European Integration Studies, Volume 20, Number 2 (2024), pp. 67-86.
https://doi.org/10.46941/2024.2.3

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 19$^{th}$ century, it meant "manipulating society"; only in the second half of the 20$^{th}$ 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 as[9] 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 encompasses 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 operation[28] 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.