IV.6

NEW TYPES OF WARFARE: INFORMATION AND HYBRID WARFARE

Chapter 16

Information Warfare Tactics and Techniques

Stjepan Groš

Abstract

Information warfare, disinformation, fake news, and similar terms are frequently used in public discourse. It is clear from real-world examples that these concepts represent a substantial danger for democratic countries, polarise societies as regards public health, and generally prevent rational and informed discussion. Yet, combating disinformation proves very difficult. Something must be done, but the question is what. The premise of this chapter is that we cannot counter disinformation if we do not agree on what we are fighting against; that is, we cannot do something if we do not know what the adversaries are using against us. In cybersecurity, databases of tactics and techniques of adversaries' behaviour have proved very useful for defence. Knowing about different types of attackers, their motives, and capabilities has also proved beneficial. Therefore, we are set to replicate this success in the case of information warfare and information operations. To achieve these goals, we review the terminology and define information warfare in a narrow sense and then discuss information operations, their relation to military domains and information space, and the domains in which information operations are run. In doing so, we determine that information operations are intertwined with and appear in all military domains. The core part of this chapter lists the tactics and techniques adversaries use for information operations. We then review the logistics support adversaries might use for information operations; moreover, we define threat sources and threat actors and classify them based on their motivations and capabilities. Finally, we map the operations run during Operation Denver to the tactics and techniques presented in this chapter to illustrate their use.

Stjepan Groš (2024) 'Information Warfare Tactics and Techniques'. In: Katarzyna Zombory – János Ede 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,* pp. 701–754. Miskolc–Budapest, Central European Academic Publishing.

https://doi.org/10.54237/profnet.2024.zkjeszcodef_16

Keywords: warfare, information warfare, information operations, cyber warfare, tactics, technics, procedures, mitre att&ck, operation Denver

1. Introduction

In today's hyperconnected world, information flows faster than ever, reaches more people than ever, and allows everyone to express their opinion that can be heard by a large audience. This state of affairs has brought many advantages and improvements, such as an easier and more enjoyable life, better and faster scientific achievements, faster industrial development, and more innovative products and services. These are just some examples of the many positive changes this new age has brought to humanity.

Significant advances are also being made in the field of machine learning (ML), specifically large language models (LLMs). ChatGPT was made publicly available on 30 November 2022, and it showed impressive performance while being available to everyone with an internet connection. This caught the eye of the mainstream media and the general public. This undoubtfully revolutionised ChatGPT's application in different aspects of everyday work and caused a huge societal shift towards this new technology.

Yet, all these advancements have a dark side that threatens the society in new – yet unexplored – ways. Some of the issues we face are new. For example, due to the rapid flow of information, we have less time to process it in an appropriate way, and thus we are more susceptible to low-quality information. However, many of the issues have been present in the society in one form or other for decades. What is new in this case is that the advancement of technology allows more people to be targeted, faster than ever, with more information than ever – and not just with information but also unverified rumours, uninformed opinions, and plain malicious information. This creates social problems that might impact even national security. In addition, what was once only a capability of nation states and their secret services is now in the reach of less resourceful groups, even individuals, which further exacerbates the already dire situation.

An example of how this situation can escalate is the manipulation witnessed during the 2016 United States (US) presidential election, which arguably changed the course of the election. Other examples include false information spread about COVID-19, because of which more people died than would have without such false information. Thus, problems created by such technological development threaten human lives and the core of today's society – its democratic processes. However, this is only the tip of the iceberg.

In October 2021, a workshop was organised to assess how new technology in the form of LLMs will impact the society and individuals through so-called influence operations.[1] The workshop gathered 30 experts from the fields of artificial intelligence (AI), influence operations, and policy analysis. The workshop concluded that there are significant changes ahead of us; however, some uncertainties were present at that time, which prevented the workshop from drawing more specific conclusions.

In essence, we are caught between fast technology development on the one hand and the slow changes in individuals and even slower changes in the society on the other. Added to this are the limited information processing capabilities of individuals, not to mention that processing is prone to errors due to human nature. It is inevitable that individuals and the society will have to change, but even if we know what changes we need to make, their implementation will take time. To conclude, as the saying goes, we live in interesting times, and we need to understand this development and the tools and techniques that will allow us to counter the negative effects of development. At the same time, we must not prevent the benefits to be utilized and developed further.

This chapter tries to tackle the negative effects of technological development by structuring the field in a way that makes thinking and analysing the current and future states of affairs easier as well as more organised, effective, and efficient. Emphasis is placed on information flow and, more specifically, on information warfare, which we think is concerned with information flow – as we see later in this chapter. However, be aware that this is only a part of the whole story. There are many other aspects to be considered, such as the psychological and cognitive aspects (warfare) as well as propaganda, which are not dealt with in this chapter. As already mentioned, we are tackling a very complex problem, and this chapter takes just a small step in finding its solution.

To organise the field, this chapter focusses on developments in cybersecurity that turned out to be useful and were consequently used frequently – specifically, the "cyber kill chain"[2] and "MITRE ATT&CK pattern".[3] Cyber kill chain is a model of the adversary's behaviour while attacking a target. The idea is that if we know how the attacker behaves, we can recognise him sooner and stop him by disrupting his processes during an attack. This idea of the cyber kill chain is taken from military sciences where the kill chain has been used for some time. The other significant development in cybersecurity that influenced this work is the MITRE ATT&CK pattern. The MITRE ATT&CK pattern aims to be a public knowledge database that contains information about all known attackers and their tactics, techniques, and sub-techniques. The difference between the cyber kill chain (or modelling of the attacker's behaviour) and the MITRE ATT&CK pattern is that the latter is not a model but a union of all models. Many tools are being produced to detect and contain attackers that heavily rely on the MITRE ATT&CK pattern.

[1] Goldstein, 2023.

[2] Hutchins et al., 2011.

[3] Strom et al., 2020; MITRE ATT&CK, no date.

One goal of this chapter is to try to create a database similar to the MITRE ATT&CK pattern for disinformation campaigns. Having such a database can open up new possibilities for studying and understanding adversaries' behaviour. Namely, it would be possible to compare adversaries and predict their behaviour, which in turn might help with countering them. Moreover, it could be possible to foresee behaviour that was not yet utilised but could be in the future.

Finally, one additional important inspiration comes from information security, a branch of security used in companies that deals with the protection of companies' information resources. One interesting fact about information security is that it does not deal with the content of what it is protecting. The content falls within the realm of business and, as such, is taken for granted by information security practitioners. Another interesting fact about information security is that it deals with information in any form and not only digital information that is stored in some computer or transmitted via a network. These facts inspired us to treat information operations as not being strictly related to information and communication technologies (even though this is their most frequent form today). More importantly, this allowed us to better distinguish between information warfare and other forms of warfare.

This chapter has additional goals. The main goal is to introduce tactics and techniques that can be used by adversaries when spreading disinformation. Because techniques depend on technical elements of the environment in which everything happens, we also review the important technical elements of this environment.

This chapter is structured as follows. First, Section 2 Background reviews the basic terminology used throughout the chapter. Then, Section 3 Information Operations discusses the central topic of this chapter as well as some connected terms in more detail. In this section, we introduce the information lifecycle, which forms the basis for a set of tactical steps. This chapter's main contribution is discussed in Section 4 Tactics and Techniques, which lists the tactics and some techniques for each tactic. In several cases, we delve into more detail in the form of sub-techniques. Certain support services for spreading disinformation are created potentially independently and are used on an as-needed basis. Some of these services are described in Section 5 Logistics Support. Moreover, we analyse the threat actors and threat sources in Section 6 Threat Sources and Actors, as it is very important to identify the adversary targeting us. Finally, in Section 7 Example of the Application of Tactics and Techniques, we present a concrete example where we map one information operation to the tactics and techniques we described. The chapter ends with conclusions and future work in Section 8 Conclusions.

2. Background

As stated in the introduction, we are concerned primarily with information warfare. Therefore, in this chapter, we tackle the term “information warfare” as well as other related terms such as “information operations”. Since a lot is happening in this and other related fields, a lot of materials are published on this topic on almost a daily basis; consequently, there is a lot of misuse of different terms for various reasons. Here, we are trying to organise and relate different terms in a way that will allow us to proceed into more detail without being distracted by the interrelation between or confusion regarding the different terminology used (or abused) in the literature.

2.1. Warfare and Information Warfare

We start with the definition of the term “warfare”, and accordingly, we define the term “information warfare”. The term “warfare” is a more technical rather than legal term, and it refers to the activity of fighting a war, including the “weapons and methods” that are used. In other words, warfare encompasses “tactics and techniques” available for use in a war. The exact set of weapons and methods used determines specific types and subtypes of warfare, such as cyberwarfare, space warfare, ground warfare, naval warfare, aerial warfare, information warfare, and hybrid warfare.

It is important to note that even though the term “warfare” is associated with war and it is implicitly assumed that it is used in war by a military, “warfare” can also be used by other groups and individuals. The key to understand this is that the tactics and techniques of traditional warfare require a lot of resources and are thus mainly accessible to militaries. On the other hand, cyberwarfare and information warfare, which make extensive use of information and communications technology, are available to a much wider audience with significantly lower resources.

Additionally, anyone can try to use the tactics and techniques of classical warfare, but because of the characteristics and restrictions of the physical world, as well as restricted resources, the effect is weak and restricted to a small area. On the contrary, few individuals can achieve a much bigger effect by using information warfare compared to that using classical weapons, mainly because of the information space and its characteristics, as well as information technology. That is, thanks to the Internet, everyone can reach everyone else throughout the world. Furthermore, by using readily available services, a much wider audience can be reached with a limited set of resources, such as by writing a blog or publishing videos on YouTube.

This reachability and availability have an important implication – potentially many more actors can engage in these activities, all of whom have varying degrees of resources and motives. This point must be considered because it is a significant departure from the things as they used to be.

In conclusion, in this chapter, "warfare" refers to tactics and techniques used to achieve the required end state. Depending on the set of tactics and techniques, we talk about different forms of warfare. One goal of this chapter is to define tactics and techniques that compose information warfare. More specifically, information warfare involves tactics and techniques used to deliver information (disinformation) to specific targets.

2.2. Related Forms of Warfare

Besides information warfare, some other closely related but not identical forms of warfare include psychological warfare, cognitive warfare, and propaganda warfare. There could be other forms as well, because it is fashionable to call something "warfare," as it raises the level of seriousness. An example is "disinformation warfare" whose validity is debatable, but many other such terms appear in the literature and especially on the Internet. Yet, the three terms psychological, cognitive, and propaganda warfare are important; the terms psychological and propaganda warfare have been known for almost a century and used much longer than that. All these types of warfare, along with information warfare, target the cognitive and psychological processes of human beings, and that is why we consider them in depth.

Human beings can be targeted in different ways in the context of information and related warfare, all ending in a human being thinking or feeling something. To make a distinction, feelings fall within the realm of psychology, while thinking is a cognitive process. The thinking and feeling of human beings can be influenced by information delivered to and received by them, which is then interpreted. Alternatively, individuals can be influenced by direct physical contact, which is also a form of information delivery.

It is not so easy to discern the two influences – that is, information received and physical contact – but here are three examples to better illustrate the difference. First, persons being targeted are given leaflets with text describing how superior their opponent is. Second, persons being targeted see enemy planes flying and demonstrating their superior performance. Finally, persons being targeted learn about the building of an artificial island, which is by itself difficult to maintain and is of questionable (classical) military value.[4]

The first example is clearly based on information received by the targeted persons. The second example is a combination of physical activity (airplanes manoeuvring) and information received (planes through sight). We classify such activity as direct physical contact since the information itself was directly perceived by the targeted persons, without employing any means of conveying information, such as the Internet, newspaper, and radio. The third example is based on information received, because few people have the ability to go and see the island for themselves;

[4] Southerland, 2016.

that is, the majority will read somewhere about such an island. Thus, we classify this example as information received.

Based on these examples, we can define the two influences, information received and physical contact, as follows: Influence by information received is any indirect means of impacting people, where people did not directly see or feel the event that occurred but somehow received information about the event. Physical contact (or experience) allows a person to directly see or feel something and accordingly create an opinion or enter a psychological state.

An additional important factor is that humans have basic instincts and higher-level thought processes. These two concepts are interrelated but can be influenced separately. Moreover, because of a disconnection between the two, one can be harmed without the other being harmed. For example, a demonstration of force might induce a feeling of fear in a person, even though a rational approach (if used) can lead to the conclusion that this demonstration is actually irrelevant. Cases with such a disconnect between basic instincts and higher-level thought processes are interesting and important; however, they can be addressed by future research, as they are outside the scope of this chapter. Rather, we focus on the levels of the human mind, feelings, and cognitive processes. Accordingly, we compare different warfare types and their connection to information warfare.

Psychological and cognitive warfare differ in the same way that psychology and cognitive psychology do. Psychology, in the broad sense, studies the mind and behaviour, but there are different schools of thought. Since psychological warfare as a field of study originated in the 1940s,[5] it originally used methods and approaches from behavioural psychology. As psychology progressed as a scientific discipline, so did psychological warfare. Cognitive psychology is a school of thought within psychology that emerged in the 1960s. We can conclude that while psychological warfare in the narrow sense and cognitive warfare differ in terms of methods and approaches, both try to influence the human mind and behaviour. Moreover, psychological warfare in the broad sense encompasses any means to influence the mind and behaviour; thus, it involves both psychological warfare in the narrow sense and cognitive warfare.

In this chapter, we treat information warfare as tactics and techniques to convey information to humans; however, information warfare itself does not deal with "what" is necessary to convey to humans to achieve a desired psychological state. This falls within the realm of psychological and cognitive warfare. In other words, we are not interested in the psychological and cognitive aspects of spreading false information. Note that, in the context of psychological and cognitive warfare, physical experience can be used to achieve the desired ends, which is obviously not in the realm of information warfare.

One important type of warfare used today is "hybrid warfare", which is thoroughly analysed in the next chapter from the legal perspective. There is no agreed

[5] Farago, 1941.

upon definition of what exactly is hybrid warfare. Considering the definition of warfare in this chapter, we treat hybrid warfare as a set of tactics and techniques that are taken from other types of warfare – psychological, information, cognitive, cyber, and propaganda – and from more traditional ones, such as asymmetric, chemical, electronic, and drone warfare. The question of which tactics and techniques might be assumed under hybrid warfare should be answered empirically by analysing the hybrid operations (if we could agree on what hybrid operations are) and taking observed tactics and techniques into the set of tactics and techniques that define hybrid warfare. This endeavour is obviously very broad and uncertain. Therefore, this chapter does not analyse hybrid warfare but instead information warfare. This is because information warfare is a narrower area of activity and thus more manageable; at the same time, principles used for information warfare can also be used for the analysis of hybrid warfare.

Finally, we also mention "propaganda",[6] a term closely related to information warfare. Propaganda, unlike information warfare, has a fixed target – the general public – and the goal of influencing public opinion and making it favourable to whoever is utilising the propaganda. To achieve its end-state, propaganda combines various aspects of psychological, cognitive, and information warfare. For that reason, we see propaganda only as a special case of these three warfare types.

2.3. War

The concept of war is very important and interesting to consider. It is defined as follows:[7]

> War – in terms of international law – is a legal condition, a state of armed conflict between different states or nations within a state. Whether a state is at war – legally speaking – depends upon the status of opponents, e.g., whether they are states, nations, peoples, belligerents, or insurgents. Not every act of hostility or use of armed force necessarily creates a war in terms of international law, but if it does, it produces legal consequences for the parties and for the entire international community. The legal consequences are determined primarily in the UN Charter.

This definition is very useful in the case of conflicts between states when both sides' armies are engaged. However, the definition does not tell much about what differentiates war from non-war states; it only shows that certain legal conditions exist in the case of war that do not exist in non-war states. Additionally, much of international law is dedicated to the rules for how war is fought to prevent unnecessary loss of human lives or unnecessary destruction.

[6] Smith, 2024.

[7] Dinstein, 2011.

Yet, the second part of the 20th century showed that in the modern world, asymmetric and other forms of conflicts are much more frequent, in which one side is so dominant that the other side avoids direct conflict. This complicates the state of affairs because it is not war in the classical sense.

Cyberwar is especially interesting in this context. There is a lot of debate about whether cyberwar is possible[8] and what could be achieved by it. Armies around the world declared cyberspace the fifth domain of war and started establishing separate branches just to fight the cyberwar. Nevertheless, the Russian aggression in Ukraine in 2022 brought a lot of surprises in terms of warfare in general and cyberwarfare and information warfare in particular. It turned out that the only way of achieving decisive gains was classical warfare and not cyberwarfare. This does not mean that no cyberwarfare occurs but that classical military actions are more influential at this point.

This development has impacted the use of information warfare and all activities in the information space. Namely, the results of information warfare activities can be expected in the medium to long term. Thus, if someone is preparing for war, activities in the information space must start much sooner and prepare the ground for activities during the war. Russia itself imposed strict control of its information space along with the repressive measures it has applied for a long time. This resulted in the absence of almost any opposition to its war efforts – at least publicly. This is interesting for at least two reasons. First, it creates an asymmetric situation in which information flows freely on one side of the conflict, while there is no free flow of information on the other side. The consequences for the spread of disinformation is obvious. Disinformation spreads easily on the side with the free flow of information, and Russia has used this intensively.

As regards the definition of war, it used to mean that nation states were on opposing ends. Today, for various reasons, this is not the case anymore. Apart from the asymmetric conflicts mentioned above, development of technology empowered additional groups to engage with the nation state or with a part of it, making it a national security problem. This has additional consequences as well. Therefore, resources invested in conflict are not a good measure to assess whether it is a war or not. In modern warfare, because of technological developments, it is possible to achieve significant damage with only a small amount of resources invested by the adversary.

2.4. Information Operations

War is an activity occurring on operational and tactical levels that has the goal of achieving or supporting the strategic end-state. The operational level of war connects the strategic end-state with its tactical-level activities; that is, it organises tactical-level activities to achieve the strategic goals. Because one operation might not be enough to achieve the strategic end-state, multiple operations could be run, all

[8] Rid, 2012; Stone, 2013.

of which strive to achieve the same strategic end-state and are collectively called "campaigns".

In the context of information warfare, we are interested in "information operations" and, consequently, "information campaigns". Information operations are activities that organise the tactics and techniques of information warfare to achieve the strategic goals. In this chapter, we use the terms "information operations" and "information warfare" interchangeably; although these terms are not the same formally, it should be clear which term we are referencing from the context.

It is interesting to look at an alternative definition of an information operation, provided by Facebook in its report on abuse of the platform:[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').

This definition is interesting for three reasons. First, it acknowledges that one side of the conflict can be a non-state actor, that is, it could be anyone. It also opens up the possibility that both sides are non-nation states. For example, outside actors try to compromise certain political movements within the country. This will impact the nation state as a whole but nevertheless is not a conflict between the outside actor and the nation state itself. Even though this is an interesting case, we are not interested in such cases in this book. Instead, this book is meant to help policymakers in decision-making regarding information operations. Therefore, we assume that the side suffering from information operations is a nation state or some part of it. Second, this definition explicitly mentions false news and fake accounts, in addition to disinformation traditionally tied with information warfare. This makes the definition appropriate in the context of Facebook but is too restrictive for our case, as we look at a much broader picture. The third reason this definition is interesting is that it enumerates the specific goal of information operations – manipulation of public opinion. We believe this is also too restrictive as the goal of information operations might be to target specific parts of the society, not necessarily those who form or influence public opinion. To conclude, the definition of information operations given by Facebook is a restricted version of our definition.

An additional term used frequently in the literature is "influence operations". We will use the definition given by Rand Corporation for this term:[10]

[9] Weedon, Nuland and Stamos, 2017, p. 5.

[10] Larson et al., 2009, p. 2.

> Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives.

This definition is much broader as it allows the use of not just information warfare but also other means such as diplomatic and even military action. At the same time, it specifically names the US as the actor running influence operations as well as a beneficiary of those operations. Obviously, influence operations, as defined by RAND, overlap with information warfare and information operations, but they are distinct concepts.

Information operations, when executed, are controlled by the "information operation operator". The task of an information operation operator is to coordinate activities, allocate resources, assign tasks, etc. We use the expressions "operator" and "adversary" interchangeably in this chapter, as they have the same meaning.

It is important to be aware that information operations are not something new. They have been conducted for a long time, although the information space used to be significantly different than it is today. An interesting example of an information operation from before the advent of the Internet and information technology is Operation Denver.[11] This operation was conducted by the Soviet Union to convince people in the West that the acquired immunodeficiency syndrome (AIDS) was developed in secret laboratories. This example is significant as it also shows how running such an operation before the Internet was a complicated, long-running process requiring a lot of resources, and thus it was not accessible to many. Such an operation also depended more on luck as many related developments were not under the control of the information operation operator.

2.5. Disinformation

What is interesting in the case of information warfare is the question of what is a weapon. We argue in this chapter that the so-called bullets in such warfare comprise misinformation, disinformation, and malinformation, while the weapons are all the technical means of generating, publishing, and distributing misinformation.

According to the Council of Europe,[12] the terms misinformation, disinformation, and malinformation have the following meanings. "Misinformation" occurs when false information is shared, but no harm is meant, such as a satire taken seriously, typos, and errors. "Disinformation" occurs when false information is knowingly shared to cause harm, such as when fabricated or deliberately manipulated content is designed and shared to mislead. Finally, "malinformation" occurs when genuine information is shared to cause harm, often by moving what was designed to stay

[11] *Operation INFEKTION*, 2024.

[12] Wardle and Derakhshan, 2017.

private into the public sphere, such as deliberate publication or leaking of private information and deliberate changes to the context of genuine content.

Unfortunately, while distinctive, these definitions are hard to apply in practice. First, the case of when disinformation is created and then shared by someone who believes in it is not covered by any of these terms. This case involves unintentional sharing of false information, which is classified as misinformation, but it started as disinformation. The key point is that using these definitions involves determining someone's motive and, more importantly, someone's state of mind, which is extremely difficult. Malinformation, on the other hand, is easy to classify, but the problem is that it might include disinformation as well; this was the case in 2016, when the Democratic National Committee's email leaks also contained disinformation. In that case, it is difficult to say if it is malinformation or disinformation. For this reason, we will use the term disinformation for any false information shared that causes harm to individuals, groups, or the society at large.

As seen in the case of Facebook, the concept of fake news[13] is also used frequently lately.[14] While fake news might be misinformation, it more commonly appears in the form of online disinformation with an added twist of imitating journalistic form to seem more credible. This leads us to the conclusion that fake news, and disinformation in general, have two components: (1) content and (2) form. Content depends on the purpose of disinformation and the target, while form is more a technical issue. We will get back to this distinction when we discuss tactics later in this chapter.

2.6. Data and Information

We should comment on data versus information. Information theory makes a strict distinction between information and data – that is, information is the interpretation of data by a human being. This state of affairs is comparable to information security, which also talks about information but deals with, and protects, data.

Whether this distinction does or does not make sense depends on the definition of information warfare. As seen earlier in this section, information warfare in the broader – and more accepted – sense usually overlaps with psychological and cognitive operations. In that case, it is justified to talk about information. We also have information warfare in the narrower sense, wherein whoever is applying the tactics and techniques of information warfare does not interpret the data – at least not with the intent to answer the question "why". This case is much more nuanced. Nevertheless, because the term "information warfare" is well accepted, we use it in this chapter and do not delve deeper into the question about whether it should be about data.

However, there is one interesting corner case. If an information operation tries to poison the data used to train ML models, then in this case, we are obviously dealing

[13] Gelfert, 2018; Pantazi, Hale and Klein, 2021.

[14] Baptista and Gradim, 2021.

with data and not information. This is just one special case and, as such, does not likely warrant a change in the accepted terminology.

2.7. Tactics, Techniques, and Sub-Techniques

Because one of our goals is to define tactics, techniques, and sub-techniques of information warfare, we must also define the meaning of these terms. One of the best databases for tactics, techniques, and sub-techniques is the MITRE ATT&CK pattern[15] for cyberwarfare. This is likely the only such database for any warfare type, and we use it as a model for building a similar database for information warfare. As already described in Section 1, the MITRE ATT&CK pattern is an extraordinarily successful database used in many situations.

The database is first divided into "tactics". For example, the tactic of "reconnaissance" encompasses all activities by the adversaries to determine as best as possible the potential target they are about to attack. Moreover, the tactic called "initial access" has the goal of entering the target network. Another tactic, "privilege escalation", is utilised while within the target network to gain appropriate privileges. Each of these tactical steps has a specific goal. Currently, there are 14 tactical steps in total, and this number changes over time. The important thing is that attackers do not have to use all the available tactical steps or follow the order listed in the database. As we already mentioned, this is not a model of attack. To conclude, tactics are defined as a reason why something is done,[16] that is, they are the objectives of the adversary.

Each tactic can be utilised in several ways, which are called techniques. Techniques are "how" the technical steps can be achieved. For example, the tactic of "initial entry" can be achieved by either exploiting a public-facing application or phishing. Some techniques can be further decomposed into more specific implementation steps, which are called sub-techniques. In the older versions of the MITRE ATT&CK pattern, they were called procedures, and the whole concept was called "Tactics, Techniques, and Procedures" (TTPs). TTP is a popular and widespread abbreviation for this concept.

The MITRE ATT&CK pattern is useful for two reasons. First, it gives defenders a catalogue of (almost) everything attackers can do (technique) to achieve something (tactic). This is invaluable to plan defences. Second, companies working on defence solutions can use this catalogue of what attackers might do to systematically cover attackers' actions in their defence solutions.

The MITRE ATT&CK pattern is developed based on what has been observed during attacks. TTPs are not the only database available in the MITRE ATT&CK pattern. It also includes a database of threats actors and the tactics and techniques

[15] MITRE ATT&CK, no date.

[16] Strom et al., 2020.

used by each actor. This allows for easier monitoring of threat groups. It also has a database of tools used by threat sources.

It is obvious that having similar databases for information warfare as well could be beneficial. However, the two domains are different, and the tactics and techniques for cyberwarfare cannot be expected to be easily transferred to information warfare. This chapter tries to do just that – identify the tactics and techniques of information warfare. Undoubtfully, this is just a first step, as more work is necessary to develop something for information warfare that is as useful as the MITRE ATT&CK pattern is for cyberwarfare.

2.8. ML, LLMs, and Generative AI

Research on ML is part of the bigger research area of AI. ML has been extremely popular for the past 15 years or so, mainly due to its success stories, not least of which is appearance of ChatGPT at the end of 2022. Even though ChatGPT initiated a new phase in the development and use of ML, ML already showed success in different vision and language processing tasks.

Before going further, it is necessary to provide a brief overview of AI/ML for easier understanding of the rest of this chapter. AI/ML was created for processing information in a way that is as similar as possible to how humans behave and work. Because a lot of important tasks in information warfare are performed by humans, it is obvious that replacing humans with something automated would make things more effective and efficient. Thus, AI/ML is a significant addition to the toolkit already used in information operations, as it opens up significant opportunities to make information operations even more dangerous than they are now.

First, we discuss ML models, specifically the ones based on artificial neural networks (ANNs), which are currently the most successful models. Each ANN model consists of mutually connected basic network elements, which are also connected to the outside world, to both receive data and output results. These basic network elements are called “neurons,” and each connection between two neurons transforms the information (or “signal”) that passes through it by amplifying or attenuating it. This transformation is called a parameter. In its basic form, ANN models are created according to the perception of how the human brain works at its most basic level. To conclude, each ANN model has several neurons connected in some way, and all these connections have parameters that determine what the connection will do when a signal passes through it.

Defining the exact structure of a model is an art, and the creation of different structures and use of experiments to determine which ones behave the best constitute the basic, and the hardest, part of the research in this field. The parameters, on the other hand, are defined through a process called “learning”. The learning takes input data fed into the model, and then parameters are optimised in such a way that the model produces the wanted outputs. This is a very demanding task that requires a huge amount of processing power, and huge quantities of data are also necessary. Compared to the human brain, ANN models are significantly inefficient at learning. After the process of learning is finished, all the connections between neurons have defined values for what they should do with the signals passing through them. The number of parameters in today's state-of-the-art models are in the range of billions. In other words, there are billions of connections between neurons in one ANN model.

After the process of learning finishes, we have a trained model that can be used. Note that there is an option of so-called "pretraining", meaning that someone who creates a model does initial training with huge amounts of data, and then the user must do "finetuning", that is, training using a smaller set of domain-specific data. Even though pretraining widens the number of those who can create their own custom models, it is still resource demanding.

In the case of information operations, we are particularly interested in two classes of ML models: LLMs and deep generative models. LLMs have the specific purpose of manipulating the natural language, while deep generative models are used to create so-called "deepfakes", which are images or videos that show events or persons that do not exist.

Creating an LLM is not an easy task, and it can incur substantial cost.[17] To create an LLM from scratch, the following resources must be available: (1) AI/ML experts who will create and train models; (2) data on which models will be trained and people to collect and purify the data; (3) infrastructure for training and data collection, as well as experts that will build and maintain this infrastructure; (4) management structure to organise and oversee everything; and finally, (5) financial resources to cover operational costs.

Note that there is a plethora of LLMs currently available for different purposes. The key distinction is whether they are proprietary or so-called "open source". Proprietary models are closely guarded by their owners and are either not accessible or accessible only under certain conditions. In any case, such models run on the owner's hardware and are accessed by users via application programming interfaces (APIs) or web browsers. Moreover, the LLMs' parameters and structure are closely guarded business secrets. In general, these models are of better quality, and their prime examples are OpenAI's ChatGPT and Google's Gemini, formerly known as Bard.

Open-source models, on the other hand, are freely available for anyone to use, and there is even a centralised repository of such models.[18] Some of them come remarkably close to proprietary models because of their performance. These models can be downloaded locally and run on a local machine. Although these models require stronger hardware due to their size (number of neurons and parameters), they are still not so inaccessible to someone with enough financial resources.

The accessibility of advanced models, no matter if they are closed- or open-source, represents a significant shift in information warfare. There are already

[17] Musser, 2023.

[18] Hugging Face, no date.

known cases of attackers using LLMs and generative deep models either to increase the success of their attacks or as a tool of attack.[19] Research also shows that the Internet already has abundant LLM-generated content,[20] and deep fakes are already used for disinformation.[21]

2.9. Related Work

This work is certainly not the first one to use the MITRE ATT&CK pattern as a model to create a framework for information warfare. The most advanced such framework is the Disinformation Analysis and Risk Management (DISARM) framework.[22] Because DISARM is the most comprehensive framework and is also supported by the European Union and North Atlantic Treaty Organization (NATO), we compare our framework to DISARM.

The motive for creating DISARM was the same as ours: to organise and structure information operations so that defenders can be more efficient in detecting, predicting, and combating information operations. However, DISARM is much broader in scope and more encompassing.

The DISARM framework tries to combine the tactics and techniques of all warfare types enumerated in Section 2.2. For that reason, it is a flat and very complex model. However, our approach is completely different. We accept that there are different forms of warfare, each with its own specifics, which require expertise that a single person cannot have. Furthermore, we believe these forms can interact in different ways. Therefore, we tried to keep all these warfare types separate while proposing a way in which they interact by utilising the “uses” and “used by” verbs. Because this chapter emphasises information warfare, we placed it in the centre and analysed how other warfare types can use or be used by it. Thus, we created a system that has a limited set of tactics and techniques, which can be combined in complex ways. The DISARM framework, on the other hand, simplifies interactions between different warfare types by combining them and imposing a rigid structure on the result.

The DISARM framework was tested by Newman et. al. for its suitability for rapid adoption by strategic communications practitioners along with its credibility among specialist foreign information manipulation and interference threat analysts.[23] The result was positive and found DISARM to be applicable and well suited for these purposes. Operation Ghostwriter was used for testing. However, the main narrative of this operation is the heavy use of offensive cyber-capabilities to spread disinformation. We find this to be overly restrictive, as cyberoperations are not the only means of spreading disinformation. As described in Section 5.5, we consider

[19] Mascellino, 2023; Hill, 2023; Chilton, 2023.

[20] Cantor, 2023; Ryan-Mosley, 2023.

[21] Satariano and Mozur, 2023; Philmlee, 2023.

[22] *DISARM Foundation*, 2024; Terp and Breuer, 2022; López, Pastor-Galindo and Ruipérez-Valiente, 2024.

[23] Newman, 2022.

cyberoperations as a means to achieve a specific position from which some goals can be achieved. As such, cyberoperations are opaque from the information warfare perspective and encapsulate complex processes that are dealt with by cybersecurity. This, again, is in line with our approach of not grouping different warfare types into a single set of tactics and techniques.

One additional restriction of the DISARM framework, which we do not have, is that it is restricted to online means of managing disinformation.[24] While most of today's information operations are conducted in the online world, traditional means are still used, especially when threat actors are nation states.

In conclusion, the DISARM framework uses a different approach to model information operations, and we offer an alternative approach. However, because DISARM is more developed with the investment of multiple manhours, it can be source of inspiration for further development of the model presented in this chapter.

Another related work is a paper presented at the 2023 Network and Distributed System Security Symposium by Shujaat et al.[25] This work deals with threats and the tactics used by threats, which makes it overlap with both our work and the DISARM framework. The value of Shujaat et al.'s work is in its threat source analysis and classification, which complements our work. However, different from our work, Shujaat et al. conflate the terms "campaign" and "operation," while we consider campaigns as consisting of multiple operations. They also treat everything as misinformation and build disinformation operations on spreading misinformation, which they call "misinformation incidents" or occurrences of misinformation. Moreover, like the DISARM framework, they heavily integrate cybersecurity tactics and techniques into the tactics and techniques for handing disinformation, while we try to keep them separate.

3. Information Operations

In this chapter, we go deeper into information operations and the environment in which they are run. We also indicate the relation between information warfare and other types of warfare. Finally, we discuss elements of information space. We start with a discussion of operational domains based on the definitions of the US Joint Forces Command and NATO, which are utilised by almost all other Western militaries.

[24] Terp and Breuer, 2022.

[25] Shujaat, 2023.

3.1. Operational Domains and Their Layers

The "operational domain" is where combat and military operations take place. According to the definition by the US Joint Forces Command and NATO, there are five domains of war: land, sea, air, space, and cyber. Information operations do not have their own separate domain but are interleaved with all domains because all of them are dependent on information, which is used for decision-making. Cyberspace, the fifth domain, and its relation to information operations are especially interesting. Cyberspace is conceptualised as having three layers – physical, logical, and social.[26] This layering fits nicely with our discussion of information being perceived (people having direct contact with the physical layer) and received (people receiving information through the logical network layer).

In the end, people base their decisions and actions on information, which is perceived directly or indirectly, and so this layer covers both the physical and logical network layers. Yet, as discussed in Section 2, the logical network layer is where most of the information warfare occurs, so it is of greater interest to us.

We might even extend this idea to other domains and say that all domains have always had an information layer between people and the domain in question. Furthermore, this information space stretches between different domains. This conceptual image is important because it shows where information warfare fits, as well as its primary purpose, which is to distort the reality for persons operating in different domains. It also allows the fitting of different warfare activities. We can thus conclude that "information warfare" is a form of a war waged in the "information space", and the information space fits between all operational domains and people.

3.2. Information Lifecycle

Information has a lifecycle, starting from the point it is conceived and created and ending when it is consumed. Creation and consumption happen in the persona layer of the model we described in the subsection 3.1, while everything else happens in the information space. Physical transmission, storage, and processing of information occur in the operational domains. The information lifecycle has six phases. Note that this is the most general model, and some specific means (techniques) will fuse multiple phases into one.

First, information is "created" (first phase). This is a creative process governed by the purpose for which the information is created, and this activity is part of the "persona" layer. The result of this process can have different forms – such as directions, claims to be made, and raw articles – many of which might not be appropriate for direct consumption by intended targets. This step of creating information is outside of the scope of information operations as it is tightly bound to the purpose and goals for which the information is created; as such, it is under the auspices

[26] Joint Chiefs of Staff, 2018.

of psychological, cognitive, and other operations, as we explain in the following subsection.

The next step is "generating" information (second phase). This step can be automated or manual. In any case, the goal is to have variations of the original information that was created, each distinct from the others. Yet, all variations are still in the spirit of the original information, as they keep the key elements same across all variations. While manual creation is important, we are primarily interested in automated ways of generating variations.

After information is generated, the next step is "production" (third phase), wherein information is prepared for the media in which it will be published. This means that a visual representation is created for all variations.

Then, information is "published" (fourth phase). Publication could be in the form of a web page, an article in a printed copy of a newspaper, a book, etc.

After being published, information is "disseminated" (fifth phase). Based on the publication form, the information can be distributed in different ways, such as in email messages or on social media via the sharing functionality. Additionally, if someone else takes the information and shares or publishes it somewhere else, we also treat this as dissemination. There are means to get people to notice information being published and disseminate it further. For example, this can be done by placing advertisements (ads), planting links in different forums, search engine optimisation poisoning, sending mail notifications, etc. We also treat this as a form of dissemination.

Finally, information is "consumed" by targets (sixth phase), which can also trigger the process of information creation in certain cases, for example, in forums or on chat applications. Consumption is a psychological process and is again outside the scope of information warfare.

Now, we will define each step of the information lifecycle, starting from generation up to dissemination, as a "tactical step" used in information operations. Thus, we have four tactical steps – generation, production, publication, and dissemination – and we will define techniques and sub-techniques that can be used to implement each of these.

3.3. Information Forms

Information can come in many forms, the most common form being text. However, this is not the only possible or even the best form. The text form is popular because it is easy to manipulate. Other forms of information include photo, video, and audio, which were once harder to manipulate. Yet, it does not mean that these forms were not produced or manipulated, but that such manipulation occurred less frequently. Because of ML advances, such forms are increasingly being used. Some forms can be divided further into subtypes. In information warfare, disinformation that should be conveyed to targets for consumption is encoded into one of the given forms.

Before the advent of digital technologies, manipulation of information forms was a very resource- and time-consuming task. Today, however, a multitude of tools are available for this purpose, and it is much easier to produce information in different forms. Still, some forms are easier to manipulate, while others are harder. This leads the forms that are harder to manipulate to be more trustworthy, and those that are easier to manipulate to be less trustworthy. The difficulty in manipulating each information form also depends on the desired change: minor changes are easier than creating the form from scratch.

As mentioned, the easiest form to manipulate is text, especially since computers became widely available, because they allow text to be very quickly typed, copied, multiplied, etc. No matter what needs to be done, it is technically easy, be it creating text from scratch, removing certain parts from the existing text, adding parts that were not present, or modifying existing parts.

Photos are next in terms of difficulty to manipulate. They are harder to manipulate than text, but it depends on the exact modification. It is well known that many people use different applications to improve their posture in photos, but these are simple manipulations achieved by applying filters. Much harder manipulations include photo montages that might require professionals. Such manipulations by professionals might be extremely hard to detect or to prove that the photo is counterfeit or manipulated in some way. The tool professionals use most frequently for this purpose is Adobe Photoshop. Note that photo manipulation has been done almost since the advent of photography.

Videos are even harder to manipulate. It involves the manipulation of a large number of still images (equivalent to photographs), which makes video manipulation much more resource demanding than photo manipulation. Thus, it is generally restricted to simple manipulations, such as blurring specific parts of videos so something is hidden. Videos are frequently accompanied by audio, especially if they show someone talking.

Audio can be manipulated as well. Today, it is extremely easy to record any conversation, because a recorder is available in all mobile phones. This means that it is easy to convince someone that an audio recording is genuine. In other words, it is not unexpected to have an audio recording because of the prevalence of audio recorder devices.

In the tactical step of information generation, it is possible for information in one form to be transformed into another form, possibly using ML techniques.

3.4. Information Operations in Relation to Other Types of Operations

As seen in Section 2, there are several types of warfare and thus operation types. Our central theme is information warfare or information operations, and we are interested in the relationship between information warfare and other types of warfare. In the subsection 3.2 we argued that information operations deal with the process of generating information based on requirements, publishing it, and finally distributing it. The requirements are specified by an outside process, which depends on the goals of an outside actor. Psychological, cognitive, economic, financial, political and propaganda operations dictate the requirements of information operations. All these operations have the specific goal of impacting people, the society, or some groups in between. As such, they are in a much better position to determine the best course of action.

For example, let us assume that someone is conducting a psychological operation that has as the goal of creating uncertainty and anxiety in the population, for whatever purposes it might serve. This end-state can be achieved using psychological operations in several ways. Each approach is grounded in the knowledge of psychology, which, based on human behaviour patterns, dictates what should be done to achieve the operational goals. One approach might be to have military exercises along the border of the target country, and another might be to have a military parade and boast one's superiority over the target country's military forces. Yet, the approach we are interested in the most is using information operations to spread psychological messages to the target country's population. In this case, the psychological operation gives directions on what should be spread, which is then taken by the information operation operator, adjusted for different information channels, and then published and distributed using those channels. In essence, information warfare is a tactic of psychological warfare.

Three relations between information warfare and other warfare types can be analysed. The first is when information warfare is "used by" some other warfare type. This is the case for psychological, cognitive, economic, financial, propaganda, political warfare. In this case, information operation is just one tactical or technical step for those warfare types. The second relationship is when information warfare uses some other warfare type. This is the case for cyber warfare, electronic warfare, social network warfare, and ad operations. Note that here we have, not so common, social network and ad warfare. The reason they are denoted as such is that they are quite complex activities and thus have non-trivial tactics and techniques. After all, there are many companies offering PR and marketing services, so this is a very developed activity which can be abused as well. Finally, the third relationship is subset of information warfare. For example, if we are talking about fake news and the way it could be spread, then this is only subset of disinformation that is handled by information warfare. Or, disinformation warfare, might also be treated as subset of information warfare because information warfare includes tactic of blocking information from spreading, which disinformation warfare – arguably – doesn't include. Note that we don't have superset relationship with information warfare, i.e. that some warfare type is superset of information warfare. The reason is that we treat information warfare as a canonical type of warfare. In other words, we could invent some warfare that will be a superset of information warfare, but we treat it as union of other warfare types or their parts (psychological, cognitive, cyber, etc.).

Cyber operations are interesting as they have a goal of bringing operators of information operation into a position to achieve some tactical step. For example, if information operation planning decides that the best approach to spread some piece of disinformation is by some popular news portal, then it needs to be compromised in some specific manner that will allow planting of disinformation. This can be done, among other things, by means of cyber warfare. In general, all cyber operations consist of two steps, one getting into position to do something, and the other step is really doing something. This is not so visible in the case of pure cyber operations but becomes obvious in some special situations. Take as an example the attack on electrical power grid. In order to sabotage this system, it is necessary first to gain appropriate position (e.g. compromise of SCADA station), and then someone who knows how electrical power grid works has to manipulate system in such a way to destroy it. It cannot be done by the people who compromised the system as they have different expertise. Upon further analysis, it becomes clear that it is also the case in operations that are wholly contained in cyber space. For example, if attackers manage to compromise some database system, the exfiltration could be done by persons not skillful in attacking, but by someone who is good database admin, or something similar. The personnel capable of hacking might be transferred to another operation where compromise is required.

3.5. Elements of Information Space

Information exists in information space, and we define information space as a set of all the elements through which or on which information is stored, transmitted, or processed. Today, the majority of information space elements are in cyberspace, or on top of cyberspace, but there are the ones that are in the physical world as well, like traditional printed newspapers, TV, or radio. Our definition is intentionally very broad to cover all those media.

In general, what differentiates information space elements are parameters like directionality, speed of information spread, reach, and possibility of targeting. Regarding directionality, information can flow from threat source to targets, but not vice versa. For example, traditional newspapers are such a type of medium. On the other hand, there are mediums, dominantly modern ones based on information technology that allow bidirectional flow of information. Regarding the speed of information spread, we mean the time necessary for disinformation to reach intended target. Again, traditional media are much slower than modern ones based on information technology. The parameter of reach determines how large is the audience reached by disinformation. Newspapers, as a traditional media, have a broad reach, as well as television and radio. Modern means of communication are not so broad, unless we count traditional newspapers published on web portals. Finally, targeting is the ability to deliver disinformation to a specific group. Traditional media is again in this respect much more restricted than modern media, but it should not be underestimated. For example, there are television broadcasters followed by people that identify with the political tone of the broadcaster. Yet, this targeting is much more versatile in the case of new media based on information technology.

In the following sections we'll survey key elements of information space and give some basic characteristics of each one of them.

3.5.1. Social Media

Social media platforms are technical infrastructures supporting social networks. Social networks, on the contrary, are networks consisting of connected human beings that communicate. Many social media platform types and specific instances exist. In this section, we go over key characteristics of the more important platforms: X (formerly Twitter), Facebook, LinkedIn, Instagram, YouTube, and others.

In essence, a social media platform is more valuable the more users it has. Thus, the primary goal of all social media platforms is to attract and retain as many users as possible. The platforms are constantly changing as new services are introduced and old ones are removed. This is done to offer users a better experience and reasons to stay on the platform. Although the number of users is an important parameter, in general, it is difficult for outside observers to assess the number of users of social media platforms. These platforms do publish some numbers for marketing purposes – but they are difficult to verify. Additionally, social media platform owners find it tough to estimate the number of users because of "bots", which are software pretending to be human users that engage in different activities on a social network.

All social media platforms have similar functionality. They allow each user to publish information, and this information is shown to everyone or only to a specific group of users – depending on the method of publication and privacy settings. Published information can be shared by other users using different mechanisms. This propagates information to users that are not in direct contact with the originator of the information. Furthermore, they allow the formation of interest groups and sharing of information only within those groups. Each group can be private or public. Only members can see the content shared within private groups' networks.

Finally, almost all social media can convey all forms of information, even though some are more specialised, such as YouTube for video, Instagram for photos, and TikTok for short videos. All platforms also use some form of advertising for monetisation.

3.5.1.1. X (Formerly Twitter)

X, formerly known as Twitter, is a very influential social media with around 368 million monthly active users as of December 2022.[27] The main feature of X is the users' ability to publish messages, called "tweets", of maximum 280 characters, which replaced the previous limit of 140 characters. On 28 October 2022, Elon Musk bought Twitter and has radically changed the company since then.[28] One change

[27] Dixon, 2023b.

[28] Zahn, 2022.

was to close APIs' access to X. Researchers had used APIs to study behaviour on X, which had made X (actually Twitter) the most studied social media. In a bid to make money from X, Elon Musk also increased the tweet limit for verified accounts to 4,000 characters.

X has two operations for information publication and sharing. First, each user can follow other users on X, meaning that they will see on their homepages tweets from the users they follow. Additionally, X sends email messages with a summary of published tweets. The second operation is the so-called "retweet", which involves publishing someone else's tweet. This means that other users can post tweets to their followers, spreading the original (retweeted) tweets even further. It is obvious that the more followers a user has, the more influential he or she is. Moreover, the more times a tweet is retweeted, the more influential it is.

Finally, as regards the information lifecycle, X can be used to publish (tweet) disinformation and disseminate it by retweeting. Those who publish disinformation can expect a fast spread, as disinformation spreads faster on X than true news,[29] which makes X an effective platform for disinformation.

3.5.1.2. Facebook

Facebook is the most used social media with over 3 billion monthly users as of the second quarter of 2023;[30] it is also much more versatile than X. As such, it is a very influential social media platform.

There are two main concepts in Facebook. The first one is a "wall". A wall is the place, or page, where a user's activities are published for others to see. The owner of the wall can communicate publicly with other users using the wall: other users can write messages on the wall, and the owner can reply to them. All these messages are publicly visible, although privacy settings can limit visibility. The second concept is the "timeline" (previously, the news feed), which is the user's private page where the user is notified about happenings on Facebook. Because a lot of activities are going on, especially for users who have a large number of friends and/or follow many different pages, only a subset of the activities is shown. The activities to be shown are selected by an algorithm, which is not known publicly.[31]

Facebook has three operations for information publication and sharing. The first one involves becoming friends with other users on Facebook and forming a network of friends. This mechanism was intended to map friend connections from the real world, but it has diverged in the virtual world because of two reasons. First, people get to know and connect with other people through purely online means, without ever meeting in person. Second, it is questionable how strict Facebook users are about not accepting friend requests from people they do not know. Additionally,

[29] Langin, 2018.
[30] Statista, no date b.
[31] Eslami et al., 2015.

Facebook constantly tries to detect people someone might know and offers an option to connect as friends. This detection algorithm is not perfect, and thus suggestions are offered to add completely unknown people as friends.

As in the case of X, when someone publishes a post on Facebook, it is shown on the timeline of friends. Each friend has the option of "sharing" a post, that is, showing it to his/her friends, and so on. This allows the post to reach even more users, just as in the case of X.

Because there is a limit on how many friends you might have, the second method of information sharing is "following" someone's page. That is, someone creates a page about something, and then users interested in the topic of this page can follow it. Following means having a higher chance of getting notifications in the timeline (news feed) about changes on the followed pages. The third way to connect is using "groups". Groups are created around a topic, and anyone interested in that topic can join the group. Groups can be private or public, searchable or not. Activities of public groups are visible to anyone, while private groups are only accessible to members. Searchable groups can be found by using the Facebook search functionality. In any case, membership can be controlled by group administrators, meaning that they have the full discretionary right to admit someone to the group or refuse membership.

From the perspective of the information lifecycle, it is obvious that Facebook can be used similar to X to publish and disseminate disinformation.

However, unlike X, Facebook allows users to market their posts to other users. This is a handy means to achieve two different goals regarding spreading disinformation: reaching new users and amplifying posts to existing users. Importantly, selection of users to whom a specific post is shown can be based on several parameters that allow precise targeting.

Facebook has advanced privacy settings that can be used to limit access to any of the three means to connect.[32] While privacy settings might restrict the reach of disinformation, it is questionable how many users change the default privacy settings.

3.5.1.3. LinkedIn

LinkedIn is quite similar in basic function to Facebook, but its primary users are professionals. They use LinkedIn to find a job, find employees, grow their professional network, connect with peers, etc. In 2022. LinkedIn had over 750 million users.[33] While Facebook had several issues with disinformation campaigns and privacy, it seems that LinkedIn has been spared from such content, at least compared to Facebook.

[32] Facebook, no date.

[33] Dixon, 2023a.

3.5.1.4. Instagram

Instagram is a social media for sharing photos. It is a more specialised version of Facebook. It also allows people to have followers and comment on photos. Instagram accounts can be private or public. A characteristic of Instagram is the so-called "influencers". Influencers are people who have a large number of followers and specialise in creating content. Often, these people participate in marketing activities and are not always transparent about it.

One important indicator on Instagram is "Instagram engagement", which is a measure of how much users interact with someone's content.[34] It aggregates all interactions – likes, comments, shares, and saves. In marketing, this measure determines how content resonates with users, and the higher the engagement, the more users identify with the content.

Just like other social media, Instagram can be used to publish and disseminate disinformation during information operations.

3.5.1.5. YouTube

YouTube specialises in video distribution. Due to its scalability and capacity, it is also used as a distribution platform for live streams. YouTube allows users to broadcast videos, which once only a few people could do. Several people specialised in content generation regularly publish on YouTube. Some of them are extremely popular and influential, meaning that they are influencers just like on Instagram. It is common for the same people have a presence on multiple social media platforms.

YouTube also has a recommendation algorithm that recommends users videos based on their watch history.[35] It is known that these recommender algorithms have issues; for example, they can radicalise people by offering more and more radical videos. Finally, YouTube is a marketing platform that inserts ads into video feeds, and its system determines who should see an ad depending on several parameters.

To allow viewer engagement, YouTube allows the comment and chat features to be attached to videos or live feeds. Moreover, each video can be "liked" or "disliked", and each view is counted. These parameters are then used as a popularity measure. Recommender algorithms use these parameters as well when determining what will be offered to a user to watch.

3.5.1.6. Other Social Media

There are many other social media platforms, which are constantly in flux, along with specialised platforms for specific interest groups. Gab is an example of a

[34] Demeku, 2023.

[35] Zhou, Khemmarat and Gao, 2010.

specialised social media.[36] Gab's social network is similar to X, as it allows all users to broadcast short messages of up to 300 characters; it also has certain features similar to Reddit, such as a voting system for content popularity. This platform has almost non-existent rules and was created in August 2016 in response to Twitter's moderation rules. Therefore, Gab has many alt-right users, conspiracy theorists, and a high volume of hate speech. This makes Gab a fertile ground for information operations.

TikTok is also an important social media platform. TikTok specialises in truly short-form videos, making this platform very popular among the younger generations. TikTok's popularity compelled already established social media platforms, such as Facebook and YouTube, to introduce similar features. TikTok has been abused for information operations, especially during the COVID-19 pandemic.[37]

The final social media platform we will mention is Reddit. Reddit has 2.203 billion monthly active users, and number of daily users reaches over 62 million.[38] Reddit is a more discussion-based social media platform where people can ask questions and discuss different topics. All discussions are organised in groups called "subreddits". Additionally, users can vote for others' posts and thus make them more visible to others. Researchers have identified subreddits that connect people who, for example, have doubts about climate change[39] or are interested in other topics. As such, Reddit can be used for publication and distribution of disinformation during information operations.

3.5.2. Digital Advertising

Digital advertising is a source of revenue for a large ecosystem of companies, starting with the biggest Internet companies such as Google and Facebook. It is projected that in 2024, the digital advertising market will reach US$740.3 billion.[40] This ecosystem consists of three groups of players.[41] The first group is "advertisers," representing those who want to advertise a service, good, idea, etc. The second is "publishers," which are entities (or web pages) visited by users. Publishers offer advertisers the opportunity to publish ads in parallel with content in which the users are interested. Publishers can be search engines, newspapers, or any other more or less popular site. Finally, "ad networks" are intermediaries between the advertisers and publishers. Their goal is to match publishers that offer places for ads to be shown and advertisers that have ads they wish to be shown.

The key to the success of digital advertising is the use of methods (algorithms) that try to show the users ads that are as close as possible to their interests at that time. For example, if a user uses a search engine such as Google to find something

[36] Zannettou et al., 2018.

[37] Basch et al., 2021.

[38] Turner, 2024.

[39] Kim, Stringhini and Vodenska, 2023.

[40] *Statista*, no date.

[41] Chen et al., 2016; Grover, 2023.

about global warming, it is possible to inject ads in the results that promote conspiracy theories about global warming. It is also possible to insert other conspiracy theories under the assumption that this person is susceptible to such disinformation. Additionally, it is possible to link ads to the geographic location of the user, which also promotes targeting. In general, ad campaigns are run by marketing and public relations agencies. These agencies offer the service of promoting goods, services, and ideas, and in doing so, they use other methods besides ads.

It is already known that certain agencies try to spread disinformation for their clients.[42] What makes this situation even worse is that these clients can deny involvement. Moreover, it is already known that cybercriminals abuse ad networks for their nefarious purposes.[43]

In conclusion, digital advertising is a great technique to implement dissemination tactics phase of the information lifecycle.

3.5.3. Communication Platforms

While communication platforms are a subset of social media, we treat them separately due to their different nature. They operate more as distribution lists, wherein information is pushed to each member of a group. This is unlike social media platforms that generally utilise a pull model of communication, wherein each user must open a specific page and fetch information. Additionally, communication platforms are less reliant on recommendation algorithms, because each user receives each message. The most popular communication platforms are WhatsApp, Viber, Telegram, and Signal, along with other, lesser known, platforms. All these platforms are bidirectional in nature, which means that every user can communicate with every other user. A notable feature of these platforms is the ability to create groups. That is, any user can create a group and add or invite other users to this group. The groups can be private or public, as in social networks. In addition, users in these groups can be anonymous because only phone numbers are necessary for registration, and temporary numbers are readily available without giving any personal data. In addition, some communication platforms guarantee end-to-end encryption, which means no third party can see the communication.

Forums are a special case of communication platforms. They are similar to WhatsApp, Viber, and others as they allow two-way communication and provide groups for discussions. Yet, they do not offer such a level of privacy and anonymity. The most popular forum, among others, that is used to spread disinformation is 4chan.[44] To create such a platform, it is enough to obtain free software support, such

[42] Fisher, 2021.

[43] *Cybercriminals are Using Paid Ads to Get to Top Cloud Provider's Customers*, 2015; Richet, 2022.

[44] 4chan, no date.

as through phpBB,[45] and obtain web hosting, which is quite cheap these days. The issue is how to make this platform popular enough to attract users.

A special case of forums involves services such as Disqus.[46] These services allow everyone to add a forum-based discussion with ease. This is used, for example, by newspaper portals. A forum is embedded under each article that allows users to comment on the article.

In conclusion, communication platforms can be used to publish and distribute disinformation. The reach varies based on the privacy settings and specific technology used, and it covers a wide range of options.

3.5.4. Traditional Media

Even though we live in a highly interconnected world dominated by the Internet and social media, we must not forget about traditional media such as radio, television, and newspapers. Even though these media have had to adjust to modern technologies, and some even suffered during such adjustment, they remain important enough. They are especially important for older people who have not embraced new technologies and do not use them much.

Note that traditional media are essentially one way communication – from broadcaster to audience. The reach depends on the popularity of the media and its targeted audience. The speed of information spread is relatively high for radio and television, but quite slow for newspapers. Finally, all these media have specific audience profiles based on their content and tone, as dictated by their publication desks.

Modern technologies have brought additional distribution channels to traditional media, along with a broader reach to consumers. That is, with the Internet, both radio and television have broadened their reach to, effectively, anywhere on the Earth. However, most radio and television stations are local in nature, or regional at most. Still, there are cases of a global influence by traditional media such as *Russia Today.*

3.5.5. Other

Other means of communication, which are not covered by the above categories, also allow information dissemination. Examples include leaflets, which can be distributed using different means, and billboards. The options are effectively countless.

We also did not mention other means of using the Internet to spread information. For example, nowadays it is easy and cheap to create an online news portal and to publish in general. All that is needed is a tool such as an instance of WordPress,[47]

[45] phpBB, no date.
[46] Disqus, no date.
[47] WordPress, no date.

which can be found on the market for as low as US$3 per month.[48] Next, it is necessary to populate this instance with news and continuously add new material, while also building a community via, for example, ads or social media. Additionally, users can be engaged when visiting the portal by allowing comments and discussions on posts. The comment system is also relatively affordable, and there are many options. Dedicated platforms such as Disqus can be used, as already mentioned. It is also possible to embed the Facebook comment system on a page. Finally, one can announce a piece of news on social media platforms, such as Facebook, and use those platforms for engagement with readers.

Additional options to publish include blogs, plain web pages, etc. These options make spreading disinformation more dangerous, as there is no quality control of the material published on the Internet, and users in general are unable to critically assess the content they find while browsing the Internet.

3.6. Information Operation Goals

The purpose of each information operation is to push certain disinformation to the target audience. However, each information operation must have a goal it wants to achieve. For example, the operation's goal might be to push certain disinformation to a specific target group, or it might be to acquire new followers on social media or groups who believe in certain disinformation. Yet another information operation might be used to initiate some action from people, such as starting a protest. As a final example, the operation's goal might be to reinforce the belief of a target group in some disinformation. The goal possibilities for information operations are countless and are dictated by outside factors.

Note that there could also be "support information operations", wherein one operation tries to push some disinformation to the target group, but several additional information operations are defined to support the main endeavour and maximise the probability of success.

Information operations are generally not easy to run, and it is necessary to plan them beforehand, organise all the necessary resources to support operation, and then execute them properly while considering any unforeseen events. In conclusion, planning, organising, and executing information operations is a topic in itself that remains underexplored.

[48] GreenGeeks Web Hosting, no date.

4. Tactics and Techniques

Section 3.2 Information Lifecycle indicated that information goes through certain phases, each of which is considered a tactic. Each tactical step defines the objective of an adversary. Tactics can be achieved using different techniques and sub-techniques. In this section, we will review some tactics that can be used as well as their associated techniques and sub-techniques, where sub-techniques are more specific technical steps. Note that this is not an exhaustive list of all techniques and sub-techniques, and only the frequently used and well-known techniques are mentioned. Also mentioned are techniques that have not necessarily been used but have the potential for use. It is left for future work to create a comprehensive database of techniques and sub-techniques, such as the MITRE ATT&CK pattern, and to better connect them to what has been observed to be used.

4.1. Generation

In some cases, disinformation that should be spread is given in a form not suitable for the targets' consumption, such as when only guidelines are given on what should be spread or the disinformation needs to be translated into another language. Alternatively, an information operation operator might want to use different publication venues. In this case, it would be harmful to use a single instance of disinformation as it might rouse suspicion among the targets regarding the validity of disinformation. For example, an information operation may create a single news article with the goal publishing it in as many newspapers or portals as possible to have an impact. In that case, the more the published texts differ, the more likely they are to leave the impression that they are the opinions of multiple people and thus will be more persuasive. Obviously, the original message, which is the core of the disinformation, must be preserved across all texts. Therefore, in general, it might be necessary to morph the original message while keeping the intended intent intact.

At least three techniques can be used to implement this step from the technical perspective: (1) humans can be used as content generators; (2) ML models can be used as content generators; and (3) ML models used by others can be poisoned to spread disinformation indirectly. In the following subsections, we go over each technique in more detail.

4.1.1. Humans as Content Generators

For a long time, the only means to manipulate information based on some prescription was by engaging human beings. While this is potentially flexible, it is also costly and dependent on the skills and knowledge of the people involved. In essence, you give instructions to workers on what they should promote along with a few specific pointers; then, the workers engage in generating different variations and possibly spreading those variations across information space elements. Obviously, there are shortcomings to this approach. First, a single person has limited quantitative capacity, as he/she can produce only a limited number of pieces of information per day. Second, the quality of materials produced by a single person might not be satisfactory because all the produced information variations will be similar. Third, the cost is high. Finally, the more people know about something, the higher is the likelihood of a leak.

In any case, to be able to use this technique, you need resources such as troll armies, employees, collaborators, and people who are like-minded but otherwise unrelated to you.

4.1.2. Use of AI/ML for Generating Content

As mentioned in Section 2 Background, ML has made great progress in recent years that allows the replacement of humans in situations that were once deemed only the realm of human intelligence. As such, this area influences information operations significantly by lowering expenses and opening up new opportunities.

Information operation operators have the option to use LLMs to generate almost infinite variations of the disinformation they need, without relying too much on human resources. This increases their capabilities and the probability of the information operation's success. To implement this technique, information operation operators have several options. They can use publicly available ML models, such as ChatGPT. This approach might raise an issue for operators, as such ML models have safeguards embedded that prevent them from generating harmful content. The next option is using the so-called "open source" ML models, with an option of further finetuning them. In this case, the adversary must have built and maintained infrastructure, which should be managed using a logistical process. This is further discussed in Section 5 Logistics Support. Finally, ML models can also be built from scratch. This is the most resource-demanding approach and, due to the availability of open-source models, an unlikely one.

One additional option for information operation operators is to use cyberoperations to steal advanced ML models from their owners. Alternatively, they may compromise the access credentials of regular users, which allows the abuse of publicly available ML models.

4.1.3. Poisoning of ML Models

One technique to generate disinformation is to poison ML models. Namely, all models are trained on data collected from the Internet. The idea is to insert poisoned data into data used for learning so that the model users are given disinformation whenever they ask something in relation to the topic of the disinformation. This can be done in several ways, depending on what is under the control of or might be influenced by the adversary. This ecosystem of creating and distributing ML models grows more and more complex with time as new companies appear that offer new services in relation to ML models. Here, we use a simplified model in which an adversary can control one of three components that comprise the lifecycle of an ML model: data, learning process, and model distribution.

If adversaries can influence the data, then the goal is to enter as much disinformation into the raw data with the hope that the model, during the process of learning, will pick it up and behave accordingly. There are several ways to achieve this, depending on the resources available to the adversary. First, adversaries can plant disinformation data at some key points on the Internet (e.g. Reddit). Note that, if this approach is taken, this becomes an information operation in itself because several tactical steps have to be performed to achieve it. Second, datasets for training can be published with disinformation covertly embedded. Due to the datasets' large sizes, it makes it difficult to check for disinformation and easy to plant it. Collecting training data is hard and highly resource intensive. This makes publicly available datasets valuable and commonly used. Additionally, these issues have led to companies offering data manipulation services.[49] Note that the existence of such companies adds an additional opportunity, as they are potentially weak points that can be attacked using cyberspace or other warfare operations to plant disinformation.

We end the discussion on the adversary controlling data by noting that "data missing" can also be a way to spread disinformation. By removing data that supports truth, the model can learn to spread disinformation indirectly.

The next step in ML models' lifecycle is the learning process. If an adversary can influence the learning process, he can inject disinformation during this process or even manipulate the learning process itself. The easiest way of achieving this is using cyberspace operations to infiltrate companies that train LLMs.

Alternatively, due to the popularity and demand for open-source LLMs, it is possible for an adversary to train LLMs with embedded disinformation, which is then given to everyone to use freely. However, due to resource demands, this is an unlikely option.

Finally, if an adversary controls or has influence over the distribution channel, he/she can plant poisoned models. For example, HuggingFace[50] is a very popular distribution site for different ML models, and existing cases show that it is a real threat.[51] Using cyberspace operations, it might be possible to compromise the site and plant some models on it.

4.2. Production

The goal of the production tactical step is to adjust generated content to specific media. For example, raw text might need to be formatted to fit the visuals of a portal, or text-only information might need to be complemented with pictures or

[49] Toloka, no date.
[50] HuggingFace, no date.
[51] Lakshmanan, 2024.

transformed completely into pictures and video. The key difference between this and the previous step is that information is only transformed in this step – that is, its appearance is changed – but otherwise it stays the same.

Several technical steps can be used to implement this tactical step. First, as always, humans can be used. For example, a journalist is given a text to publish, and she might need to transform this information into a form suitable for publication in the journal she is working for. Likewise, the information needs to be converted into segments for a local television station. In these examples, the persons engaging in production might or might not know that they are spreading disinformation.

Second, some automation processes might be used. Certain transformations can be done relatively easily using simple processing means. For example, a given text to be published may need a heading and footer, which can be added easily. After all, many web pages – such as The New York Times, The Guardian, eBay, and Amazon – use this mechanism to achieve consistency and improve the readability of the content for the users.

The third approach is to use ML models. More complex processing, especially transformation of information from one form to another or augmentation of one form with another, once fell exclusively in the domain of humans. However, ML models, specifically generative ML models, show great promise in this regard. A day may come when all the user needs to tell a machine is to, for example, "[t]ake this text and make it look like it was published on by *The New York Times*", and the machine will do the rest.

We can consider fake news as being a combination of content that should be communicated to targets and a form that makes this fake news more appealing. This is because people believe it was published by a reputable source – even without checking the source. To conclude, fake news is created as a combination of two tactical steps, generation and production, and as such, multiple techniques can be used to create fake news.

4.3. Publication

Publication is the process of making a specific instance of disinformation available to people or groups targeted by the information operation. This is probably one of the richest tactical steps, along with dissemination, as regards the number of available techniques. That is, abundant techniques can be used to implement this step, including publication on social media, publication through communication platforms, publication on compromised web sites, publication through traditional communication media (radio, television, and printed newspapers), starting of rumours, use of chatbots to spread disinformation, and use of "useful idiots" to inject disinformation.[52]

[52] Thrush and Feuer, 2024.

In the following subsections, we discuss some of these techniques in more detail based on the information space elements they use for publication.

4.3.1. Social Media

Social media are likely the most prominent means of publishing disinformation. The additional benefit of social media is the possibility of acquiring new supporters, as anyone can see or share a post. Moreover, social media allow targeting based on demographic and other parameters. Sub-techniques that could be used here include operators publishing information in groups on social media or on highly connected users' profiles; troll armies pushing disinformation via their social media accounts; social network bots pushing disinformation; proxies being used to push disinformation; and using cyberoperations to compromise specific users or a social media platform as a whole.

4.3.2. Communication Platforms

Communication platforms are more closed off than social media platforms, and thus they can be used primarily to reinforce the beliefs of those who already believe in a disinformation. Obviously, to be able to publish on those platforms, an agent as well as a member of the targeted group must be present on those platforms.

Again, the same sub-techniques for social media can be used for communication platforms.

4.3.3. Traditional Media

Many sub-techniques can be used to publish in traditional media: owning traditional media nd using it for publishing disinformation, sending a letter to the editorial office by pretending to be a whistle-blower, using cyberspace operations to create the possibility of injecting disinformation within other published information, sending press releases, and bribing journalists to publish some information.

4.4. Dissemination

Dissemination is the process by which published information is pushed to users that did not directly receive that information. This is another rich tactical step as regards the number of available techniques, besides the publication tactical step.

This tactical step exists to reach a broader public with disinformation that is not possible with just the publication step. For example, when something is published on Facebook, friends and followers of the person publishing might not see the message because their newsfeeds might be overwhelmed with posts from other users. The process of dissemination aims to solve this and many other issues so that information is shared widely to reach as many users within the targeted group as possible.

The following techniques can be used for the dissemination tactic. The first technique is “sharing”, All social networks support some form of sharing. The potential problem with sharing is that it is not under the control of the one who published the information, and thus the operator must rely on luck in this case. Some sub-techniques might be used to persuade people to share information. The second technique is “digital advertising.” By using ad networks, or ads, it is possible to push notifications about disinformation to people to whom the operator is not directly related. Furthermore, it is possible to target specific geographies, demographic characteristics, etc., as discussed in Section 2 Background. Third, it is possible to perform “advertising via proxies”. In this case, the information operation operator uses proxies, as a friendly force, to push the ad instead of the operator itself. Proxies might knowingly or unknowingly participate in pushing disinformation. Good proxies that have a wide reach include influencers on social media. The fourth technique is “recommender algorithm manipulation”. As we said, not all users may see the published information in certain cases. For example, on Facebook, an algorithm determines what will appear in a user’s feed. In this case, manipulation is necessary for the news to be pushed high in other users’ feeds.

These techniques can be further amplified and supported using troll armies, social media bots, proxies, and botnets. We further describe these in Section 5 Logistics Support.

4.5. Attenuating the Information Spread

Section 3.2 Information Lifecycle showed the phases (dis)information goes through from the point it is conceived until it is consumed by targets. However, it is also important to consider the case when information does not reach people. The tactic of “attenuating information spread” is used to prevent targets from receiving valid information that will counter the disinformation campaign. Suppressing the truth from reaching people and serving them disinformation first might have an anchoring effect on the targets.

One technique to implement this tactic is the use of cyberspace operations to prevent information flow. The easiest operation is to conduct a denial-of-service attack on the source that tries to fight disinformation. Alternatively, troll armies can be used to cast doubt on truthful information by bombarding people with questions and statements that sow uncertainty and doubt. Electromagnetic warfare can also be used to disrupt communication. These are just some examples of techniques that can be used, but there are others as well.

5. Logistics Support

Support for certain technical steps must be prepared in advance so it is available to the information operation operator. These elements can be prepared specifically for certain operations, shared between different information operations, or rented from third-party providers. The key point is that all such steps require significant resources and time to establish while also incurring maintenance costs. In this section, we review some support elements for information operations.

5.1. Troll Armies

Troll armies comprise people that either willingly or unwillingly participate in actions that aim to spread disinformation. They can be under a single command as employees of a company, such as in the case of the Internet Research Agency,[53] and they can also be distributed and loosely controlled,[54] often recruited by bribing different, unrelated people.

There are many potential usages of troll armies. They can engage in discussions related to a topic of interest for the information operation operator; they can poke around and push their agenda; or they can be used to disable or slow down the spread of information using fear, uncertainty, and doubt techniques to suppress the dissemination of true information and cast doubt on it among the targets.

Troll armies also engage in creating social media accounts and building their reputation so that they can be more persuasive when they are used.

5.2. Social Media Bots

Social media bots[55] are programs that imitate human online behaviour. They are either autonomous or semiautonomous. The advantage of social media bots is that it is much easier to create a large number of artificial users and control them. Their functionality and complexity can vary from simple activities such as liking posts or sharing them to complex interactions with humans. For example, researchers have shown how using social media bots allowed them to infiltrate the users of different organisations.[56] The advent of LLMs has opened up further possibilities. Note that certain companies also create and sell large social bots. The first such company to be exposed was Devumi.[57]

[53] Bastos and Farkas, 2019.
[54] Aro, 2016.
[55] Chang et al., 2021; Oentaryo et al., 2016.
[56] Elyashar et al., 2013.
[57] Confessore, 2018.

5.3. Interest Groups

Certain information space elements support the concept of groups, which might be created naturally and in a self-organised fashion. As this does not allow any control over the process, another controllable approach needs to be used.

The controllable approach may involve a group being built in a specific time, around a common theme, and grown to be of a specific size by someone who leads the process. This group would then be used to disseminate disinformation and be abused to spread this disinformation even further.

During the build-up, other techniques might be used to speed up the process. To overcome the chicken-and-egg problem – the problem of users having no incentive to join the small group – troll armies or social media bots might be used to artificially inflate the number of group users and make it more attractive. Additionally, information about the group might be spread using, for example, ad services and troll armies, to get more people on board.

5.4. Proxies

Proxies are news outlets, groups, or individuals who push someone's agenda, but without being involved in its fabrication. In other words, they believe in the disinformation they are spreading, potentially making this misinformation. However, as discussed in Section 2 Background, we do not differentiate between disinformation and misinformation, as it requires analysing motives, which is very difficult.

Of all the proxies, certain types have great potential to spread disinformation. One such group is the so-called influencers,[58] or people with a large number of followers on social media. Influencers are just one form of celebrities, which are as old as the human society. All influencers are ready to promote products, services, or ideas in exchange for monetary compensation. They are especially dangerous if they are malleable to disinformation, truly believe in it, or do not have any moral or ethical standards. Moreover, many of today's influencers are relatively young people in their early 20s, meaning that they are inexperienced and not yet fully mature. Furthermore, many celebrities in the past openly supported certain ideas, such as political, ecological, or humanitarian ideas. Therefore, it is easy to see that they can and will be used to promote disinformation.

Another type of proxies is groups on social media that connect people with similar thinking and might be susceptible to disinformation. If a large number of members of such groups accept certain disinformation, it might start to amplify, attract other members, and start to spread outside the group.

[58] Gómez, 2019.

5.5. Cyberoperations

Disinformation might also be published using cyberoperations. As argued in Section 3.4 Information Operations in Relation to Other Types of Operations, cyberoperations allow one to be in the position to take actions that are not strictly part of the cyberoperations or cyberspace in general. For example, in the case of operational technology, reaching control stations (e.g. SCADA) might allow attackers to act in the physical world – which is not in the cyber domain. For information operations, cyberspace operations could use the following sub-techniques: (1) compromise news portals, which will allow the information operation operator to engage in unauthorised publication of disinformation or change existing content and (2) compromise potentially large number of web sites, which will allow the information operation operator to publish disinformation on these sites. These sub-techniques will have effects, such as search engines rating this content higher and more users being exposed to it. Cyberspace operations are used to create and maintain botnets, which can be used for many purposes, such as mass mailing, hosting social bots,[59] generating artificial traffic, and penetrating social media or communication platforms to push disinformation.

It is noteworthy to stress the connection between three stakeholders that might cooperate or just use each other's resources. These stakeholders include (1) the nation state that potentially runs the information operation, (2) cybercriminals who have infrastructure for cyberattacks, and (3) private companies that work in the grey area of the legal framework. It is well known that the Russian state does not prosecute cybercriminals in Russia, provided that they do not attack domestically.[60] Rather, Russia actively uses cybercriminals' resources and capabilities for its state objectives.[61] Recently, connections between Chinese government institutions and private companies doing hacking-for-hire were exposed through a large data leak from the company I-Soon.[62]

All this makes cyberoperations a valuable support tool for executing information operations. Yet, as cyberoperations can do much more than that, they are a topic in themselves and are covered by dedicated chapters in this book.

5.6. News Outlets

Traditional media continue getting stronger globally, and having such outlets under direct or indirect control is valuable for spreading disinformation. There are three main types of new outlets. The first and the most influential are television networks. The second are radio stations, followed by printed newspapers. All three can

[59] Greig, 2022.
[60] Maurer, 2018.
[61] Insikt Group, 2021.
[62] Hawkins, 2024.

use the Internet to reach a broader viewership, but they dominantly operate using traditional distribution methods. This also distinguishes them from Internet-only media. Television and radio are special as they require a licence to broadcast on certain frequencies. The alternative is using satellite to reach an even broader audience.

Establishing television networks with a global reach is an expensive investment, but it is a valuable tool for nation states aspiring to become global forces to spread their influence. The most prominent example in this case is RT, previously known as *Russia Today*, an outlet for spreading Russian disinformation. More common are smaller regional and local television stations. To increase their influence and prospect of surviving, these stations might cooperate or grow through mergers and acquisitions. This way, they can become quite influential, but without proper oversight.[63]

5.7. Marketing Campaigns Support Services

Marketing is a very old discipline and currently a multi-billion-dollar industry, meaning that it has accumulated a great deal of knowledge. Moreover, the market for support activities is quite vibrant. Modern marketing heavily relies on the Internet, particularly social media. Because information operations can be seen as a form of marketing, much of the marketing knowledge and even support tools can be abused for information operations. Tools developed for marketing campaigns can also be abused for information operations.

Malicious users can develop their own tools or use already existing tools, which is much easier. According to the Gartner Magic Quadrant for B2B Marketing Automation Platforms,[64] the leaders in marketing automation platforms are Adobe, Oracle, Salesforce, HubSpot, and Creatio. The key characteristic of marketing automation platforms is their ability to seamlessly integrate different social media platforms and make it much easier to have a presence on all of them.

5.8. Environment to Run ML Models

The final important logistical support is the environment for running ML models. With the increasing capability of ML models and their potential in information warfare, it is expected that their use will increase. Therefore, it is necessary to have an appropriate environment to run the models. In essence, it is necessary to have compute resources, and there are multitude of options for obtaining such resources.

The first option is using commercially available ML models such as ChatGPT. These models are relatively cheap and offer APIs, so they can be accessed programmatically and integrated into one's own applications. On the other hand, the issue for malicious users is that owners of publicly available ML models embed safeguards

[63] *Last Week Tonight with John Oliver*, 2017.

[64] Wagner, 2021.

to prevent misuse and protect users. As such, those models will refuse to generate malicious content. Although these safeguards are not perfect and there are ways to circumvent them, they create an annoyance for malicious users, leading them to use other tools.

Currently, it is not known to the author of this chapter if the cybercrime underground offers the service of running ML models. However, if ML models prove useful to malicious users, there will be a demand for such models, which will provoke the supply part as well.

Another option for malicious users is to buy and use their own equipment. This can range from a single computer to a computer cluster in a dedicated room. Using this equipment, malicious users can train, finetune, and run open-source ML models. As there will be no restrictions on these models' use, they would offer the greatest flexibility with an appropriate price tag.

6. Threat Sources and Actors

Many actors see information operations as a means to achieve their goals. However, throughout much of history, the only ones who could utilise information operations were nation states. In the 20th century, a significant shift occurred as big industries with a lot of resources also started manipulating information to achieve their goals. The prime examples were the tobacco and oil industries, which respectively used scientists with questionable ethical standards to cast doubt on the health damage caused by tobacco[65] and to question research showing how climate change can impact the Earth.[66] Proliferation of the Internet and popularity of social media have caused another significant shift that opened up additional powerful avenues for manipulating public opinion. Finally, the advancement of AI will undoubtedly open up means for manipulating others to achieve some gain.

For all these reasons, the question of "who" is conducting influence operations is not so straightforward as it used to be and is thus difficult to answer. By knowing who is running the information operation, we can determine their motives, capabilities, and resources, which allows us to better protect ourselves, and vice versa. That is, if we know something about the information operation, it will allow us to deduce who is behind it and the take appropriate measures.

The terminology in this subsection is taken from cybersecurity. A "threat actor" or "threat agent" is an entity that initiates a threat:[67] it might be a human being, malware, or an AI/ML model. "Threat sources", on the other hand, are the ones

[65] McKee, 2017.
[66] Hulac, 2016.
[67] Johnson et al., 2016.

with motive, and they control or influence threat agents. Note that it is possible for a threat agent and threat source to be the same, but they are generally separate entities. We use the following parameters to distinguish threat sources. The first is “motives”, which determine why the threat source is doing something. The motive can be to gain (geo)political advantage, spread conspiracy theories because threat sources believe in them, gain competitive advantage, maintain the current market position, etc. The second parameter is “capabilities”, which are the skills and knowledge of people that the threat source has at its disposal. This also includes existing material resources in the form of technology, such as computing power and AI/ML models. The final parameter is “resources”, which represent everything a threat source might employ, including finance, but they take time to operationalise. Resources are also important for persistence, since without resources, capabilities cannot be sustained or expanded.

The most capable threat sources are still nation states. They have the greatest capabilities and almost unlimited resources. Their motives are mainly geopolitical. On the other end of the spectrum are groups and individuals. Their motives can be, for example, political or religious, but their resources and capabilities are not as great as that of a nation state. This does not mean that individuals and, especially, groups cannot obtain a significant number of resources. Groups can be formed from the industry, be politically motivated, etc. Moreover, they can be formal or informal. Formal groups are coordinated and have aligned motives. Informal groups, on the other hand, do not have coordination mechanisms between members, who may have widely different motives that overlap only in some parts that are common to the group.

Attribution is the process of answering the question of “who” is behind an information operation – who the threat sources and threat actors are. Attribution is a much studied problem in cybersecurity where it is considered a difficult issue for several technical and legal reasons.[68] This section presents the technical issues that make attribution a problem and show where the legal issues come into play.

Attribution can be direct or indirect. “Direct attribution” is achieved when there is a clear chain of artefacts that connect an action to a threat source or threat actor. “Indirect attribution” occurs when there is no direct sequence, but we must somehow associate two or more such sequences. In general, attribution is a probabilistic process, wherein we can attribute an action to a threat source or threat actor with certain probability.

As an example of direct attribution, let us say that a threat actor published a post in a public forum using his work machine. In that case, the forum’s server logs will have an entry that contains the Internet protocol (IP) address of where the post came from, and this IP address can be specifically pinpointed to some organisation. The chain in this case consists of the post in the public forum, IP address, and information that this IP address is assigned to a specific organisation. Note that this

[68] Rid and Buchanan, 2015.

is a specific case as a lot of details can break this chain. To illustrate breaking of the chain, suppose that the recorded IP address comes from a dynamically allocated range belonging to an Internet service provider (ISP) that randomly assigns them to different users for a limited amount of time. In this case, to complete the chain, we need information about "who" was using this IP address at a given time, which should be provided by the ISP. Now, here is where the legal issues come into play. To obtain information on who used the IP address, a warrant must be issued to the ISP to disclose this information to law enforcement. However, if the ISP is in another country, the process becomes slower, to a point that can become impossible to obtain the required information due to another country's unwillingness to cooperate.

The above examples used a single technical artefact (IP address) for attribution; however, generally, it is necessary to connect several technical artefacts to identify the threat actor.

Threat actors, especially the more sophisticated ones, actively try to conceal their whereabouts by using different mechanisms and techniques. First, threat actors might compromise a server on the Internet and use it as a steppingstone for the attack. In this case, what the victim can see is the IP address of a compromised host. In addition, if the threat actor used a compromised host in a country that does not want to cooperate, then the victim will not be able to obtain logs from the compromised server, and thus the threat actor's IP address will stay hidden. Additionally, there might not be any logs, they might not be kept for a sufficiently long time, or they might be erased by the threat actor. In any case, this means that it is harder or impossible to reach the threat source. There are many other variations of this theme that achieve the same goal of disrupting the chain of artefacts. Second, several approaches to conceal one's IP address are frequently used on the Internet. The first approach is the use of virtual private networks (VPNs),[69] which allow users to hide their original IP address. The problem with this approach is that the threat actor places trust in the VPN provider, which could be justified in some cases but not in others. Another approach involves using an anonymising network such as Tor.[70] When used correctly, the Tor network makes it almost impossible to find the perpetrator.

Note that the use of direct methods could reveal the threat actors but not threat sources. This should be obvious, as threat sources are the ones executing operations and thus using technical means. On the other hand, threat sources just issue orders, give directions, and are engaged in similar activities so there is no chain of artefacts linking the threat actor to the threat source.

If direct methods fail, we are left to use indirect methods. In this case, we enter into the realm of intelligence, which, by its very nature, deals with uncertainties, clues, indications, hypotheses, etc. As an example of an indirect method, suppose that some disinformation appeared. The easiest way to identify the threat source is to analyse who benefits the most from it. Yet, there is no conclusive proof, as

[69] Khan et al., 2018.

[70] Çalışkan, Minárik and Osula, 2015.

someone else might have initiated the disinformation for certain reasons. In other words, these methods only provide an indication. However, by accumulating indications, we increase the probability until we can treat the inference as highly likely, almost conclusive. Note that in this example, we are deducing the identity of the threat source but do not know the threat actor – unless they are the same.

Finally, it is instructive to read the 2012 blog post[71] by Sophos, which shows how it is possible to identify threat actors using only open sources on the Internet.

7. Example of the Application of Tactics and Techniques

To show how these tactics and techniques might be used, we take a well-known information operation and map it to the proposed tactics and techniques. Note that this is not meant to be a validation step, as it would require much more space than we have at our disposal. This task is left for future work.

There are several known complex information operations whose consequences are still felt. Among these is Operation Denver, an information campaign by the KGB to spread disinformation about AIDS being the product of scientific research. Moreover, denials of the global warming issue still create a lot of obstacles for actions to remedy this situation. We already mentioned the tobacco industry and its fight to prevent the prohibition of smoking. Finally, most recently, COVID-19-related disinformation made it harder to implement appropriate responses to the pandemic. These are not the only disinformation campaigns. For example, because of the current Russian aggression on Ukraine, Russia spread a lot of disinformation to try to induce disagreements and conflicts between Western countries and Ukraine to weaken support for the latter. Moreover, there is an increased level of disinformation activity during each election. Certain publicly available sites monitor disinformation as it appears and try to debunk it.[72]

Disinformation is spread in not only Europe but also Africa and other underdeveloped regions in the world where Russia and other countries fight for influence. This is a huge strategic issue because fighting disinformation "at home" has no effects on disinformation elsewhere; thus disinformation takes root in other places, making it very difficult to counteract it in the future.

Of all disinformation campaigns, we selected the oldest one, Operation Denver, to illustrate the use of tactics and techniques presented in this chapter. This operation was thoroughly analysed and is documented in great detail, making it perfect

[71] Drömer and Kollberg, 2012; unfortunately, the original post is lost due to the changes to the Sophos site. The cited work is a Croatian translation, but you can use Google Translate to translate it into English or any other language.

[72] EU Disinfo Lab, no date; EUvsDisinfo, no date; *Tracking Disinformation and Conflict,* no date.

for our needs in this section. This campaign is also interesting because it occurred before widespread use of the Internet and modern technologies in general, while its consequences are still felt, especially in Third World countries.

Operation Denver,[73] also known as Infektion, was a complex and elaborate campaign by the Soviet Union (threat source) in the 1980s. It used the then newly discovered human immunodeficiency virus (HIV-1) to build a public image that the virus was created in the US in secret military laboratories. Additionally, there was a complex interplay with misinformation spreading from the LGBT community in the US, and multiple threat sources and threat agents were involved. All this makes this case very hard to untangle, but our goal is to identify the information operations run by KGB (threat agent), and we will ignore all other developments, as we believe that this case also falls in the realm of psychological operations.

As already mentioned, a campaign refers to several operations that all support the end-state. The motives and goals of the HIV campaign were to[74] (1) discredit the US and generate anti-American sentiments abroad; (2) reinforce the longstanding false Soviet propaganda of biological warfare activities by the US and counter US reports of Soviet violations of the 1925 Geneva Protocol on Chemical Weapons and 1972 Biological Weapons Convention; (3) undermine US defence arrangements with allied countries and create pressures for the removal of US military facilities overseas by linking the spread of AIDS to the presence of US armed force personnel stationed abroad; and (4) discourage contacts with Americans (including tourists, diplomats, and businesspeople).

The threat source in this case was a nation state, the Soviet Union. The threat actors were the KGB, scientists, and other Eastern intelligence agencies, notably East Germany’s Stasi.

From the perspective of KGB, everything started with a letter published in 1983 in the Indian newspaper *Patriot*, which was a KGB-run operation. Regarding the information lifecycle, the sequence of tactical events for this specific event (letter appearing in the newspaper) was as follows: (1) Generating information: The information purporting to come from an anonymous yet “well-known American scientist and anthropologist” in New York was created. The key points of this letter were the given “facts” – AIDS was created in a laboratory and was developed in cooperation with the US Centers for Disease Control. (2) Production: The text had to be converted into a letter form and mailed to the intended destination while ensuring that it would not be lost. (3) Publication of information: The falsified letter was published in the Indian news outlet *Patriot*. (4) Distribution of information: The initial distribution was done by *Patriot*.

The follow up operation was initiated two years after, when this disinformation was reproduced in the Soviet Union. On 30 October 1985, Soviet newspaper *Literaturnaya Gazeta*, also an outlet for spreading KGB disinformation, published an

[73] Selvage, 2019; Selvage, 2021.

[74] US Department of State, 1987.

article by Valentin Vasilevich Zapevalov. Zapevalov was a threat agent tasked with further spreading the disinformation published in the letter in *Patriot*.

Yet another operation was run during August and September 1986, when a photocopied brochure was handed out before, during, and after a summit meeting of the Non-Aligned Movement in Harare, Zimbabwe. The purpose of the operation was to downplay the green monkey hypothesis regarding the African origin of AIDS.

Again, if we look at the information lifecycle, the sequence of events was as follows: (1) Generating information: This step was a bit more involved as it requested the aggregation of information from several sources. The result was a text that was to be published. (2) Production: This step involved the preparation of leaflets. (3) Publication and distribution of information: In this case, the information's publication and distribution were indistinguishable.

Another operation used falsified scientific research to corroborate the initial thesis of HIV being a biological weapon created in US laboratories. The following tactical steps were used in this operation: (1) Generation: The information was generated by a corrupt scientist, Jakob Segal, who produced flawed scientific research "proving" that HIV was created in US laboratories. The input for this step was the narrative about HIV being created in secret US laboratories. (2) Production: This step was non-existent in this case as everything was done by either the person who generated the disinformation or the publication venue as part of its standard procedures. Thus, it was not under the control of an information operation operator. (3) Publication: The falsified research was published in a journal, which made it publicly available and thus increased the validity of the disinformation. (4) Dissemination: The paper was cited on different occasions and in media outlets as a reputable source to confirm the initial thesis – HIV was created in a secret US laboratory.

In conclusion, Operation Denver was a complex campaign that consisted of several operations spread over many years. The operations were run by different threat actors and threat sources, which were not all mutually coordinated, nor did they have the same motives. Nevertheless, the basic idea of HIV being produced in US biological laboratories suited all threats and was used by the threat sources for their ends, although the explanation for why it was produced differed.

8. Conclusions

Fake news and disinformation in general are significant threats to modern societies and their democracies. There are many documented cases of the negative impact of disinformation on election results, population health, etc. Efforts that try to combat the spread of disinformation exist, but they are lacking, and new approaches must be found and pursued. These approaches must come from the highest levels of political decision-making. Yet, it is difficult to create strategies to address disinformation if there is no systematisation of disinformation activities to describe in a structured and clear way what the adversaries are doing, what they might do, and how the problem of information warfare develops over time. The goal of this chapter was to lay the foundation to solve this issue through the collaborative work of many individuals.

In the beginning, we first clarified the terminology used in this chapter. We started from the basics as there are no official standards or similar regarding the use of terminology in this area. The first contribution of this chapter is viewing information warfare and warfare in general as tactics, techniques, and sub-techniques used during information operations. We also distinguished between information warfare in the narrower and broader senses. Information warfare in the broader sense includes tactics, techniques, and procedures from psychological warfare, political warfare, propaganda warfare, and other warfare types. In this chapter, the emphasis is on information warfare in the narrower sense. Information warfare in the narrower sense does not deal with the question of why there is specific disinformation nor how it affects targets. It only deals with ways of delivering disinformation to the given targets. This approach was inspired by information security. Namely, information security deals with the security of information, but it does not try to understand the content of information or how it impacts users. So, we took the perspective that information warfare deals with how to spread disinformation, while we considered the questions of why it is created and what its psychological and other consequences are as outside the scope of information warfare.

We also dealt with information operations. We reviewed the military operational domains to determine where information warfare fits. We concluded that information warfare is embedded in all military domains as it impacts people as its final target. We also defined the information lifecycle by defining the four phases of generation, production, publication, and dissemination. These four phases are tactical steps we later studied in more detail. We also showed that information has several forms: text, video, audio, pictures, and different combinations thereof. Finally, we analysed the information space and its main elements where information operations take place.

This chapter had the main goal of systematising activities related to information warfare in a way that allows more effective and efficient combating of adversaries who use information warfare. The main inspiration comes from the success of the MITRE ATT&CK pattern database for cyberwarfare. This database contains a list of tactics, techniques, and sub-techniques observed in the real world. It also contains a list of threat actors, along with the tactics and techniques they use. The database is used in discussions on attackers' behaviour as well as in products used for defence, and new uses are constantly being identified. Therefore, in Section 4 Tactics and Techniques, we tried to develop a similar database for information warfare. Because creating something as comprehensive as the MITRE ATT&CK pattern is a huge endeavour, the results presented here should be taken as only a first step.

Certain techniques depend on logistical support, and in Section 5 Logistics Support, we enumerated infrastructure that might be created before certain information operations are enacted and that could be shared between several information operations. We also discussed troll armies, social media bots, interest groups, proxies, cyberoperations, news outlets, marketing campaign support services, and the environment to run ML algorithms.

Finally, we argued that there should be a taxonomy of threat actors and threat sources based on their motives, capabilities, and resources. This is important because we are no longer dealing with only nation states when talking about information warfare. Information warfare can be, and is, used by many other actors, and cataloguing them and identifying their tactics, techniques, and sub-techniques is a valuable addition to a toolbox that allows more efficient and effective suppression of disinformation.

Finally, we considered Operation Denver as an example. We described its operations and showed how the actions taken during this operation can be mapped to our proposed tactics, techniques, and sub-techniques.

In future work, this activity should be more data driven. Namely, data about information operations should be collected, and each information operation should be mapped to the proposed tactics, techniques, and sub-techniques. This mapping would generate feedback on what is good and what needs to be changed. Moreover, a database of threat actors and their activities should be created.

We believe that by expanding the work presented here, more efficient and effective policies and mechanisms can be created to combat information and disinformation operations. This will help achieve the ultimate goal of protecting modern societies and their democracies from the harm caused by disinformation.

References

4chan. (no date). [Online]. Available at: https://www.4chan.org/ (Retrieved: 15 March 2024).

Aro, J. (2016) 'The cyberspace war: propaganda and trolling as warfare tools', *European view,* 15(1), pp. 121–132; https://doi.org/10.1007/s12290-016-0395-5.

Baptista, J.P., Gradim, A. (2021) '"Brave New World" of fake news: How it works', *Javnost-the public*, 28(4), pp. 426–443; https://doi.org/10.1080/13183222.2021.1861409.

Basch, C.H., Meleo-Erwin, Z., Fera, J., Jaime, C., Basch, C.E. (2021) 'A global pandemic in the time of viral memes: COVID-19 vaccine misinformation and disinformation on TikTok', *Human Vaccines & Immunotherapeutics*, 17(8), pp. 2373–2377; https://doi.org/10.1080/21645515.2021.1894896.

Bastos, M., Farkas, J. (2019) '"Donald Trump is my President!": the Internet Research Agency propaganda machine', *Social Media+ Society*, 5(3); https://doi.org/10.1177/2056305119865466.

Çalışkan, E., Minárik, T., Osula, A.-M. (2015) *Technical and legal overview of the tor anonymity network*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. [Online]. Available at: https://www.ukita.co.uk/surveillance/2015/TOR_Anonymity_Network.pdf (Accessed: 14 March 2024).

Cantor, M. (2023) 'Nearly 50 news websites are 'AI-generated', a study says. Would I be able to tell?', *The Guardian*, 8 May 2023. [Online]. Available at: https://www.theguardian.com/technology/2023/may/08/ai-generated-news-websites-study (Accessed: 14 March 2024).

Chang, H.-C. H., Chen, E., Zhang, M., Muric, G., Ferrara, E. (2021) 'Social bots and social media manipulation in 2020: the year in review' in Engel, U., Quan-Haase, A., Liu, S., Lyberg, E.L. (eds.) *Handbook of Computational Social Science, Volume 1*. 1st edn. London, UK: Routledge; pp. 304–323; https://doi.org/10.4324/9781003024583.

Chen, G., Cox, J.H., Uluagac, A.S., Copeland, J.A. (2016) 'In-Depth Survey of Digital Advertising Technologies', *IEEE Communications Surveys & Tutorials*, 18(3), pp. 2124–2148; https://doi.org/10.1109/COMST.2016.2519912.

Chilton, J. (2023) 'The New Risks ChatGPT Poses to Cybersecurity', *Harvard Business Review*, 21 April 2023. [Online]. Available at: https://hbr.org/2023/04/the-new-risks-chatgpt-poses-to-cybersecurity (Accessed: 14 March 2024).

Confessore, N., Dance, G.J., Harris, R., Hansen, M. (2018) 'The follower factory', *The New York Times*, 27 January 2018. [Online]. Available at: https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html (Accessed: 15 March 2024).

Demeku, A. (2023) 'What You Need to Know About Your Engagement Rate on Instagram', *Later*, 14 July 2023. [Online]. Available at: https://later.com/blog/instagram-engagement-rate/ (Accessed: 16 February 2024).

Dinstein, Y. (2011) *War, aggression and self-defence*. 5th edn. Cambridge: Cambridge Univeristy Press; https://doi.org/10.1017/CBO9780511920622.

Dixon, S.J. (2023a) 'LinkedIn – Statistics & Facts', *Statista*, 12 December 2023. [Online]. Available at: https://www.statista.com/topics/951/linkedin/ (Accessed: 14 March 2024).

Dixon, S.J. (2023b) 'Number of X (formerly Twitter) users worldwide from 2019 to 2024', *Statista*, 15 November 2023. [Online]. Available at: https://www.statista.com/statistics/303681/twitter-users-worldwide/ (Accessed: 5 February 2024).

Drömer, J., Kollberg, D. (2012) ‘Istraga bande iza Koobeface zloćudnog koda’ [Investigation of the gang behind the Koobface malware code], *Blogspot*, 22 January 2012. [Online]. Available at: http://sgros.blogspot.com/2012/01/istraga-bande-iza-koobeface-zlocudnog.html (Accessed: 8 June 2024).

Elyashar, A., Fire, M., Kagan, D., Elovici, Y. (2013) ‘Homing socialbots: intrusion on a specific organization’s employee using Socialbots’, *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pp. 1358–1365; https://doi.org/10.1145/2492517.2500225.

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Hamilton, K., Sandvig, C. (2015) ‘“I always assumed that I wasn’t really that close to [her]”: Reasoning about Invisible Algorithms in News Feeds’, *CHI ‘15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 153–162; https://doi.org/10.1145/2702123.2702556.

EU Disinfo Lab (no date) ‘A Vibrant Home for Disinformation Activists and Experts’. [Online]. Available at: https://www.disinfo.eu/ (Accessed: 15 March 2024).

EUvsDisinfo (no date). [Online]. Available at: https://euvsdisinfo.eu/ (Accessed: 15 March 2024).

Facebook (no date) ‘Basic Privacy Settings & Tools’. [Online]. Available at: https://www.facebook.com/help/325807937506242 (Accessed: 28 December 2023).

Farago, L. (1941) *German psychological warfare*. New York: Committee for National Morale.

Fisher, M. (2021) ‘Disinformation for Hire, a Shadow Industry, Is Quietly Booming’, *The New York Times*, 25 July 2021. [Online]. Available at: https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html (Accessed: 21 February 2024).

Gelfert, A. (2018) ‘Fake News: A Definition’, *Informal Logic*, 38(1), pp. 84–117; https://doi.org/10.22329/il.v38i1.5068.

Goldstein, J.A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., Sedova, K. (2023) ‘Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations’, *arXiv*, preprint arXiv:2301.04246; https://doi.org/10.48550/arXiv.2301.04246.

Gómez, A.R. (2019) ‘Digital Fame and Fortune in the age of Social Media: A Classification of social media influencers’, *aDResearch ESIC International Journal of Communication Research*, 19(19), pp. 8–29.

GreenGeeks Web Hosting (no date) ‘WordPress Hosting – Fast, Secure & Managed by Expert 24/7 Support’. [Online]. Available at: https://www.greengeeks.com/wordpress-hosting (Accessed: 15 March 2024).

Greig, J. (2022) ‘Russian government procured powerful botnet to shift social media trending topics’, *The Record*, 20 May 2022. [Online]. Available at: https://therecord.media/russia-botnet-fronton-social-media-nisos (Accessed: 20 May 2022).

Grover, S. (2023) ‘22 Best Ad Networks for Publishers in 2023’, *adpushup*, 4 May 2023. [Online]. Available at: https://www.adpushup.com/blog/the-best-ad-networks-for-publishers/ (Accessed: 11 November 2023).

Hawkins, A. (2024) ‘Huge cybersecurity leak lifts lid on world of China’s hackers for hire’, *The Guardian*, 23 February 2024. [Online]. Available at: https://www.theguardian.com/technology/2024/feb/23/huge-cybersecurity-leak-lifts-lid-on-world-of-chinas-hackers-for-hire (Accessed: 15 March 2024).

Hill, M. (2023) ‘5 ways threat actors can use ChatGPT to enhance attacks’, *CSO*, 28 April 2023. [Online]. Available at: https://www.csoonline.com/article/575205/5-ways-threat-actors-can-use-chatgpt-to-enhance-attacks.html (Accessed: 14 March 2024).

HuggingFace (no date) ‘The AI community building the future’. [Online]. Available at: https://huggingface.co/ (Accessed: 14 March 2024).

Hulac, B. (2016) ‘Tobacco and oil industries used same researchers to sway public’, *Scientific American*, 20 July 2016. [Online]. Available at: https://www.scientificamerican.com/article/tobacco-and-oil-industries-used-same-researchers-to-sway-public1/ (Accessed: 15 March 2024).

Hutchins, E., Cloppert, M., Amin, R. (2011) *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Washington, DC: Academic Publishing International Limited.

Insikt Group (2021) ‘Dark Covenant: Connections Between the Russian State and Criminal Actors’, *Recorded Future*, 9 September 2021. [Online]. Available at: https://www.recordedfuture.com/blog/russian-state-connections-criminal-actors (Accessed: 15 March 2024).

Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C. (2016) ‘Guide to Cyber Threat Information Sharing’, *National Institute of Standards and Technology*, October 2016; http://dx.doi.org/10.6028/NIST.SP.800-150.

Joint Chiefs of Staff (2018) ‘Cyberspace Operations’, *Joint Publication 3-12*, 8 June. [Online]. Available at: https://irp.fas.org/doddir/dod/jp3_12.pdf (Accessed: 8 June 2024).

Khan, M.T., DeBlasio, J., Voelker, G.M., Snoeren, A.C., Kanich, C., Vallina-Rodriguez, N. (2018) ‘An empirical analysis of the commercial VPN ecosystem’, *Proceedings of the Internet Measurement Conference*, pp. 443–456; https://doi.org/10.1145/3278532.3278570.

Kim, H., Stringhini, G., Vodenska, I. (2023) ‘How Climate Disinformation Spreads: Reddit’, *Institute for Global Sustainability*, 31 May 2023. [Online]. Available at: https://www.bu.edu/igs/research/projects/climate-disinformation-initiative/reddit/ (Accessed: 14 March 2024).

Langin, K. (2018) ‘Fake news spreads faster than true news on Twitter – thanks to people, not bots’, *Science*, 8 March 2018. [Online]. Available at: https://www.science.org/content/article/fake-news-spreads-faster-true-news-twitter-thanks-people-not-bots (Accessed: 14 March 2024).

Larson, E.V., Derilek, R.E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L.H., Thurston, C.Q. (2009) *Foundations of effective influence operations: A framework for enhancing army capabilities*. Santa Monica, CA: Rand Corporation.

López, A., Pastor-Galindo, J., Ruipérez-Valiente, J.A. (2024) ‘Frameworks, Modeling and Simulations of Misinformation and Disinformation: A Systematic Literature Review’, *arXiv*, preprint arXiv:2406.09343.

Mascellino, A. (2023) ‘New ChatGPT Attack Technique Spreads Malicious Packages’, *Infosecurity Magazine*, 6 June 2023. [Online]. Available at: https://www.infosecurity-magazine.com/news/chatgpt-spreads-malicious-packages/ (Accessed: 14 March 2024).

Maurer, T. (2018) ‘Why the Russian Government Turns a Blind Eye to Cybercriminals’, *Slate*, 2 February 2018. [Online]. Available at: https://carnegieendowment.org/2018/02/02/why-russian-government-turns-blind-eye-to-cybercriminals-pub-75499 (Accessed: 15 March 2018).

McKee, M. (2017) ‘The tobacco industry: the pioneer of fake news’, *Journal of public health research*, 6(1); https://doi.org/10.4081/jphr.2017.878.

MITRE ATT&CK (no date). [Online]. Available at: https://attack.mitre.org/ (Accessed: 14 March 2024).

Musser, M. (2023) 'A cost analysis of generative language models and influence operations', *arXiv.* [Online]. Available at: https://arxiv.org/abs/2308.03740 (Accessed: 8 June 2024).

Newman, H. (2022) *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM' (prepared in cooperation with Hybrid COE)*. Helsinki: The European Centre of Excellence for Countering Hybrid Threats, NATO Strategic Communications Centre of Excellence.

Oentaryo, R.J., Murdopo, A., Prasetyo, P.K., Lim, E.-P. (2016) 'On profiling bots in social media' in Spiro, E., Ahn, Y.-Y. (eds.) *International Conference on Social Informatics*. Bellevue, WA, USA: Springer International Publishing, pp. 92–109; https://doi.org/10.1007/978-3-319-47880-7_6.

Pantazi, M., Hale, S., Klein, O. (2021) 'Social and Cognitive Aspects of the Vulnerability to Political Misinformation', *Political Psychology,* 42(1), pp. 267–304; https://doi.org/10.1111/pops.12797.

Philmlee, D. (2023) 'Practice Innovations: Seeing is no longer believing – the rise of deepfakes', *Thomson Reuters*, 18 July 2023. [Online]. Available at: https://www.thomsonreuters.com/en-us/posts/technology/practice-innovations-deepfakes/ (Accessed: 14 March 2024).

phpBB (no date) *phpBB forum software*. [Online]. Available at: https://www.phpbb.com/ (Accessed: 15 March 2024).

Richet, J.-L. (2022) 'How cybercriminal communities grow and change: An investigation of ad-fraud communities', *Technological Forecasting and Social Change*, 2022/174; https://doi.org/10.1016/j.techfore.2021.121282.

Rid, T. (2012) 'Cyber war will not take place', *Journal of strategic studies*, 35(1), pp. 5–13; https://doi.org/10.1080/01402390.2011.608939.

Rid, T., Buchanan, B. (2015) 'Attributing Cyber Attacks', *Journal of Strategic Studies*, 38(1), pp. 4–37; https://doi.org/10.1080/01402390.2014.977382.

Ryan-Mosley, T. (2023) 'Junk websites filled with AI-generated text are pulling in money from programmatic ads', *MIT Technology Review*, 26 June 2023. [Online]. Available at: https://www.technologyreview.com/2023/06/26/1075504/junk-websites-filled-with-ai-generated-text-are-pulling-in-money-from-programmatic-ads/ (Accessed: 14 March 2024).

Satariano, A., Mozur, P. (2023). 'The People Onscreen Are Fake. The Disinformation Is Real', *The New York Times*, 7 February 2023. [Online]. Available at: https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html (Accessed: 14 March 2024).

Selvage, D. (2019) 'Operation "Denver": The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985–1986 (Part 1)', *Journal of Cold War Studies*, 21(4), pp. 71–123; https://doi.org/10.1162/jcws_a_00907.

Selvage, D. (2021) 'Operation "Denver" The East German Ministry for State Security and the KGB's AIDS Disinformation Campaign, 1986–1989 (Part 2)', *Journal of Cold War Studies*, 23(3), pp. 4–80; https://doi.org/10.1162/jcws_a_01024.

Shujaat, M., Labeeba, B., Liang, N., Sarah, P., Azza, A., Papotti, P., Popper, C. (2023) *Tactics, Threats & Targets: Modeling Disinformation and its Mitigation*. San Diego: Network and Distributed System Security (NDSS) Symposium.

Smith, B.L. (2024) 'propaganda', *Encyclopedia Britannica*. [Online]. Available at: https://www.britannica.com/topic/propaganda (Accessed: 19 February 2024).

Southerland, M. (2016) *China's Island Building in the South China Sea: Damage to the Marine Environment, Implications, and International Law.* Washington DC, USA: US-China Economic and Security Review Commission.

Stone, J. (2013) 'Cyber war will take place!', Jou*rnal of strategic studies*, 36(1), pp. 101–108; https://doi.org/10.1080/01402390.2012.730485.

Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B. (2020) 'MITRE ATT&CK®: Design and Philosophy', March 2020. [Online]. Available at: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (Accessed: 8 June 2024).

Terp, S.-J., Breuer, P. (2022) 'DISARM: a framework for analysis of disinformation campaigns', *2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management* (CogSIMA), pp. 1–8; https://doi.org/10.1109/CogSIMA54611.2022.9830669.

Lakshmanan, R. (2024) 'New Hugging Face Vulnerability Exposes AI Models to Supply Chain Attacks', *The Hacker News*, 27 February 2024. [Online]. Available at: https://thehackernews.com/2024/02/new-hugging-face-vulnerability-exposes.html (Accessed: 15 March 2024).

Thrush, G., Feuer, A. (2024) 'Ex-Informant Accused of Lying About Bidens Said He Had Russian Contacts', *The New York Times*, 20 February 2024. [Online]. Available at: https://www.nytimes.com/2024/02/20/us/politics/fbi-informant-hunter-biden.html (Accessed: 23 February 2024).

Toloka (no date). [Online]. Available at: https://toloka.ai/data-labeling-platform/ (Accessed: 15 March 2024).

Turner, A. (2024) 'Reddit User Base & Growth Statistics: How Many People Use Reddit?', *bankmycell*, 4 March 2024. [Online]. Available at: https://www.bankmycell.com/blog/number-of-reddit-users/ (Accessed: 14 March 2024).

US Department of State (1987) 'Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-87', vol. 9627, August 1987. [Online]. Available at: https://jmw.typepad.com/files/state-department---a-report-on-active-measures-and-propaganda.pdf (Accessed: 8 June 2024).

Wagner, J. (2021) 'Oracle named a Leader in the 2021 Gartner® Magic Quadrant™ for B2B Marketing Automation Platforms', *Modern Marketing Blog*, 6 October 2021. [Online]. Available at: https://blogs.oracle.com/marketingcloud/post/oracle-named-leader-gartner-magic-quadrant-b2b-marketing-automation-platforms (Accessed: 11 November 2023).

Wardle, C., Derakhshan, H. (2017) *Information disorder: Toward an interdisciplinary framework for research and policymaking.* Vol. 27. Strasbourg: Council of Europe.

Weedon, J., Nuland, W., Stamos, A. (2017) 'Information operations and Facebook' *Facebook*, 27 April. [Online]. Available at: https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf (Accessed: 5 January 2024).

WordPress (no date). [Online]. Available at: https://wordpress.com/ (Accessed: 15 March 2024).

Zahn, M. (2022) 'A timeline of Elon Musk's tumultuous Twitter acquisition', *ABC News*, 11 November 2022. [Online]. Available at: https://abcnews.go.com/Business/timeline-elon-musks-tumultuous-twitter-acquisition-attempt/story?id=86611191 (Accessed: 5 February 2024).

Zannettou, S., Bradlyn, B., De Cristofaro, E., Kwak, H., Sirivianos, M., Stringini, G., Blackburn, J. (2018) 'What is Gab: A Bastion of Free Speech or an Alt-Right Echo Chamber', *WWW '18: Companion Proceedings of the The Web Conference 2018*, pp. 1007–1014; https://doi.org/10.1145/3184558.3191531.

Zhou, R., Khemmarat, S., Gao, L. (2010) 'The impact of YouTube recommendation system on video views', *IMC '10: Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, pp. 404–410; https://doi.org/10.1145/1879141.1879193.

Cybercriminals are Using Paid Ads to Get to Top Cloud Provider's Customers (2015) *TrendMicro,* 1 May 2015. [Online]. Available at: https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/cybercriminals-using-paid-ads-top-cloud-providers-customers (Accessed: 15 March 2024).

Statista (no date a) *Digital Advertising – Worldwide*. [Online]. Available at: https://www.statista.com/outlook/dmo/digital-advertising/worldwide (Accessed: 14 March 2024).

DISARM Foundation (2024). [Online]. Available at: https://www.disarm.foundation/ (Accessed: 16 February 2024).

Disqus (no date). [Online]. Available at: https://disqus.com/ (Accessed: 15 March 2024).

Last Week Tonight with John Oliver (2017) *Sinclair Broadcast Group*, 3 July 2017. [Online]. Retrieved: 15 March 2024, from HBO: https://www.youtube.com/watch?v=GvtNyOzGogc.

Statista (no date b) *Number of monthly active Facebook users worldwide as of 3rd quarter 2023*. [Online]. Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (Accessed: 9 February 2024).

Operation INFEKTION (2024) *Wikipedia*, 14 March 2024. [Online]. Available at: https://en.wikipedia.org/wiki/Operation_INFEKTION (Accessed: 8 June 2024).

Tracking Disinformation and Conflict (no date) *Empirical Studies of Conflict*. [Online]. Available at: https://esoc.princeton.edu/projects/tracking-disinformation-and-conflict (Accessed: 15 March 2024).