacing a destroyed robot or drone is certainly more

¹³ Semendiai et al., 2023, p. 731.

¹⁴ Kratky et al., 2020, p. 449.

¹⁵ Monte, 2018, p. 6.

cost-effective than replacing a highly trained, well-equipped soldier. However, this is primarily applicable to Western armies and their warfare strategies, where the adoption of new technologies aims to preserve the lives of their own soldiers (in some other societies, individuals are being seen as easily replaceable assets with minimal economic worth). Autonomous systems can significantly level the playing field between two armies, especially when one possesses a significant numerical advantage in terms of available personnel.

Autonomous systems provide the capability for extremely quick responses to enemy actions. In the event of changes on the battlefield, these systems can swiftly adjust, capitalising on any new opportunities for advancement or promptly reinforcing defences where necessary. The impact of human errors is reduced – a highly significant aspect, especially considering that a significant portion of contemporary accidents, leading to the costly destruction of sensitive equipment, originates from human errors.¹⁶

From the standpoint of resilience against enemy EW measures, AI-driven systems can continue with combat operations even if the connection with remote pilots is disrupted. In accordance with mission-oriented or mission-type commands, autonomous systems do not require detailed or subsequent instructions once clear objectives are assigned to them. The degree of autonomy depends on the specific system.¹⁷ Semiautonomous systems are often referred to as “human-in-the-loop”, where a pilot has to make a positive decision to engage a target. All other actions (such as movement, target tracking, or perimeter monitoring) can be carried out autonomously by such a system. Supervised autonomous systems (“human-on-the-loop”) represent the next level, where the robot can autonomously find, identify, and even engage targets, but a pilot monitors the situation and is able to intervene to discontinue the engagement. The highest level of independence is provided by full autonomous weapons, where human pilots are “out-of-the-loop”, meaning they have no ability to intervene in the process of weapon engagement. There are also additional classifications of systems based on the level of autonomy achieved.¹⁸ The ‘loop’ that is mentioned here is actually the OODA loop, which stands for observing,

¹⁶ Wróbel, 2021, p. 9.

¹⁷ Feldman, Dant and Massey, 2019.

¹⁸ Haider, 2021, pp. 14–15.

orienting, deciding, and acting, depending on the current state of the weapon and the target.¹⁹

Autonomous systems across all three autonomy levels (especially fully autonomous ones) could profoundly alter modern warfare, potentially undermining the current strategies and capabilities of less developed armies. These armies could only reach for the robust EW procedures as a relatively cost-effective asymmetric measure to neutralise the advantages of adversaries with highly sophisticated systems and methods of armed combat.²⁰

The enhanced safety of both our troops and civilians is also worth noting. Regarding our forces, it has been previously mentioned that autonomous systems could be deployed in combat operations, either in lieu of soldiers or alongside them, to mitigate the risk of damage. Additionally, in terms of civilian safety, autonomous systems could potentially adhere more strictly to the international humanitarian laws of war, even more reliably than humans, who may be influenced by heightened emotions and stress induced by prolonged fear and uncertainty.²¹ Yet, in order for such civilian protection to be effectively realised, it is imperative for autonomous systems to be able to accurately detect civilians and differentiate them from adversary soldiers. Regrettably, AI-driven systems are currently unable to fulfil this task with an adequate level of reliability.

Considering the aforementioned factors, at present it is foreseeable that there will be further advancement in the concept of manned-unmanned teaming (MUM-T). This concept emphasises a team encompassing multiple units, with the human-operated unit retaining a central role, while additional AI-driven units serve for support and protection. Over time, these AI-driven units are likely to be granted increasing levels of autonomy and to be tasked with more complex assignments. However, the central unit should always remain under human control, ensuring oversight over the entire team. The MUM-T approach is moving towards a model of 'human-on-the-loop' supervised autonomy, wherein AI-driven units can autonomously perform a significant part of their tasks, thereby relieving humans from routine supervisory duties such as movement or obstacle avoidance. Nonetheless, human intervention remains crucial for decisions about whether certain actions should proceed or be halted.

¹⁹ Morgan et al., 2020, p. 12.

²⁰ McDermott, 2017, p. 3.

²¹ Monte, 2018, p. 162.

The emergence of the MUM-T concept is expected to remain a prominent trend for the foreseeable future, spanning over years or even decades. AI models will require thorough testing and refinement, raising questions about the feasibility of granting them full autonomy ('human-out-of-the-loop'), given the potential for numerous incidents and collateral damage. In parallel with technological progress, there must be a concerted effort to develop a suitable legal framework, which may involve amendments to international humanitarian law.

As for the "human-out-of-the-loop" (HOOTL) concept, it indeed offers a number of advantages. It provides unprecedented efficiency and speed, scalability (these systems can handle large-scale operations without the limitations of human attention span and fatigue), increased safety for the implementing side, and significant cost reduction. HOOTL fully autonomous weapons and surveillance systems could operate independently in complex and potentially hostile environments. Nevertheless, there are also many challenges and risks associated with such systems, where safety and reliability are paramount. Errors or malfunctions can lead to catastrophic consequences. As AI and machine learning technologies advance, the potential for HOOTL systems to become more prevalent increases.

5. Techniques and Tools of Artificial Intelligence

Artificial Intelligence (AI) represents a specific field of computer science that deals with creating systems capable of performing tasks that typically require human intelligence. One of the key tools in the field of AI is machine learning (ML), which enables computers to learn from experience without explicit programming. ML is based on the concept of algorithms that analyse data, identify patterns in those data, and use those patterns to make decisions or predictions. Examples of ML applications span from image and speech recognition to product recommendations and data analysis.²²

Machine learning is characterised by its capability to automatically enhance system performance through experience. Instead of manual rule definition by programmers, ML algorithms utilise data to discern implicit patterns and regularities, applying acquired knowledge to novel,

²² Wang and Siau, 2019, pp. 61-63.

unencountered situations.²³ There are three primary types of ML: supervised learning, unsupervised learning, and reinforcement learning. In supervised learning, algorithms are trained on labelled data with correct answers, with the aim to generalise learned patterns to new, unlabelled data. Unsupervised learning involves analysing data that lack labelled correct answers, with algorithms tasked with discovering hidden patterns and structures, such as clustering similar items or reducing dimensionality. In reinforcement learning, algorithms interact with the environment, adjusting their strategies based on feedback to maximise rewards or minimise penalties.²⁴

A special and widely applicable subtype of ML is deep learning (DL), used for its ability to learn from highly complex datasets. Deep learning also uncovers patterns in data but employs different techniques. Both methodologies (DL and ML) start out with training using sample data and models, during which they establish relevant connections between different data points. Following this, they undergo an optimisation process to ascertain the most precise weighted values among these connections and to ensure that the model aligns as closely as possible with the data.

DL employs artificial neural networks with numerous layers, hence the term “deep”. These networks can recognise intricate patterns within data, allowing them to address highly complex tasks.²⁵ Rather than manually defining features or rules, deep neural networks learn implicit patterns and structures through layers of data transformations. Each layer processes input data and generates output features, which then serve as input for subsequent layers, allowing for a progressive abstraction and broader generalisation of the data.²⁶

Some of the most commonly utilised DL networks are convolutional neural networks (CNNs) and recurrent neural networks (RNNs). CNNs are particularly efficient in analysing images and video content by utilising convolutional layers to extract local features and reducing the dimensionality of input data. Conversely, RNNs are adept at handling sequential data such as text or time series, utilising recurrent connections between neurons to model temporal dependencies.²⁷

²³ Janiesch, Zschech and Heinrich, 2021, p. 686.

²⁴ Carleo et al., 2019, p. 045002-5.

²⁵ Bengio, Lecun and Hinton, 2021, p. 60.

²⁶ Mu and Zeng, 2019, p. 1745.

²⁷ Janiesch, Zschech and Heinrich, 2021, pp. 688-690.

CNNs have achieved remarkable results in areas such as object recognition, image classification, face detection, medical diagnostics, and other domains where visual data analysis is utilised. The main characteristic of CNNs is the use of convolutional layers, alongside which CNNs typically involve pooling layers that serve to reduce the dimensionality and computational complexity of the model. The aim is to aggregate and summarise information from convolutional layers, thereby facilitating the further processing and interpretation of features.

A key advantage of CNNs is their ability to automatically learn hierarchical features from input data. In this sense, CNNs seek to simulate the functioning of the central nervous system of living organisms, namely the brain. Similar to our biological nervous system, CNNs consist of simple processing units whose task is mutual communication through a high number of connections.²⁸ Instead of manually defining features or patterns, CNNs use data-driven learning through an iterative process of optimising network weights to minimise prediction errors. An activation function (often referred to as a transfer function) is then used for further information transfer. Some of the most common ones are the threshold function, the piecewise linear function, and the sigmoid function.

The technique of using CNNs has attained outstanding results in many tasks, at times surpassing human capabilities. It is applied in image recognition, object detection and segmentation, medical diagnostics, natural language translation, time series analysis, and much more – including autonomous driving through the analysis of geospatial data. However, it is important to emphasise that the level of accuracy and reliability of these techniques still varies depending on the data presented and the quality of the training process.

6. Problems and Limitations of AI Training

Below are some of the most common issues encountered with the techniques discussed above.

6.1. Data Bias

If the training dataset is not sufficiently diverse or representative, the algorithm may learn biased patterns and become unbalanced in its predictions. Data bias, also known as dataset imbalance, is caused by a

²⁸ Li et al., 2021, pp. 6999-7002.

situation where certain classes or categories have a greater number of examples in the dataset compared to other classes. This phenomenon often occurs in real-world datasets due to natural variations or irregularities in the data collection process and can result in unfair models that prefer dominant classes, while neglecting or misclassifying less represented ones.²⁹ For example, in a dataset aimed at recognising armoured vehicles, there might be more images of Abrams tanks than images of other tanks. If a CNN is trained on such a dataset, there is a risk that the model will recognise Abrams tanks better than other armoured vehicles, which will subsequently be recognised with significantly lower reliability.

Employing biased algorithms in autonomous weapons systems would negatively impact already marginalised groups. The solution to this problem involves collecting a larger and more diverse dataset, along with additional data collection for less represented classes, and applying techniques such as data augmentation (generating new examples from existing data) or adjusting weights in learning algorithms to account for class imbalances in the sample.

6.2. Overfitting

Overfitting is a common problem in the context of CNNs. When a CNN becomes too tailored to the training dataset, it can lose the ability to generalise to new data. Solutions for overfitting include using regularisation techniques such as dropout, early stopping, and gradient normalisation.

Overfitting can occur for various reasons. One of the main causes is the complexity of the model. If the model is too complex and has too many parameters relative to the amount of available data, it may learn overly complex patterns that are not necessarily relevant to the general population of data. The model develops excessive adaptations to the sample used during training, while losing the ability to generalise to new data acquired later. Unlike human problem solving, which is inherently flexible and capable of adapting to new and diverse challenges, machine-learning systems are usually not transferable to entirely different problem contexts.³⁰

Overfitted models have poor generalisation ability with regard to new data, resulting in poor performance in real-world applications. For example, if an overfitted model is used for image classification, incorrect predictions

²⁹ Ntoutsis et al., 2020, pp. 4-5.

³⁰ Surden, 2021, p. 175.

may ensue when the model is applied to images that were not present in the training dataset.

Fortunately, there are various strategies for addressing overfitting (if a larger training dataset is not available). One of the most common strategies is regularisation, which involves adding additional constraints to the model to prevent overfitting. This can include techniques such as dropout, where certain neurons are randomly excluded during training, as well as cross-validation and early stopping.

6.3. Scarcity of Data

Under particular circumstances, acquiring the sufficient volume of data for training a CNN may present challenges, particularly in cases involving constrained datasets, such as those pertinent to medical diagnostics. The process of data collection for scientific inquiry can similarly involve significant costs, time investments, or ethical considerations. Moreover, impediments of a technical or legal nature might obstruct access to extant datasets. Irrespective of the underlying factors contributing to these obstacles, the scarcity of data can curtail the CNN's capability to learn general patterns and structures.³¹

An effective strategy to address this scenario involves employing transfer learning methodologies, wherein the model undergoes training on a comparable yet more expansive dataset. Along with regulating the quantity, it is imperative to oversee the quality, particularly the representativeness, of the training data. This entails processes such as filtering, cleansing, and normalising the data to eliminate any problematic or incongruous instances.³²

6.4. Interpretability

The interpretability of CNNs, or the ability to understand and explain their predictions, also poses a significant challenge. Given that CNNs are complex models with numerous parameters, it is difficult to discern the features or patterns utilised by the model to make decisions.

Interpretability could prove to be a crucial aspect in the context of public trust in AI, as it helps understand why models have made certain decisions and how they have arrived at their predictions. Public trust is particularly vital in critical domains such as medical diagnostics, finance,

³¹ Janssen et al., 2020, p. 2.

³² Bansal, Sharma and Kathuria, 2022, p. 8.

and legislative issues³³ — but perhaps most notably in the realm of military decision-making.

There are several approaches to interpretability in machine learning. One of them is feature visualisation, where techniques like heatmaps and saliency maps are employed to display the relevant features of input data that have influenced the model's final decision. Additionally, attribution methods such as LIME (Local Interpretable Model-agnostic Explanations) approximate any black-box ML model to a local, interpretable model.

6.1.1. Introducing Noise into Data During Wartime

In wartime conditions, the adversary will likely undertake all available actions to disrupt the process of training AI models or to corrupt established connections. Introducing noise into field data poses a significant problem in the realm of data analysis and machine learning. Noise can be defined as unwanted additions to or disturbances in data and can be introduced from various sources. Noise can compromise the accuracy and reliability of data analysis or model predictions. For example, in image recognition or object detection in images, the presence of noise can lead to incorrect classifications or inaccurate predictions. Furthermore, noise can reduce the interpretability of analysis results by making it difficult to distinguish relevant signals from unwanted interference.³⁴ Finally, noise can increase the complexity of the model and consume resources for data processing and learning.

Resolving the problem of noise in input data requires the application of various strategies and techniques. One possible approach is the application of data filtering and cleaning, where algorithms are used to detect and remove noise. This technique may involve the use of different filters such as median filters or averaging. Another possibility is to apply techniques which reduce the model's sensitivity to noise. This might include employing robust algorithms that are more resilient to data noise or utilising regularisation techniques to avoid overfitting on data corrupted by noise.³⁵

The strategy of introducing noise can be viewed as a type of electronic warfare or, alternatively, a form of tactical deception. Injecting noise into the visual identification of equipment by adversarial systems can be

³³ Rodrigues, 2020, p. 2.

³⁴ Xiong et al., 2006., pp. 305-307.

³⁵ Gupta and Gupta, 2019, pp. 471-472.

executed through diverse methods, contingent upon the precise technical attributes of the image recognition system being used. Here are a few possible scenarios.

The first is image manipulation, which means altering or distorting the appearance of one's equipment to make it less recognisable to adversary systems. This may include adding false details, altering colours or textures, or even completely changing the visual shape to deceive image recognition algorithms. The problem of image manipulation is particularly significant with the advent of deep-fake technology. Innovative tools are being developed to detect such manipulations and uncover genuine information,³⁶ but at the same time, new methods for even more sophisticated image and video manipulation are being constantly revealed.³⁷

The second is masking, which means employing camouflage techniques to hide equipment. This can entail using colours and patterns that blend seamlessly with the surroundings. Additionally, natural cover or artificially created shapes may be utilised to integrate the equipment into the environment, making it less conspicuous to sensors. Furthermore, equipment can be coated with reflective materials to disrupt enemy IC or laser sensors.

The third is distorting sensor data, which implies disrupting the operation of sensors or cameras using flashes, laser devices, or other devices that could interfere with or overload enemy sensors.

And finally, there is the injection of false data, namely introducing distorted facts or images into the training set of the opponent's system, leading it to draw incorrect conclusions. This can be done by sending false signals or data through electronic communication channels, or even by hacking the opponent's system while it is still in the training phase.^{38,39}

Employing such tactics carries significant implications, including potential ethical and legal ramifications. While the methods described may indeed disrupt the adversary's recognition systems, they also pose risks of unintended consequences or misinterpretations of the battlefield situation. Specifically, such tactics could lead to false negatives, where AI systems fail to identify the adversary's assets or combatants accurately, but also lead to false positives, where the adversary's AI wrongly identifies civilians and

³⁶ Lee et al., 2023, pp. 3-4.

³⁷ Zhang, Li and Chang, 2024, p. 4.

³⁸ Tufail, Batool and Sarwat, 2021, p. 3.

³⁹ Gong and Wang, 2023.

their vehicles or structures as military targets. Given these risks, the legitimacy of such tactics is subject to scrutiny. The use of noise can be interpreted as a form of unfair combat or a violation of international rules of warfare, especially if it results in unjustified civilian casualties or unnecessary destruction.

In their paper “Intriguing Properties of Neural Networks”, Szegedy et al. (2014)⁴⁰ introduced the concept of an “adversarial example”, which refers to an example created with the aim of manipulating or inducing errors in deep learning models. The authors acknowledge that deep neural networks (DNNs) are ‘powerful learning models that achieve excellent performance on visual and speech recognition problems,’ but they also point out two counter-intuitive properties of deep neural networks. The first is a significant question regarding the conjecture that neural networks disentangle variation factors across coordinates. The second is related to the stability of neural networks with respect to small perturbations to their inputs. Unlike intuitive thinking, DNNs (which otherwise generalise well on the task of object recognition) may react even to very small perturbations, carefully crafted so that the DNN completely misidentifies the object category in the presented image.

Adversarial attacks involve making slight alterations to input data, introducing changes so subtle that they are practically imperceptible to the human eye. On the other hand, DNNs can become “confused” and produce erroneous object detections on images manipulated by adversaries. An illustrative instance of such an attack is the image of a panda, initially identified by a DNN with a confidence of 57.7%. However, after injecting noise into the image, the DNN incorrectly classified the object as a gibbon with an exceedingly high confidence level of 99.3%.⁴¹ Similarly, 3D-printed toy turtles were persistently misidentified as rifles by the targeted AI.⁴²

Some methods can enhance the resilience of DNNs against attacks, like expanding capacity (by incorporating more connections into a DNN) and adversarial training (training DNNs where each input is adjusted by a synthetic adversary before being processed by the network). While these approaches enable DNNs to maintain some level of accuracy in the face of attacks, they are particularly resource-intensive, demanding substantially

⁴⁰ Szegedy et al., 2014, p. 2.

⁴¹ Goodfellow, Shlens and Szegedy, 2014, p. 3.

⁴² Athalye et al., 2018, p. 284.

more storage and computational resources. Consequently, they become highly impractical for everyday usage.⁴³

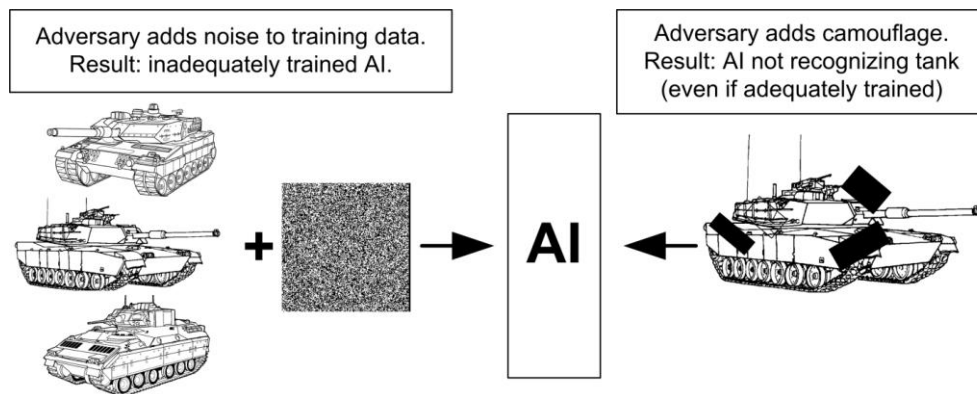
The adversary attacks described above involve modifications to images that are almost imperceptible to the human eye before being presented to the DNN. However, if more significant alterations are applied (physical adversarial perturbations), the outcomes become even more striking. This relates to the previously discussed ability to deceive image recognition models, as numerous studies have shown the effects of alterations that the human brain notices but is not deceived by them, while AI algorithms struggle to interpret them accurately. These studies demonstrate that even by adding small stickers to the surface of an object that the attacker seeks to conceal (e.g., a military vehicle) a significant number of misidentifications ensue.⁴⁴ Equally vulnerable are today's commercially available autonomous driving models that can be easily disguised as changes to traffic signs and fake obstacles by malicious attackers.⁴⁵ The placement of counterfeit lane markers is particularly dangerous, as it can easily cause vehicles to veer off their intended path of travel. Adversary attacks have been presented in Figure 1.

⁴³ Gilles, 2020, p. 19.

⁴⁴ Brown et al., 2017, pp. 4-5.

⁴⁵ Eykholt et al., 2018, p. 1626.

Figure 1 Different kinds of adversary attacks: adding noise to training data (left) and using camouflage (right).



Source: original author's work.

Different strategies are being taken into consideration in the literature as responses to adversarial attacks. These countermeasures can be broadly classified into three main categories: 1) gradient masking, which aims to conceal or obscure the gradient information of the classifier, 2) robust optimisation, which involves the re-learning of the parameters of a DNN classifier, and 3) adversarial examples detection, which focuses on identifying adversarial examples and preventing them from being fed into the classifier.⁴⁶ However, considering that the attacker always plays an active role, meaning they are the first to discover the new methods of provoking false detections to which the defending side must then find a response, we can conclude that the advantage lies on their side.

7. The Analysis: Perceived Benefits and Drawbacks of AI-driven Military Systems

Although autonomous, AI-driven military systems such as UAVs, UGVs, unmanned surface vehicles (USVs), and unmanned underwater vehicles (UUVs) have yet to see extensive implementation on battlefields, the potential they hold motivates military leadership to continually push for their accelerated development. This chapter will present a brief analysis,

⁴⁶ Xu et al., 2020, p. 161.

focusing on the major benefits and drawbacks of fully autonomous military systems as they are perceived today.

7.1. Advantages

Reduced Risk to Human Lives: One of the most compelling arguments in favour of autonomous military systems is their ability to minimise the risk to human militaries. By deploying unmanned vehicles and drones, combatants can conduct reconnaissance, surveillance, and even combat operations without endangering soldiers' lives. Autonomous systems can navigate through unsafe terrain, detect and disarm explosives, and engage enemy targets. Autonomous systems can also be utilised for logistical support and supply delivery, further moderating the exposure of human personnel to potential threats.

Enhanced Situational Awareness: Autonomous systems equipped with advanced sensors and surveillance capabilities provide real-time situational awareness to military commanders and personnel. This comprehensive understanding of the battlefield facilitates strategic decision-making while minimising the need for soldiers to physically scout enemy positions or gather intelligence in dangerous areas.

Reduced Psychological Impact: Warfare can have significant psychological effects on soldiers, including post-traumatic stress disorder (PTSD) and other mental health issues. By leveraging autonomous systems for combat and support operations, military forces can potentially reduce the psychological burden on human personnel, sparing them from the trauma associated with direct engagement in conflict.

Humanitarian Considerations: By employing autonomous systems to carry out missions with precision and efficiency, militaries can strive to minimise civilian casualties and collateral damage, thereby upholding the principles of proportionality and distinction in an armed conflict. Autonomous systems can execute missions with minimal deviation from objectives, and their precision is particularly valuable in targeted strikes against high-value targets surrounded by civilians.

The ability to operate 24/7: Unlike human soldiers who require rest and sleep, autonomous systems can operate continuously, with the capacity of providing persistent surveillance and monitoring. This enables militaries to maintain constant vigilance over large areas for extended periods, improving situational awareness and response times.

Cost-Efficiency: While the initial development and procurement costs of autonomous systems can be high, they often prove cost-effective in the long run. Compared to retaining large standing armies or deploying manned aircraft, autonomous systems are more affordable to deploy and maintain, particularly in prolonged conflicts.

7.2. Disadvantages

The Risk of the Autonomous System Executing Incorrect Actions: Perhaps the most significant drawback of autonomous military systems is the risk that they may not function as intended. Despite their precision, autonomous systems are not immune to errors or malfunctions. Software glitches, communication failures, or misinterpretation of data can lead to unintentional consequences, including civilian casualties or friendly fire incidents. The potential for these systems to malfunction raises significant concerns regarding their reliability and safety. In the preceding sections, we have outlined the methods through which our adversaries might intervene and disrupt the AI training process. In such an event, autonomous systems, although designed to target specific objectives with precision, may mistakenly identify and engage non-combatants or civilian infrastructure. Miscommunication, faulty identification algorithms, or inaccurate situational awareness may also lead to friendly fire incidents.

Technical Failures: Just as in case of any other technical object, autonomous systems are also susceptible to technical failures, including hardware malfunctions, software glitches, and sensor errors. These failures may be caused by manufacturing defects, environmental factors, or wear and tear over time, leading to disruptions in operation and potential mission failure. Accessing and servicing autonomous systems deployed in remote or hostile environments can pose logistical challenges, potentially leading to delays in maintenance and reduced system availability. On the other hand, poor reliability erodes trust and confidence in autonomous systems among operators, commanders, and stakeholders. Concerns about the system's ability to perform reliably under operational conditions may lead to hesitancy in relying on autonomous capabilities, resulting in a reluctance to fully integrate these systems into military operations.

Ethical and Moral Concerns: Concerns about accountability, decision-making ethics, and the potential for autonomous weapons to violate international humanitarian law raise profound moral questions. The lack of

human oversight in critical decision-making processes can lead to unintentional consequences and ethical breaches.


Lack of Emotional Intelligence and Contextual Understanding: Autonomous systems lack the emotional intelligence and contextual understanding of human soldiers. They may struggle to interpret complex social and cultural dynamics, leading to misjudgements or inappropriate responses in sensitive situations. Additionally, the absence of human intuition and empathy can hinder their ability to make nuanced decisions in dynamic and unpredictable environments.

Legal and Regulatory Challenges: The existing legal frameworks governing the use of autonomous vehicles and weapons are insufficient to address the complex challenges autonomous systems pose. Questions regarding accountability, liability, and compliance with international humanitarian law remain unresolved. Establishing clear regulations and norms for the use of autonomous military systems is essential to mitigate the risks associated with their deployment.

7.3. Conclusion of the Analysis

The preceding comparison clearly illustrates the numerous benefits of autonomous systems, with the greatest one certainly being the potential to save the lives of soldiers and civilians in war zones. Considering these arguments, the implementation of AI-driven systems, as swiftly and extensively as possible, enjoys almost unquestionable support. However, what alters the conclusions of the analysis is the risk that autonomous systems may fail to fulfil their mission or even commit errors so severe that they could endanger friendly troops and civilians (Figure 2).

Figure 2 The malfunctioning of a Figure 1: Different kinds of adversary attacks: adding noise to training data (left) and using camouflage (right). As a result of this threat, we believe that the deployment of fully autonomous systems is still premature, at least until issues stemming from sensor errors, enemy electronic warfare, and insufficiently robust AI models are addressed.

Benefits	Drawbacks
1. Saves lives 2. Situational awareness 3. Humanitarian benefits ... (etc.)	1. Possibility of malfunction...  <div style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 80%;"> Critical factor: nullifies all the operational advantages of autonomous systems </div>

Source: original author's work.

Several authors maintain that autonomous weapons need to be used along with intelligible human control to comply with legal and ethical norms – in other words, the use of weapons without meaningful human control should be prohibited. Fully autonomous weapons systems do not allow a human to make a legal and moral judgment as to whether the effects of an attack are acceptable. A treaty that would restrict the use of autonomous military systems should not be built around specific existing technologies but rather based on the idea of how technology may evolve and how it could be used in the future.

Controlling lethal autonomous weapons systems (LAWS) is imperative to ensure adherence to international law, particularly the principles of distinction, proportionality, and precautions in attacks as delineated by International Humanitarian Law (IHL). Human judgment plays a pivotal role (and should not be excluded from the decision-making chain) in ensuring that the potential deployment of LAWS is consistent with

international legal norms and IHL standards. Consequently, there is a critical need for maintaining and enhancing human-machine interaction, where human decision-making continues to hold superiority over decisions made exclusively by AI.

8. Summary

In this paper, we have presented an assessment of the development of disruptive technologies. These technologies vary in terms of their capabilities, acceptance, and dissemination. Using unmanned aerial vehicles (UAVs) and unmanned ground vehicles (UGVs) as examples, the assessment reveals that UAVs have already established themselves as widely adopted, high-capability technology, while UGVs are still searching for their place within global armed forces.

Moreover, the acceptance and applicability of AI within military systems have been thoroughly assessed. Despite considerable progress in the processing of images and real-time video transmissions, the potential for the misidentification of observed objects remains significant. Granting complete autonomy to current AI-driven systems could also entail a notable risk of inadvertent engagement with civilian or neutral targets. Such occurrences may arise from the absence of adequate sensors or models, or as a result of adversary attacks.

The implications of the aforementioned errors in AI-powered military systems diverge in severity, though none of these can be dismissed as insignificant. For example, AI may incorrectly classify an enemy vehicle or weapon, leading to the selection of inappropriate weaponry or tactical manoeuvres. Additionally, mistaking a friendly vehicle for an adversary could result in incidents of friendly fire and fratricide. In view of the attained capabilities and vulnerability to adversary attacks, it currently appears unfeasible for AI to effectively monitor the movements of multiple entities and swift changes on the battlefield while maintaining the requisite high level of situational awareness. If granted complete autonomy, AI-driven military systems would need to accurately and flawlessly distinguish between friendly troops, enemy combatants, and unarmed civilians. AI should be able to discern whether a person is carrying a weapon or any other item and adjust its responses accordingly, with only the highest level of reliability deemed acceptable.

Considering the stated factors, further advancement in manned-unmanned teaming (MUM-T) is predictable. This concept involves a team where the human-operated unit plays a pivotal role, with AI-driven units providing support and protection. These AI units will likely gain more autonomy and take on complex tasks over time, but the central unit will always remain under human control. The MUM-T approach is evolving towards “human-on-the-loop” supervised autonomy, where AI units manage routine tasks while humans make critical decisions. This trend is expected to persist for years or decades, with thorough testing and a legal framework required to ensure safety and compliance with international humanitarian law.

In the final chapter, an analysis was conducted regarding the advantages and disadvantages of fully autonomous systems. Arguments supporting the potential to save the lives of soldiers and civilians serve as the primary motivation for the eventual deployment of such technical units, ideally in significant numbers. However, numerous still-unresolved issues, ranging from hardware and software imperfections to insufficient resilience against enemy attacks, warrant caution. With the declining number of young people willing to enlist in the military, it is almost certain that autonomous systems will eventually assume a significant share of tasks currently reliant on human soldiers. Nevertheless, insistence on such a fundamental transition must be tempered until the aforementioned issues have been addressed, as unsuccessful experiments will be paid for in blood and human lives.

Bibliography

- [1] Athalye, A., Engstrom, L., Ilyas, A., Kwok, K. (2018) ‘Synthesizing Robust Adversarial Examples’, in Dy, J., Krause, A. (eds) *Proceedings of the 35th International Conference on Machine Learning. PMLR (Proceedings of Machine Learning Research)*, pp. 284–293. [Online]. Available at: <https://proceedings.mlr.press/v80/athalye18b.html> (Accessed: 18 October 2023).
- [2] Bansal, M. A., Sharma, D. R. Kathuria, D. M. (2022) ‘A systematic review on data scarcity problem in deep learning: solution and applications’, *ACM Computing Surveys (CSUR)*, 54(10s), pp. 1–29; <https://doi.org/10.1145/3502287>.
- [3] Bartulović, V., Trzun, Z., Hoić, M. (2023) ‘Use of Unmanned Aerial Vehicles in Support of Artillery Operations’, *Strategos*, 7(1), pp. 71–92.
- [4] Bengio, Y., Lecun, Y. Hinton, G. (2021) ‘Deep learning for AI’, *Communications of the ACM*, 64(7), pp. 58–65; <https://doi.org/10.1145/3448250>.
- [5] Brown, T., Mané, D., Roy, A., Abadi, M., Gilmer, J. (2017) ‘Adversarial Patch’. arXiv:1712.09665; <https://doi.org/10.48550/arXiv.1712.09665>.
- [6] Carleo, G., Cirac, I., Cranmer, K., Daudet, L., Schuld, M., Tishby, N., Vogt-Maranto, L., Zdeborová, L. (2019) ‘Machine learning and the physical sciences’, *Reviews of Modern Physics*, 91(4), pp. (045002)1–39; <https://doi.org/10.1103/RevModPhys.91.045002>.
- [7] Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C. (2018) ‘Robust Physical-World Attacks on Deep Learning Visual Classification’, in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 1625–1634; <https://doi.org/10.1109/CVPR.2018.00175>.

-
- [8] Feldman, P., Dant, A. Massey, A. (2019) '*Integrating artificial intelligence into weapon systems*', arXiv preprint arXiv:1905.03899 [Preprint].
 - [9] Gilles, J. (2020) *The lottery ticket hypothesis in an adversarial setting*. Massachusetts: Massachusetts Institute of Technology.
 - [10] Gong, Z., Wang, W. (2023) 'Adversarial and clean data are not twins', *Proceedings of the Sixth International Workshop on Exploiting Artificial Intelligence Techniques for Data Management*, pp. 1–5; <https://doi.org/10.1145/3593078.3593935>.
 - [11] Goodfellow, I. J., Shlens, J., Szegedy, C. (2014) 'Explaining and Harnessing Adversarial Examples', *CoRR*, abs/1412.6; <https://doi.org/10.48550/arXiv.1412.6572>.
 - [12] Gupta, S., Gupta, A. (2019) 'Dealing with noise problem in machine learning data-sets: A systematic review', *Procedia Computer Science*, 161, pp. 466–474; <https://doi.org/10.1016/j.procs.2019.11.146>.
 - [13] Haider, A. (2021) 'Introduction', in Willis, M., Haider, A. (eds) *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. Kalkar, Germany: Joint Air Power Competence Centre, pp. 14–15; https://doi.org/10.1007/978-3-030-67341-3_1.
 - [14] Janiesch, C., Zschech, P., Heinrich, K. (2021) 'Machine learning and deep learning', *Electronic Markets*, 31(3), pp. 685–695; <https://doi.org/10.1007/s12525-021-00475-2>.
 - [15] Janssen, M., Brous, P., Estevez, E., Barbosa, L. E., Janowski, T. (2020) 'Data governance: Organizing data for trustworthy Artificial Intelligence', *Government information quarterly*, 37(3), 101493; <https://doi.org/10.1016/j.giq.2020.101493>.
 - [16] Kratky, M., Minarik, V., Sustr, M., Ivan, J. (2020) 'Electronic Warfare Methods Combatting UAVs', *Advances in Science, Technology and Engineering Systems Journal*, 5(6), pp. 447–454; <https://doi.org/10.25046/aj050653>.

- [17] Krishnan, A. (2009) *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Surrey, UK: Ashgate Publishing Limited.
- [18] Kunertova, D. (2021) 'European Drone Clubs Stall Strategic Autonomy', *CSS Policy Perspectives*, 9(5), pp. 1-4.
- [19] Kunertova, D. (2022) 'The Ukraine Drone Effect on European Militaries', *CSS Policy Perspectives*, 10(15), pp. 1-4; <https://doi.org/10.3929/ethz-b-000584078>.
- [20] Lee, J., Jeon, S., Park, Y., Chung, J., Jeong, D. (2023) 'A Forensic Methodology for Detecting Image Manipulations', arXiv preprint arXiv:2308.04723 [Preprint].
- [21] Li, Z., Liu, F., Yang, W., Peng, P., Zhou, J. (2021) 'A survey of convolutional neural networks: analysis, applications, and prospects', *IEEE transactions on neural networks and learning systems*, 33(12), pp. 6999–7019; <https://doi.org/10.1109/TNNLS.2021.3084827>.
- [22] McDermott, R. (2017) *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. Talinn: International Centre for Defence and Security.
- [23] Monte, L. Del (2018) *Genius Weapons*. New York: Prometheus Books.
- [24] Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., Grossman, D. (2020) *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. Santa Monica, CA: RAND Corporation, <https://doi.org/10.7249/RR3139-1>.
- [25] Mu, R., Zeng, X. (2019) 'A review of deep learning research', *KSII Transactions on Internet and Information Systems (TIIS)*, 13(4), pp. 1738–1764; <https://doi.org/10.3837/tiis.2019.04.001>.

-
- [26] Ntoutsis, E., Fafalios, P., Gadiraju, U., Iosifidis, V., Nejd, W., Vidal, M.-E., Ruggieri, S., Turini, F., Papadopoulos, S., Krasanakis, E., Kompatsiaris, I., Kinder-Kurlanda, K., Wagner, C., Karimi, F., Fernandez, M., Alani, H., Berendt, B., Kruegel, T., Heinze, C., Broelemann, K., Kasneci, G., Tiropanis, T., Staab, S. (2020) 'Bias in data-driven artificial intelligence systems—An introductory survey', *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 10(3), p. e1356; <https://doi.org/10.1002/widm.1356>.
- [27] Rodrigues, R. (2020) 'Legal and human rights issues of AI: Gaps, challenges and vulnerabilities', *Journal of Responsible Technology*, 4, p. 100005; <https://doi.org/10.1016/j.jrt.2020.100005>.
- [28] Semendiai, S., Tkach, Y., Shelest, M., Korchenko, O., Ziubina, R., Veselska, O. (2023) 'Improving the Efficiency of UAV Communication Channels in the Context of Electronic Warfare', *International Journal of Electronics and Telecommunications*, 69(4), pp. 727–732; <https://doi.org/10.24425/ijet.2023.147694>.
- [29] Smith, P. (2020) *Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy*. American Security Project.
- [30] Surden, H. (2021) 'Machine learning and law: An overview', *Research Handbook on Big Data Law*, pp. 171–184; <https://doi.org/10.4337/9781788972826.00014>.
- [31] Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., Fergus, R. (2014) 'Intriguing properties of neural networks', ArXiv [Preprint].
- [32] Tufail, S., Batool, S., Sarwat, A.I. (2021) 'False data injection impact analysis in AI-based smart grid', *SoutheastCon 2021*. pp. 1–7; <https://doi.org/10.1109/SoutheastCon45413.2021.9401940>.

-
- [33] Wang, W., Siau, K. (2019) ‘Artificial intelligence, machine learning, automation, robotics, future of work and future of humanity: A review and research agenda’, *Journal of Database Management (JDM)*, 30(1), pp. 61–79; <https://doi.org/10.4018/JDM.2019010104>.
- [34] Watts, B. (2013) *The Evolution Of Precision Strike*. Washington DC: Center for Strategic and Budgetary Assessments.
- [35] Wróbel, K. (2021) ‘Searching for the origins of the myth: 80% human error impact on maritime safety’, *Reliability Engineering & System Safety*, 216; <https://doi.org/10.1016/j.ress.2021.107942>.
- [36] Xiong, H., Pandey, G., Steinbach, M., Kumar, V. (2006) ‘Enhancing data analysis with noise removal’, *IEEE transactions on knowledge and data engineering*, 18(3), pp. 304–319; <https://doi.org/10.1109/TKDE.2006.46>.
- [37] Xu, H., Ma, Y., Liu, H.-C., Deb, D., Liu, H., Tang, J.-L., Jain, A. K. (2020) ‘Adversarial attacks and defenses in images, graphs and text: A review’, *International journal of automation and computing*, 17, pp. 151–178.
- [38] Zhang, Z., Li, M., Chang, M.-C. (2024) ‘A New Benchmark and Model for Challenging Image Manipulation Detection’, *Proceedings of the AAAI Conference on Artificial Intelligence*, 38(7), pp. 7405–7413; <https://doi.org/10.1609/aaai.v38i7.28571>.
- [39] Zhou, X., Xiang, Y., Youmin, Z., Yangyang, L., Xiaoyan, P. (2021) ‘Trajectory Planning and Tracking Strategy Applied to an Unmanned Ground Vehicle in the Presence of Obstacles’, *IEEE Transactions on Automation Science and Engineering*, 18(4), pp. 1575–1589; <https://doi.org/10.1109/TASE.2020.3010887>.

European Integration Studies

ISSN 1588-6735 (Print)

ISSN 3004-2518 (Online)

DOI prefix: 10.46941

Responsible for the publication: Prof. Dr. Csilla Csák, dean

Faculty of Law, University of Miskolc

Published by Faculty of Law, University of Miskolc

Technical editor: Andrea Jánosi, Csenge Halász, Gergely Cseh-Zelina