

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).