CSS CYBER DEFENSE

Cyber Influence Operations: An Overview and Comparative Analysis

Zurich, October 2019

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zurich

ETH zürich

Author: Sean Cordey

Table of Contents

Executive Summary

Objective & Method

Influence and influence operations are nothing new under the sun. They have been exercised since times immemorial by all kinds of actors, whether individuals, groups, or states, and in all kind of forms. States in particular have been using them to further their strategic interests in various contexts, whether during wars, peace or the large spectrum in between. Today, however, the dawn of the information age has seen these influence activities migrate toward cyberspace, making use of the opportunities that new ICT, most notably social media, has to offer.

The overall aim of this trend analysis is to investigate and explore the concept of influence operations and the emerging term of cyber influence operations (CIOs) in order to help foster a clearer understanding of the issue, in particular to enhance policy debate. This analysis looks first at the academic concepts pertaining to influence. Second, it explores the existing definitions of cyber influence and highlights its core features, techniques, and primary targets. Third, it provides a comparative analysis of public CIO campaigns by the US and Russia to map out the evolution and use of CIOs as well as discuss how nation states are leveraging them as tools for pursuing strategic interests.

Results

There are four main conclusions to this report. The first being that, despite the great deal of academic and policy attention dedicated to cyber influence operations since the 2016 US presidential election, the conceptual framework pertaining to them and their related terminology (e.g. "cyber-propaganda", "information cyber operations" or "cyber-persuasion) remains unclear, confused and to some extent incoherent, rendering any rational political or legal debate of the issue complex if not impossible. This report therefore contextualizes and disentangles the definition conundrum surrounding influence operations, and defines cyber influence operations as "activities that are run in cyberspace, leverage this space's distributed vulnerabilities, and rely on cyber-related tools and techniques to affect an audience's choices, ideas, opinions, emotions or motivations, and interfere with its decision-making processes" (Bonfanti, 2019). Influence operations thus encompass not only activities referred to as *information operations* but also non-military and coercive activities (e.g. propaganda). While typically used in times of conflict, CIOs are increasingly also used in times of peace or in the context of mere rivalry.

The second finding is that the targets, end-objectives and strategies of CIOs are the same as with traditional influence operations. However, they differ in that they involve new digital tools (e.g. cyberattacks, bots or social media), which have greatly enhanced psychological warfare techniques and strategies. In this regard, a distinction can be made between two types of CIOs: *cyber-enabled technical influence operations* (CeTIOs) and *cyber-enabled social influence operations* (CeSIOs), with the former relying on a repertoire of cyber capabilities with varying degrees of sophistication to influence targets and the latter focusing on utilizing cyberspace to shape public opinion and decision-making processes through the use of social bots, dark ads, memes and the spread of disinformation.

The third key finding is that cyberspace has acted as an equalizer and enabler for influence operations. Notably, the relatively low cost of entry, widespread availability of tools and possibility to circumvent traditional controls of information have allowed anyone to engage in CIOs. Meanwhile, the ease, speed and virality of information dissemination as well as the increasing reach, scale, penetration, precision and personalization of information targeting have greatly enabled their use. These elements, and the fact that CIOs present an asymmetric option and tool for counterbalancing conventional power at little cost yet with great flexibility, with low risks of detection and escalation but high potential results, has made them particularly attractive for state and non-state actors alike. However, due to the complexity of observing and measuring intent and effect, the medium to long-term strategic implications and impacts of these types of operations are still uncertain.

Finally, the comparative analysis shows that the toolboxes used by individual states are highly dependent on the context and specific objectives they are intended to achieve. Furthermore, autocratic regimes do not restrain their use of CIOs to the same norms as liberal democracies do, particularly when it comes to using them against their own populations and in times of peace. This, however, does not mean that liberal regimes do not exercise cyber influence, but such influence tends to be driven by market forces rather than being driven by market forces.

Disclaimer

The data for this Trend Analysis was drawn from open-source material, which is of great value but also problematic. Indeed, as influence operations and their cyber equivalents are usually covert, details are rarely published and often remain highly classified, with reports only

becoming available when an operation is uncovered and studied in depth. However, there is no obligation to report such cases to the public. Furthermore, relevant reports come mostly from Western sources, which can present some inherent biases. As a result, comparing a complete dataset on CIOs is challenging. The cases discussed here are already in the public domain and reasonably well documented in the cybersecurity and defense literature. As a result, the associated dataset is comprehensive enough to draw the conclusions presented in this Trend Analysis.

1 Introduction

Since the 2016/2017 elections in the United States and Europe, the term "Cyber Influence" (CI) has become a buzzword for many politicians, academics and across the general population. Lawmakers have come to realize that the threats in and through cyberspace do not limit themselves to a nation's critical infrastructure but can also be leveraged to pro-actively shape the social and psychological fabric of society. Accordingly, more and more reports and articles theorizing and studying the matter have been published. Until recently, many reports and policies limited their focus on information security and systems (i.e. integrity, confidentiality, availability). However, the current focus has shifted toward content security, meaning how to secure, monitor and manage the effects of large-scale information sharing across a multitude of social media platforms.

While the issue appears to be novel for many, it goes back to influence operations, which are really nothing new under the sun. All kinds of actors have been practicing influence activities since the dawn of time, from powerful individuals to secret groups and modern companies. States, in particular, have been prone to deploying a variety of techniques to further their strategic interests both domestically and abroad as well as in times of peace and war. Indeed, one only has to look back to the two World Wars or the Cold War to find some preeminent examples.

As such, cyber influence is only the latest adaptation of these time-honed techniques to the modern paradigm and tools that have evolved with recent technological change. It makes use of the novel opportunities afforded by information and communication technology (ICT), networked systems and cyberspace to change or influence an audience's choices, ideas, opinions, emotions, and motivations.

With that in mind, the goal of this trend analysis is to shed light on the concept of *influence operations* and the emerging term of *cyber influence operations* (CIOs). It attempts to answer a number of questions including: What is influence? How has the concept been used and is used today by states? How does cyber influence come into this? How distinguishable is it from traditional influence? What are the core features, techniques, targets and actors of CIOs? What implications do CIOs have for international relations? And finally, how are different states, notably the US and Russia, exercising influence in cyberspace? Are there any discernible patterns and differences between autocratic and liberal regimes?

To answer these questions, this TA is divided into the following four sections: Section 1 explores in depth the concept of influence operations and its affiliated terms, such as political warfare, psychological warfare and information warfare. By examining the definitions,

categories, examples and historical context around these terms and operations, this section aims to disentangle the definition conundrum surrounding the entire field of influence-related terminology. It moreover identifies a number of core attributes which cut across all of the various terms in order to provide a conceptual understanding of influence operations and arrive at a specific and at the same time synthetic definition.

Section 2 examines in depth the "cyber" aspects of influence operations. It defines and frames the concept of *cyber influence operations* before exploring their similarities to and differences from traditional influence operations notably mentioned in this section. Specifically, it looks at the question of targets, objectives, tools, techniques and strategies as well as types of CIOs, two of which are identified, namely *cyber-enabled technical influence operations* (CeTIOs) and *cyber-enabled social influence operations* (CeSIOs). Accordingly, this section therefore examines how digital, information and communication technology has shaped influence operations before discussing the implications of CIOs in terms of attractiveness, legal and international implications.

Section 3 investigates the concrete application of cyber influence today and over the last two decades by means of a comparative analysis of various instances of CIOs deployed by Russia and the United States. It aims to identify patterns (techniques, goals, actors, and targets) of operations and at the same time to place them into context, notably in terms of war, political tension and election meddling. Lastly, it discusses the general implications and differences that can be observed in terms of the use of CIOs between liberal and autocratic regimes.

This technical analysis concludes with the main takeaways of this research as well as a broader comment on the necessity to take action.

2 Summary of the Debate Around Influence Activities

2.1 Influence and Some Historical Examples

Influence is a commonly used form, mechanism, and instrument of power that is, according to Robert Dhal (1957), the ability for "A to have B doing, to the extent that he can get B to do, something that B would not otherwise do". Brangetto & Veenendaal (2016), expanded on this definition by noting that the objective of influence is thus to exert power by shaping the behavior and opinions of a target audience through the dissemination of information and conveying of messages.

Throughout history, national governments and sub-national entities have resorted to using information and influence operations to advance their national and international interests, whether they were of a security, economic or political order (Matteo Bonfanti, 2019). One can find a plethora of examples of such activities, whether in peacetime, within the context of rivalry, political or economic tensions or during open conflict or warfare.

Although influence operations are often regarded as modern inventions, examples can be found throughout human history. In the 12th century AD, Genghis Khan and his tribesmen orchestrated one of the first large-scale disinformation campaigns by widely disseminating rumors about the horde's strength and cruelty to weaken an enemy's resistance (Bentzen, 2018).

Similarly, during World War I, allied airplanes dropped leaflets behind the German lines of defense to erode troop morale and call upon them to surrender. Similar influence operations were also conducted during World War II, the Cold War, the two wars in Iraq, and more recently in Libya, Afghanistan and Syria (Bonfanti, 2019).

During the Cold War, propaganda in all its various forms was the primary tool for pushing ideological narratives into foreign spheres of influence. Such attempts to undermine or change information narratives have continued over the past years, notably in 2016 and 2017, with allegations of Russian interference in Latvian news media and the Indonesian government accusing "terrorists" of releasing fake anti-government news reports.

Table 1: US Military Information Operations Definitions (Joint Chiefs of Staff, 2010)

IO	Description
PSYOP	Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.
MILDEC	Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.
OPSEC	A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. identity those actions that can be observed by adversary intelligence systems; b. determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and c. select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.
EW	Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support
CNO	Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

2.2 The Definition Conundrum of Influence Activities and Techniques

While literature on the subject of information operations has grown exponentially in recent years, there is a fundamental "lack of consensus when it comes to defining all the elements that make up the strategic application of power in the information domain" (Brangetto & Veenendaal, 2016).

Specifically, a number of similar terms have emerged throughout contemporary history that are still extensively used in the literature to describe influence activities. Examples range from propaganda, political warfare, psychological warfare, and information warfare to psychological operations, information operations, neocortical warfare (Conway, 2003; Szafranski, 1997), perception management, and netwar (Arquilla & Ronfeldt, 1997).[1] These various terms are supported by specific context-dependent case studies conducted over time. It therefore seems relevant to review some of the most important terms in chronological order, starting with propaganda.

Propaganda

The origins of the term "propaganda" can be traced back to the *Congregatio de Propaganda Fide,* a 17th-century Catholic committee that fought the Reformation (Walton, 1997). It promoted and advocated for the church's doctrine and viewpoints though various means, including printed pamphlets, seminars and missionaries. More recently, the widespread use of the term by Allied Forces during the two World Wars and the Cold War to refer specifically to hostile opinion-forming activities has strongly entrenched its present negative connotation in popular minds (Marlin, 1989). Indeed, today it is commonly used in both times of peace and war to attack a rival's arguments on the basis that they are unsound, intentionally deceptive, unethical, illogical and aimed at manipulating a mass audience. Within the US military literature, the term "propaganda" has been used to denote lies and distortions normally associated with an enemy and has been differentiated from perception

---

1   This list is non-exhaustive.

management. [2] More specifically, according to Douglas Walton (1997), propaganda is defined by the systematic use and selection of a multitude of means, whether they are arguments, facts or displays of symbols (historical, religious, cultural, etc.). These uses are designed and pursued with strategic intent to appeal to the people, pitch their emotions over rational thinking, and engender political commitments and enthusiasm for change. The goal of propaganda activities is primarily to further an agenda by getting the target to fake or take a particular course of action as well as to change its beliefs. In terms of techniques and forms, the literature (Becker, 1949; Gray & Martin, 2007; Jowett & O'Donnell, 2006)" commonly identifies three different types of propaganda, namely *white, black* and *gray*. The first refers to official or overt propaganda, where sponsorship can be traced back to a recognized actor. The second refers to untruthful and covert activities whose origin is faked or hidden. Lastly, the third is situated in between white and black propaganda, with no clear indication of its origin (or an origin attributed to an ally), and uncertain veracity of information.

Political warfare

The term and concept of *political warfare* has been in use since World War I and was originally coined by the UK (Schleifer, 2014). Its application, however, dates back several decades, if not centuries. According to Blank (2017), political warfare can be regarded as the logical application of Clausewitz's doctrine in times of peace. Specifically, he defines it as "the employment of all the means at a nation's command, short of war, to achieve its national objectives, both in an overt and covert fashion." Relevant activities range from peaceful to aggressive means as well as from overt actions (e.g. political alliances, economic measures, or white propaganda) to covert operations (e.g. support of foreign resistance cells or black propaganda) (Blank, 2017). Violent means notably include tactics such as assassination, paramilitary activity, sabotage, coup d'état, infiltration, revolution, guerrilla warfare, and support of civil war opponents (Blackstock, 1964). Accordingly, influence operations and propaganda form only part of the subversive arsenal.

Psychological warfare and operations

The concept of *psychological warfare* (aka. PSYWAR) was officially developed by the US forces when they joined World War II (Garnett 2002; in Schleifer, 2014) but actors have engaged in it since ancient times.[3] Specifically, the term "denotes any action which is practiced mainly by psychological methods with the aim of evoking a planned psychological reaction in other people" (Szunyogh, 1955). Similar to political warfare, it makes use of various techniques to influence a target audience's values, beliefs, emotions, motives, rationales, or behaviors to reinforce behaviors favorable to the user's objectives. For example, it can be used to strengthen the resolve of allies or resistance fighters as well as to undermine and erode the morale and psychological state of enemy troops. Psychological warfare includes techniques such as manipulation and brainwashing of prisoners of war (Doob, 1949). There are a number of historical examples of specialized units trained for this kind of warfare, notably during World War II by the German and Allied Forces but also by the US Armed Forces during the Korean and Vietnam wars.

Accordingly, PSYWAR closely relates to the use of *psychological operations*[4] (PSYOPs), a term that rose to preeminence after the end of the Korean War and is still in use today as part of the US understanding of information warfare capabilities (Paddock 2010; in Schleifer, 2014). PSYOPs are all about using information dissemination to cripple the target's morale and will to resist. Classical PSYOP techniques include the air-dropping of propaganda leaflets and use of airborne loudspeakers to broadcast demands for surrender (Nichiporuk, 1999.) The underlying rationale thus lies in persuasion through the use of different logics (i.e. fear, desire or ideology) to promote specific emotions, attitudes and behaviors. As such, PSYOPs can be used in times of peace or open war and are considered a force multiplier using nonviolent means in often violent environments. Furthermore, PSYOPs are sometimes divided into three levels (i.e. strategic, operational and tactical) by practitioners to reflect the areas in and the times at which they are expected to be deployed. Each level has its own goal (e.g. to promote a positive image, to deter, encourage, recruit, or lower morale), context, and means of delivery. In the past, the primary means of delivery were newspapers, paper leaflets, and the airwaves (radio and television). Today, soldiers have access via cellular phones to television, e-mails, and social media, as well as old and new media (Schleifer, 2014).

---

2   Defined by the US DoD as "Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations." (Dearth, 2002, in Conway, 2003)

---

3   For instance, Cyrus the Great used it against Babylon, Xerxes against the Greeks, and Philip II of Macedon against Athens.

4   Aka. Military Information Support Operations (MISO) for the US military since 2010.

Information warfare

Another preeminent, but contentious, concept in use since the 80s – mostly in the US military and the intelligence community – is that of *information warfare* (IW), which is motivated by opportunities and vulnerabilities that arise from the dependence of individuals and societies on vulnerable ICT and systems.

The term has, according to Derian (2003), become an umbrella term for conceptually understanding cyberwar, hackerwar, netwar, virtual war, and other network-centric conflicts (Huhtinen, 2007). It refers to the use of "a range of measures or actions (including information & ICT) intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary" (Alger, 1996; in Cronin & Crawford, 1999; Nichiporuk, 1999).

Specifically, IW may include a wide variety of activities, which are closely linked to psychological warfare and include (Kiyuna & Conyers, 2015): collecting tactical information; ensuring that one's own information is valid; spreading propaganda or disinformation to demoralize or manipulate the enemy and the public; undermining the quality of opposing forces' information; and denying information-collection opportunities to opposing forces.

Several IR scholars have extensively written and theorized about IW, notably Schwartau and Libicki, who have both developed different classifications and forms of IW. According to Schwartau, IW can be broken down into three sub-groups, namely personal, corporate and global information warfare (Schwartau, 1994), with the scale and risks increasing between one category and the next. Meanwhile, according to Libicki, IW occurs in seven different forms (Damjanović, 2017; Libicki, 1995): command and control warfare; intelligence warfare; electronic warfare; psychological warfare; hacker warfare; economic-information warfare; and cyber warfare. Over the years, other scholars have, however, divided IW into two main strands, both of which are based on earlier concepts, namely "soft IW", which includes psychological warfare, media warfare and perception management; and "hard IW", which includes net/electronic warfare (Huhtinen, 2007). In any event, IW transcends the traditional domains of warfare and finds itself at the intersection of the information, physical and cognitive/social domains. Its scope goes beyond the military and touches on the political, diplomatic and economic spheres of information.

Furthermore, the action of information warfare is defined as *information operations* (IOs) in the US military literature, a term that has been widely adopted by other actors (Wilson, 2006). As such, IOs are formally (and quite broadly) defined by the US DoD in JP 3-13 as "actions taken in times of crisis or conflict to affect adversary information and information systems while defending one's own information and information systems" (Joint Chiefs of Staff, 2014). Accordingly, IOs traditionally comprise five core capabilities (defined in table 1.1).[5] In addition, these core capabilities are accompanied by related and supporting activities, which are public diplomacy (PD), public affairs (PA), civil military operations, information assurance, physical security, physical attack, and counter intelligence.

As a note, the term computer network operations (CNOs) has been replaced in the more recent literature by cyberspace operations (COs), which the US DoD (Joint Chiefs of Staff, 2018) broadly defines as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace". As such, CO missions can be offensive (OCO), defensive (DCO) and DODIN operations (relating to the ministries' internal networks). In terms of actions, these encompass cyberspace security, cyberspace defense, cyberspace exploitation, and cyberspace attacks. The latter three replace the (still widely used) terms of computer network attack (CNA), computer network defense (CND) and computer network exploitation (CNE)[6]. In terms of techniques, these involve the use of computer technology and cyberweapons to shut down, degrade, corrupt, or destroy various information systems (Dewar, 2017).

This understanding and classification of IW and IOs are, however, neither universal nor do they represent a uniform Western vision. Indeed, many other states, from France to the United Kingdom, have developed their own understandings and doctrines. Another particular case is none other than Russia, which has a long tradition of strategic thinking about the role of information in projecting national power, the best-known examples of which include the active measures the country took during the Cold War. In contrast to the US view, Russia's understanding of IW[7], or information confrontation (informatsionoye protivoborstvo [IP]), does not distinguish between war and peace activities. According to Pernik (2018), "borders between internal and external, tactical, operational and strategic levels of operations, and forms of warfare (offense and defense) and of coercion are heavily blurred". This mostly goes back to the country's national security policy, which is built upon the perception that Russia is under constant siege by foreign influence and thus finds itself in a constant struggle for its survival (Blank, 2017). Furthermore, the Russian approach to IW is much more holistic and whole-of-government. It mobilizes the entire

---

5   For more examples please refer to JP 3−13 and Wilson, 2006.

6   For a detailed classification please refer to the new JP 3−12 on cyberspace operations.

7   In recent years, many Western actors have referred to the Gerasimov Doctrine as the Russian theory of asymmetric and information warfare. It has, however, been debunked by its author Mark Galleoti since.

Russian state (and para-state) apparatus for a wide variety of activities, which include "intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems, and propaganda" (Brangetto & Veenendaal, 2016). As such, most of the Russian information warfare activities are fundamentally non-military (or at least less military than their US counterparts).

Influence operations

Among the IO capabilities described above, four main objectives can be identified, which are: to influence/inform; to deceive; to deny/protect; and to exploit/attack. Following these lines, IOs can be divided into two broad strands:

1. The first is *technical influence operations (TIOs),* which target the logical layers of the information space and include information delivery systems, data servers and network nodes. This strand thus includes operations such as EW, OPSEC, OCO, or DCO.

2. The second is *social influence operations (SIOs)* (aka. information influence activities or cognitive influence activities), which are focused on the social and psychological aspects of information operations and aim to affect the will, behavior and morale of adversaries. This strand includes elements out of the military playbook such as PSYOPS and MILDEC but also public affairs and military-civilian relations.

SIOs can in turn be considered as a subset of *influence operations* but are limited to military operations in times of armed conflict (at least for the US). Influence operations are, however, not limited to the military context, but form part of a larger effort by nations to exert power over adversaries in multiple spheres (i.e. military, diplomatic, economic). These efforts can, for example, involve targeted corruption; funding and setting up Potemkin villages (e.g. political parties, think thanks or academic institutions); putting in place coercive economic means; or exploiting ethnic, linguistic, regional, religious, and social tensions in society (Pamment et al., 2018).

Influence operations are therefore an umbrella term covering all operations in the information domain, including all soft power activities (e.g. public diplomacy) intended to galvanize a target audience (e.g. individuals, specific groups, or a broad audience) to accept approaches and to adopt decisions that mesh with the interests of the instigators of the operation (Cohen & Bar'el, 2017). Specifically, they can be defined as:

"the coordinated, integrated, and synchro-

nized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict aimed at influencing decisions, perceptions and behavior of political leaders, the population or particular target groups (such as experts, military personnel or the media) with the objective of achieving the state actor's security policy objectives" (Schmidt-Felzmann, 2017).

According to Pamment et al. (2018), influence operations are underpinned by a number of core elements. On the one hand, with the exception of public diplomacy, they are – at least in the context of peace – regarded as illegitimate attempts to influence opinion-formation and the behavior of targets (domestically or abroad). This is because they are inherently deceptive with the intention to do harm and disrupt. As such, they constitute interference with normal behavior and opinion formation, but also domestic (democratic) processes and the sovereignty of states. Adding to that, influence operations exploit different sets of existing societal and individual vulnerabilities in opinion formation and the epistemic chain linked to our media system as well as our public opinion and cognitive processes[8]. Furthermore, influence operations are conducted with the intention to benefit and advance the strategic interests of their sponsor, whether this is a state, a non-state or a proxy group. They are conducted in a wide spectrum of settings, which includes the contexts of peace and war but also ambiguous contexts such as hybrid and asymmetric conflicts.

---

8   Please refer to (Pamment & al., 2018) for more information.

3 Cyber & Influence Operations

This section takes an academic and typological approach toward influence operations in cyberspace. It defines the term *cyber influence operations* and explores the similarities and differences between traditional, non-digital influence operations and those conducted within cyberspace. It additionally describes, categorizes and lays out the techniques and strategies of two types of cyber influence operations before highlighting their potential legal and international implications.

they also tend to not distinguish between influence campaigns that may be executed fully or partially in and through cyberspace on the one hand, and cyberattacks that apply cyber capabilities with the purpose of causing certain effects in cyberspace on the other (Pernik, 2018).

This technical analysis consistently uses the term *cyber influence operations* (CIOs) to refer to illegitimate (sometimes illegal) activities that are run in cyberspace, leverage the distributed vulnerabilities of cyberspace, and rely on cyber-related tools and techniques to affect an audience's choices, ideas, opinions, emotions or motivations, and interfere with its decision-making processes (Bonfanti, 2019).

3.1 Definition and Scope of Cyber Influence Operations

The advent of the information age, with its innovative technologies (including the internet) and socio-economic-cultural changes, has progressively transformed the information environment both in its constituent elements and its inherent dynamics, which contributed to the formation of the additional dimension that is cyberspace: a space within which a wide range of actors have access to and the ability to use information for a myriad of activities, including influence-related ones.

This is especially true nowadays, as one consequence of this transformation has been that the control and release of information is no longer monopolized by only a few actors (i.e. the state and accredited media). Indeed, today, any organization or individual can create and disseminate information to a mass audience using internet-connected devices and social media (Bonfanti, 2019). An additional consequence has been the financial reconfiguration of large parts of the media system (i.e. social media, online media), which has prioritized commercial imperatives over the reliability and integrity of information. One common example is the use of misleading information or disinformation for clickbait and advertising revenue.

Accordingly, many traditional influence activities (e.g. propaganda) have increasingly shifted to cyberspace. In the literature, this has notably led to the emergence of a plethora of related terms to denote this particular vector. These include "cyber-propaganda", "cyber-enhanced disinformation campaigns", "cyber-abetted inference", "cyber-persuasion activities", "influence cyber operations", "cyber hybrid operations" and "cyber-enabled information operations", among others. However, these terms are often given and used without a clear definition. In addition,

3.2 Influence Operations and Cyber Influence Operations: Similarities and Differences

The targets, objectives and to some extent strategies/stratagems of CIOs are similar to those of influence operations conducted throughout the last century. However, the tools, actors, scope, scale and availability, are all different.

Targets

CIOs primarily target three levels of order (Pamment et al., 2018):

1. **General societal targeting** aimed at mass audiences by aligning messages with symbols and narratives which are widely shared by a society's population. In addition, the general society is also targeted where attacks are directed against critical societal infrastructures and institutions (e.g. the government, voting systems or energy supplies).

2. **Socio-demographic targeting** aimed at various social groups and networks, whether a region's civilian population or military personnel when used in an ongoing conflict. Messages can be adapted in keeping with general socio-demographic factors, such as age, ethnicity, profession, income, gender, or education.

3. **Psychographic targeting** entailing activities aimed at individuals selected on the basis of their psychographic profiles, be they key decision/policy-makers or ordinary citizens.

Influence activities can thus be differentiated between those that are increasingly "message-oriented" and tailored to specific individuals, narratives or issues, and those that are more "environmentally oriented" towards the general public and the information environment at large.

Furthermore, it must be borne in mind that, while cyberattacks are directly (technically) aimed at target systems belonging to various actors (e.g. businesses, government institutions, media institutions, or political parties), such attacks invariably also have indirect cognitive effects to various degrees and at different levels.

At the same time, it should be noted that CIOs are not only used against foreign targets but can also be used by governments against their own populations. Indeed, during the Syrian civil war, the Assad government targeted its domestic population with social media-based propaganda in an attempt to boost Assad's standing as the legitimate ruler of Syria while trying to dissuade the population from promoting or supporting any of the rebel groups.

Objectives

With regard to the objectives of CIOs, these remain the same as with other influence operations, namely to modify attitudes and shape the target audience's psychological processes, motivations and ideas (Palmertz, 2017). However, specific objectives are varied and depend on both context and target. They include, among others, targeting the civilian population in a particular region with dis/misinformation and cyberattacks to foment distrust toward an opponent's military and government, thus undermining the credibility of authorities and instilling a sense of insecurity. Moreover, in a conflict situation, combatants (and civilians) can be targeted by online counter-propaganda and cyberattacks in order to reduce their willingness to fight, or even to induce them to change sides. This can also be done with a purely disruptive purpose to undermine people's psychological resilience. Conversely, CIOs can also create a positive effect by raising morale and boosting troop recruitment.

One of the main objectives of such operations is, however, to promote, control or disrupt a given narrative. In this regard, and according to Pamment and his co-authors (2018), the aims of influence operations can be divided into three main categories, namely constructive, disruptive, and distractive.

1. Constructive IOs aim to (re)establish a coherent narrative (e.g. an ideology such as communism or capitalism) amongst its targets/audience. For instance, at the general level, this can take the form of mass audience ideological propaganda through various means of information dissemination. At the group level, this can entail the recruitment and promotion of adherent groups (e.g. students) to an ideology, while at the individual level it can take the shape of highly individualized, targeted political propaganda based on interest and preferences.

2. Disruptive IOs aim to be disruptive or destructive toward an emerging or existing narrative. As such, relevant operations are often conducted via highly divisive and contested issues, such as crime and immigration. At a general level, this can mean, for instance, a general polarization of societal actors to foment distrust, while at the group level, it may involve the spreading of disinformation amongst key policy-makers in order to disrupt their decision-making and opinion-forming processes. At the individual level, this can take the form of harassing and discouraging specific individuals from taking part in public debate or taking specific actions.

3. Lastly, distractive IOs aim to draw attention to a specific minor issue or action in order to distract the audience from a key issue. Such activities tend to focus on the information environment, seeking to dilute, flood or poison it with alternative messages. They can, for example, be performed by hijacking public debate through false allegations or highly sensitive topics.

Cyber: an equalizer and enabler

The difference between traditional influence operations and CIOs lies in the tools used and some of the actors involved. This is due to the new features afforded by cyberspace as an operational space. Indeed, modern CIOs are able to exploit not only how information is generated, distributed and consumed on new platforms and services (e.g. social media platforms and services), but also how users and communities interact and establish relationships among themselves (Bonfanti, 2019). Specifically, the use of cyberspace has acted as a great equalizer and enabler for influence operations.

On the one hand, the widespread availability and low cost of entry of cyber technologies and tools has allowed anyone and everyone to engage in influence operations, whether at a small or large scale. In terms of availability, the choice of platforms, vectors, tools, and software is huge, and most of these are easily (and cheaply) available on the internet or the Dark Web. There is, for instance, an extensive market for bots and botnets of all sorts. Meanwhile, there exists a range of forums, threads and chats (e.g. on discord, 4chan, Reddit, etc.) in which communities exchange information and support each

other in using these different tools and new techniques (Baezner, 2018)[9].

The material cost of entry to engage in such activities at the very basic level is also low. Hardware and processing power are increasingly low-cost, and one needs only an internet connection, an internet-enabled device and access to free account-based applications to start to write and spread propaganda. The only resource that can be considered costly is the time needed to set up and engage in these activities, but this can be reduced through optimization and the use of more sophisticated tools and techniques, such as automated bots and possibly artificial intelligence.

In addition, the knowledge needed to engage in basic CIOs is quite minimal. Indeed, only an elementary understanding and knowledge of how to use Photoshop and social media is necessary to create and spread any photomontage. This includes, for instance, widely accessible meme (e.g. Imgflip) or fake tweet generators (e.g. simitator). Accordingly, more sophisticated tools are also becoming increasingly democratized and user-friendly (Chesney & Citron, 2018). FakeApp, for example, allows extremely realistic faceswapping videos to be created using AI[10].

It must, however, be mentioned that engaging in influence operations and actually achieving their goals are two very different things. While the former only necessitates limited skills, the latter requires not only (a certain level of) precise technical knowledge and adequate infrastructure but above all a finely honed understanding of the human psyche, the context in which it operates and the function of the information and cyberspheres. This therefore constitutes a critical element for differentiating between actors with advanced capacities, preparation and intent, and bored or lonely individuals.

Cyberspace also acts as a liberator from traditional controls (and intermediaries) of information, which implies that today anyone can become a propagandist. Indeed, as Cohen (2017) puts it, "the internet has shifted the traditional model of information dissemination via the media and government entities to the dispersal of information by individuals and small groups, who (at times) operate without a clear hierarchical model, and are mostly lacking rules, regulation or government enforcement". Traditional media and the state have lost the monopoly on information dissemination. In comparison to most social media, established news media have editorial guidelines which oversee the type and veracity of information published. Such in-house editorialization is, however, far from openly accessible. Only those with certain credentials – journalists or invited commentators – can access

these outlets. Meanwhile, governments may censor or direct official/conventional media outlets in order to ensure they convey the preferred message and align with the national interests. But in contrast to these, social media and other ICT enable people to bypass these channels and circumvent censorship, as was notably seen during the Arab Spring. Conversely, this delayering and disintermediation (i.e. the loss of intervening controls, such as editors, fact checkers, reputable publishers, social filters, verifying agencies, peer reviewers, and quality controllers) has greatly helped to foster a climate prone to disinformation and propaganda in which the lines between provider and consumer are often indistinct (Cronin & Crawford, 1999; Lin & Kerr, 2019).

Overall, these transformations have allowed a plethora of new actors to engage in influence activities within the information and cyber spaces. This development has been notably reinforced by the relatively high level of anonymity granted to actors, allowing them to operate free of inhibitions (Lin & Kerr, 2019). Among them are traditional actors such as states and state-related groups as well as unconventional ones, such as hacktivists, cyberterrorists, cybercriminals and lone hackers. All of them present new threats and are driven by underlying motives which can overlap due to the multidimensionality and composition of such groups. For instance, states aim to pursue political goals through IW and engage in a wide array of state-sponsored influence activities in order to do so. Cybercriminals, on the other hand, are primarily interested in financial profit but, as such, can also work alongside with or against governments to pursue their economic and political agendas. Cyberterrorists generally aim to exploit cyberspace to cause loss of life, major economic or political disruption, or to create a climate of fear. However, they also use this space to disseminate their propaganda; collect intelligence and funds; radicalize and recruit; and to incite acts of terrorism. Finally, lone hackers also engage in such activities for various reasons, from wanting to demonstrate their technical exploits, to seeking economic benefit or just for the thrill of challenges.

On the other hand, cyber-related technologies have been an enabler for influence activities in several aspects. The first being that the instantaneous nature (or low latency) of interconnected ICT and cyberspace has – in comparison to traditional state or private media, such as printed press – drastically reduced, if not nullified, the time needed to broadcast and disseminate information (Lin, & Kerr, 2019). There is no need to wait for things to be printed, delivered or parachuted. They can simply be published online on a wide variety of platforms, whether it is social media, blogs, Reddit threads or newsletters. In addition, information and messages can take a variety of forms and combinations, from text and photos to video and audio clips, all of which are easily distributed by a

---

9   This was the case during the 2017 presidential election in France, for example, where different national and international groups used various forums to exchange not only tools and techniques but also content (e.g. leaked documents, rumours, text, videos, etc.) for CIOs.

10   This has mostly been developed and used for pornographic purposes.

wide range of content providers (e.g. individuals, bots or states) and prone to manipulation and misappropriation.

At the same time, new cyber-related means of information dissemination have greatly expanded the possible reach and scale of influence activities at very little cost for perpetrators, with information now able to reach a wide and geographically distributed audience and transcend traditional national barriers. Anyone or anybody having an internet connection is theoretically able to publish something capable of being read all over the world. This logic has, however, some limits, with some countries having put in place a number of measures to control and restrict this flow of international information and content for political and social control reasons, with China's "great firewall" being one of the most preeminent examples. Meanwhile, the penetration of social media varies greatly across geographical regions and segments of the population, rendering information dissemination activities highly context-dependent.

As mentioned before, this ease and speed of dissemination means that the control and release of information is no longer the purview of state organizations or established private media companies. This makes control over information – e.g. for social control or political censorship – complex and resource-intensive, especially as responsibilities for relevant actions are not clearly defined. This concerns social media platforms in particular, whose responsibilities regarding the content they convey are still subject to intense discussion. While there is some legal basis for monitoring the veracity of information (e.g. in terms of services), relevant documents are mainly prepared in order to protect social media companies, ISPs and content hosts against criminal liability. The main issues are thus the speed and stringency with which they are enforced as well as the repercussions if they are not.

Furthermore, one could also argue that, in addition to the technical (cyber-related) component which supports the current virality of information, there is also a societal if not psychological aspect to be taken into account. Specifically, the hyperconnectivity of modern societies and the multiplicity of information platforms and media have reinforced a natural human tendency to create, exchange and consume information and news. Indeed, being social and political animals, humans have always had a thirst for more information, news and gossip at all levels of life (e.g. friends, family, politics). In turn, new ICT, above all social media with their sharing functionalities (e.g. re-tweeting or Facebook page sharing), has enabled people to indulge in this need even further. This, alongside the commercial reconfiguration of modern media towards the attention-based business models that are infotainment and sensationalist news, has greatly boosted the propagation and speed of dissemination of information, whether true or false, across wide swathes of society. This is especially true for false information or "fake news" and disinformation,

which tend to diffuse further, faster, deeper and more broadly than truths (Vosoughi et al., 2018). Indeed, this particularly concerns information relating to politics, terrorism, science and natural disasters, as it not only tends to be presented in a novel fashion (and is shared more), but is able to target, trigger and encourage emotional responses and polarized debate (Vosoughi et al., 2018).

This consequently makes online disinformation and propaganda campaigns increasingly effective (Paul & Matthews, 2016), and leads to a vicious circle in which information with little veracity and verifiability is widely shared and then accepted both within and outside social groups, exploiting what some experts call the "illusory truth effect", in which repetition leads to familiarity and thus acceptance. Specifically, the information overload that is concomitant with online information and the internet causes a certain cognitive laziness among users, meaning that they employ various different heuristics and shortcuts to determine whether new information is trustworthy (Paul & Matthews, 2016). Moreover, the development of computer technologies and bots has helped create a sense of legitimacy, allowing fake news to appear legitimate and real, as fake stories are pushed, circulated and engaged with and thus accrue a false sense of social capital (Pamment et al., 2018).

CIOs of this type are also increasingly effective and optimized as the use of targeted online advertisements has allowed for an increasing penetration, precision, and personalization of information targeting. As mentioned earlier, ongoing technological advances, notably in AI technologies, the architecture of the internet and the widespread use of social media platforms (and other apps) have greatly facilitated the collection, analysis (again by AI) and exploitation of psychographic data by states as well as private companies. These technical affordances have enabled the creation and distribution of information (ads or messages) using highly personalized models of contemporary information influence activities at an unprecedented level.

One striking example is none other than the Cambridge Analytica scandal, in which personal data of 87 million Facebook users was improperly shared with the company. The data was then used by a wide variety of actors (political and economic, foreign and domestic) to carry out in-depth electorate analyses and possibly also to target elections in a number of countries, including India, Kenya, Malta, Mexico, the United Kingdom (i.e. the Brexit vote) and the United States (i.e. the 2014 midterms and 2016 presidential election). These targeted activities relied on a number of existing algorithmic recommendations tools (e.g. on Facebook and YouTube) to feed information confirming or reinforcing existing cognitive biases[11], thus creating an increasingly fragmented

---

11 For a detailed list of cognitive biases please refer to Lin & Kerr, 2019.

information sphere which could then be exploited by actors benefiting from the promotion of wedge issues.

On a more general side note, it seems important to recognize the dual use and implications of the above-mentioned technological and societal developments. Indeed, whilst most of these have acted as great equalizers and enablers of influence operations, thus reinforcing the offensive-oriented side of cyberspace, they can also be used for counter-influence efforts. This is increasingly the case with AI, which is now used for the (early) detection of influence campaigns and in-depth analysis of (social) networks.

Types, tools, and techniques

As mentioned earlier, what has changed between Influence operations then and cyber influence operations now are the tools and techniques used. In order to further examine these, one must first make an additional distinction between two categories of CIOs, namely (1) cyber-enabled technical influence operations (CeTIOs); and (2) cyber-enabled social influence operations (CeSIOs). This distinction is also important in terms of counter and protection measures. For instance, better social media content filters and regulations, greater media literacy, or improved educational programs could counter the impact and spread of disinformation. In contrast, cyberattacks and their detection require the development of highly specialized technical and contextual (e.g. culture, language) expertise as well as certain investments (Pernik, 2018). In addition, the choice of response to such cyber influence activities will also depend on the legality or illegality of relevant acts, an element which differs between the two.

1.   Cyber-enabled technical influence operations (CeTIOs)

CeTIOs are a subset of cyber influence operations that are often referred to as cyberattacks in support of influence operations or influence cyber operations (ICOs). Specifically, they affect the logical layer of cyberspace through intrusive means to gain unauthorized access to networks and systems in order to destroy, change, steal or inject information with the intention of influencing attitudes, behaviors, or decisions of target audiences (Brangetto & Veenendaal, 2016). ICOs are thus illegal and criminal activities[12] undertaken in and through cyberspace and therefore qualify as cyberattacks[13].

The spectrum of CeTIOs ranges from low to high-end attacks (Pernik, 2018). As a note, their attribution can be affected by false-flag attacks, where the use of specific techniques (IP spoofing, fake lines of code in a specific language) results in misattribution.

At their lowest end, CeTIOs are aimed at sowing confusion, disseminating propaganda, undermining credibility and trust, or disrupting activities. They are used across the spectrum of peacetime and war (including in low-intensity conflict). Among the most common CeTIO activities are[14] Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, website defacement, social media hacks, and doxing (organizational or individual). Examples include the 2007 DDoS campaign against Estonia, the 2013 hack of Associated Press's Twitter account and the Sony Corporation hack and leaking of sensitive information.

At the middle end of the spectrum, one can find most unauthorized access to information systems (i.e. hacks) by means of cyber capabilities, such as malware (e.g. Trojans, viruses, worms, or rootkits) with the aim to modify data for various purposes, be it to discredit targets or alter perceptions of reality. Examples of such attacks include the hacks of some information systems, which can dramatically undermine trust in national authorities. This was the case in 2015, for instance, when the US Office of Personnel Management was breached and 21.5 million records were stolen. This alleged Chinese espionage stunt became a major embarrassment for the US government and gave the impression that the US authorities were not able to protect sensitive information on their population.

Finally, at the very high end of the spectrum, one finds cyberattacks that include highly sophisticated hacks against, for instance, industrial control systems of critical infrastructure. Corresponding cyber capabilities and vectors include highly customized malware, logic bombs or zero-day exploits. The only example of activities at this level remains the hack of the Ukrainian electrical grid and Triton. Meanwhile, the case of Stuxnet remains debatable, as it seems that the attack was meant to remain hidden, whereas the two previous cases had a clear psychological impact.

Overall, cyberattacks can have effects on one or more layers of cyberspace (Libicki, 2007; in Pernik, 2018): the physical layer (hardware and physical infrastructure such as cables, routers and servers); the syntactic or logical layer (software instructions and rules); or the semantic layer (information in cyberspace). Examples of such effects include rendering laptops dysfunctional (physical), disrupting information stored on a computer (syntactic) or altering such information (semantic).

In addition, cyberattacks can have particularly potent cognitive effects, although these are difficult to measure, above all due to the ambiguity inherent in cyberattacks. Indeed, CeTIOs are not only capable of instilling a

---

12   Intrusion into a computer system for the purpose of espionage is illegal under both domestic law and the Budapest Convention on Cybercrime.

13   Please refer to the glossary for definitions.

---

14   Please refer to the glossary for definitions.

sense of insecurity, but they also (attempt to) disrupt the information environment, which, in turn, impacts on the target population's access, behavior and decision-making processes as information distributed through these systems is controlled (Cohen and Bar'el, 2017). The 2015 cyberattacks against the Ukrainian power distribution grid, which caused 225,000 consumers to lose power for several hours (Baezner & Robin, 2018), and the 2007 cyberattacks against Estonia are two examples which entailed major cognitive repercussions. Indeed, both attacks had significant effects on decision-makers and the population at large (e.g. uncertainty, raised awareness, etc.).

2. Cyber-enabled social influence operations (CeSIOs)

Cyber-enabled social influence operations (CeSIOs) differ from the previous category in that they do not involve the deployment of cyber capabilities to affect either the physical or logical layer of cyberspace. Instead, they target and attack the semantic layer of cyberspace (i.e. information content) through a wide variety of tools and techniques in order to support and amplify various political, diplomatic, economic, and military pressures. As such, they constitute non-coercive or "soft" influence operations. Most of these techniques (e.g. big data exploitation or the purchase of political ads) are not illegal per se but often fall into a gray area of legality, frequently due to the absence of relevant domestic or international legal frameworks and diverging national understandings.

With regard to such activities, Pamment et al. (2018) have devised the following list of techniques and tools most commonly used for the purposes of CeSIOs. Most of these tools and techniques are derived from traditional ones, but have been enhanced through cyberspace:

- **Sociocognitive (communities) and psychographic (individual) hacking** aims to get inside the mindset of a person or group by exploiting cognitive vulnerabilities, psychosocial trigger points and emotions (e.g. fear, anger, hate, anxiety, honor, etc.) to influence their behavior. Contrary to marketing campaigns, cognitive hacking is conducted with the intent to covertly influence an audience and does not need to offer any coherent narrative or even be based on fact in the middle to long term. This is powerfully illustrated by the practice of "swiftboating", in which politicians are subjected to timely smear attacks just before elections without giving them a possibility to respond. One example of sociocognitive hacking was the 2013 social unrest and violence that ensued in India after social media, specifically WhatsApp, helped spread rumors (through an unrepresentative video) which led to severe interfaith violence (Magnier, 2013). Psychographic hacks, in contrast, target individuals by isolating them and mostly rely on the collection of big data and the provision of

commercial services by social media platforms such as Facebook (Pamment et al., 2018). Specifically, psychographic data can be used to design interventions based on individual sentiments. One example are *dark ads*, i.e. ads only visible to the user and designed to influence (e.g. politically) on the basis of their psychographic data. However, the identities of those targeted, and the messages they are targeted with, remain clandestine, rendering such influence operations highly potent and discreet. Psychographic ads were, for instance, used on Facebook and paid for by the Internet Research Agency (IRA), an organization with alleged links to the Kremlin, during the 2016 US presidential election. Most of its (over 3000 types of) ads focused on controversial topics (e.g. race, gay rights, gun control and immigration) to further polarize the political debate and public (DiResta et al., 2018).

- **Social hacking** aims to exploit vulnerabilities arising from sociocognitive features of the human mind, notably our tribal nature and drive for in-group conformity. This is particularly prevalent on social media, where humans are vulnerable to the exploitation of various group dynamics. Social hacking can be categorized into three main groups: harnessing social proof, the bandwagon effect, and selective exposure. The first involves the exploitation of people's tendency to believe something not based on sound arguments but because a lot of others seem to believe it (Pamment et al., 2018). In this regard, likes and recommendation algorithms in social media are primed to push disinformation and propaganda more readily than other types of information. The second effect relates to the known phenomenon of ideas self-amplifying and becoming more widely accepted to an ever greater degree the more "popular" they become. While present in many domains (e.g. fashion), this phenomenon is especially preeminent in politics, where the deceptive technique of *astroturfing*, i.e. "suggesting that there are a lot of people who support a political agenda, while in fact there is no such support" (Pamment et al., 2018), is widely used. Lastly, algorithms on social media platforms can enable forms of selective exposure by contributing to the creation of filter bubbles or echo chambers, with the former referring to a state of intellectual isolation resulting from algorithmic personalization and the latter describing "organically created internet sub-groups, often along ideological lines, where people only engage with others with which they are already in agreement" (Bright, 2016). These can lead to polarization, a fragmentation of online opinion and political division, particularly given that social media are increasingly used as media sources and platforms for information, as well as for the reinforcement (radicalization) of existing ideologies.

- **Para-social hacking** refers to the exploitation of para-social (i.e. illusionary) relationships, which occur when individuals experience one-sided relationships as being two-sided (i.e. symmetrical and reciprocal). Social media, such as Instagram, Twitter or Snapchat, and the celebrity culture have allowed everybody to build immediate and intimate para-social relationships with strangers, celebrities and decision-makers, enabling them to share information and messages directly, bypassing the scrutiny of classic gatekeepers such as journalists. In this context, there are three possible forms of exploits: influencers providing information directly to their followers (fake friends); friendship networks (e.g. Facebook) being exploited to share content uncritically, thus contributing to the spread of propaganda or disinformation (faked friendly); and propagandists posing as ordinary people, making their messages less threatening, seemingly more authentic and more easily shareable.

- **Disinformation** is an ancient technique based on the distribution of false or partial information intended to mislead and deceive. The term remains highly contested and elusive in both relevant literature and the public debate, and the popularization of new terms such as "fake news" has not helped the discussion. For the purposes of this analysis, disinformation strictly refers to "news articles that are intentionally and verifiably false and could mislead readers" (Allcott & Gentzkow, 2017). As mentioned earlier, digitalization has had a powerful impact on the ease, speed and effectiveness with which disinformation is created and disseminated. Without going into excessive detail, one can differentiate several types of disinformation, ranging from slightly illegitimate activity regarding selective facts to the disruptive creation of fake news outlets. More specifically, disinformation activities include *advertising, satire, propaganda, misappropriation, manipulation* and *fabrication* (Pamment et al., 2018), with the degree of illegitimacy escalating as follows: selective facts < out-of-context information < lying < creation of false facts < denial of attempts to correct < creation of fake platforms or media.

- **Forging & leaking** refers to the illegitimate dissemination of falsified evidence (e.g. on social media or the Dark Web) with the aim of propagating falsehoods, fueling misleading narratives, and discrediting associated parties, as well as "cultivating distrust among citizens and inducing them to question the integrity, reliability and trustworthiness of the media" and public institutions and figures (Pamment et al., 2018). Relevant activities can include the use of fake letterheads, official stamps and signatures, sometimes combined with the leaking of secret communiqués (Pamment et

al., 2018). A well-known example is the large-scale Russian-linked "tainted leaks" campaign against government agents, academics (e.g. David Satter), activists (e.g. the Open Society Foundation) and journalists (Hulcoop et al., 2017). These leaks have illustrated that the internet and social media provide a convenient platform for spreading and amplifying forgeries and leaks. In addition, by blurring the line between truth and falsehood, this technique tends to distract decision-makers and victims by shifting the burden of proof, contributing not only to policy paralysis but also to a certain extent to cynicism and fatigue towards key institutions.

- **Potemkin villages of evidence** refer to the attempt to set up intricate institutional networks that are controlled and used by actors as a fact-producing apparatus for the promotion and amplification of specific narratives. Potemkin villages can, for instance, consist of an array of illegitimate or fake research, (online) journals, NGOs or thinktanks that produce studies, working papers, conferences, etc. to present the respective narrative as a product of careful scholarly consideration. As such, they tend to exploit the *Woozle effect,* which refers to seeing what one is expected to see rather than what is actually there, and assuming that well-referenced sources are necessarily true (Pamment et al., 2018). Persistent examples in Western literature are the Russian-sponsored online journals RT-news and Sputnik. However, it should be noted that these are not the only ones, and some Western online news could also be considered to fall within this category.

- **Deceptive identities** refer to the exploitation and transfer of legitimacy from a legitimate actor or platform to an illegitimate one by *shilling, impersonating* or *hijacking* (Pamment et al., 2018). Shilling involves a person engaging with a particular subject (e.g. through marketing or a review) jointly with the actor concerned, for example someone writing a glowing customer review or answering their own questions under different identities to simulate a debate. Impersonators, as suggested by the term, pretend to be someone else (whether online or offline) to better spread disinformation, while hijacking refers to websites, hashtags, memes, events or social movements being taken over by a hostile or other party for a different purpose, whether to disrupt or to disseminate disinformation. Deceptive identities can be generally grouped into first-hand (i.e. actors assuming the role of someone else) or second-hand identities (i.e. actors assigned an identity by someone else, e.g. being cited as an expert in matters outside their sphere of knowledge) (Pamment et al., 2018).

- **Bots & Botnets**: Short for robots, bots refer to "a piece of automated computer software that performs highly repetitive tasks along a set of algorithms" (Michael, 2017; in Pamment et al. 2018). There are myriads of bots, many of which can be and are used for legitimate and useful purposes (e.g. crawler, monitoring, aggregator, or chat software), but a number of bots are used for nefarious reasons, such as spreading disinformation and illegitimate content, price scraping, spamming forums, web analytics, DDoS, distributing malware, and other scams (Pamment et al., 2018). As such, bots are powerful tools used to support information influence activities, as they can easily mimic organic behavior in order to mislead, confuse and influence publics beyond their own social networks. In terms of influence operations, there are four main social bots in use: hackers, spammers, impersonators and sockpuppets. Hackers are employed in ICOs to attack websites or networks or help establish botnets used for DDoS attacks. Spammers are created to post content in forums or commentary sections (including malicious links for phishing) in order to help spread disinformation and other illegitimate content, or simply to crowd out legitimate content. Impersonators focus on replicating natural behavior in order to best engage with political content on social media platforms or to scam people (Pamment et al., 2018), while sockpuppets are semi-automated lookalike or imposter accounts controlled and coordinated by individuals to conduct false-flag operations or to disseminate disinformation. Overall, social bots and botnets can act as very efficient amplifiers for other influence techniques at a very low cost. They are able to exploit social and cognitive (cf. bandwagoning) as well as technical vulnerabilities of social media platforms (e.g. trending algorithms, friend lists, recommendations or hashtags) to reinforce the virality and penetration of specific messages and narratives.

- **Trolling & flaming** refers to users of (or social bots on) online social platforms deliberately trying to aggravate, annoy, disrupt, attack, offend, or cause trouble by posting provocative and unconstructive content (Moreau, 2017). Trolling generally targets particularly naïve or vulnerable users, while flaming aims to incite readers in general (Herring, 2002). A distinction is generally made between classic and hybrid trolls, with the former being ordinary people engaged in trolling for the sake of some personal motivation or attention-seeking. While often not fundamentally politically engaged they can, however, be recruited by actors within the context of information influence campaigns to unwittingly contribute to the spread of disinformation. The latter operate under the direction of someone else, most often an organization, state or state institu-

tion (NATO, 2016) with a clear instrumental purpose often connected to communicating a particular ideology to a particular target audience in a systematic manner. They include both the highly organized trolls working in "troll factories" and individual trolls operating in a less organized manner under the influence of someone else. As such, trolling and flaming are particularly potent in polarizing debates, silencing opinion, distracting online debate and generally disrupting the formation of public opinion (Pamment et al., 2018).

- **Humor & memes** refer to the use of humor as a "communication tool that entertains, attracts attention [and] serves as light relief" (NATO, 2017), but which, at the same time, also serves to covertly manipulate and influence "hearts and minds" to advance goals and agendas not recognized by the audience. Indeed, humor is particularly powerful, as it causes people to be less guarded and more open to sensitive issues. It can influence ideas, which then shape beliefs, and subsequently generate and influence political positions and opinions. On the internet, a commonly used and potent vector for humor and influence are "memes", which are more than just funny pictures with jokes written on them. Indeed, they are expressions of shared cultural ideas, making them immediately appealing and thus hard to avoid. Furthermore, their interpersonal, ambiguous and ready-to-be shared simplistic design gives them not only a high viral potential but also a high acceptance potential (as they come from within people's own social networks, cf. availability bias). As such, they are ideal tools for legitimizing fringe or controversial ideas, opinions and narratives, and for ridiculing, humoring and joking to "weaken monopolies of narratives and empower challenges to centralized authority" (Pamment et al., 2018). Other related examples include humoristic GIFs, caricatures, and videos.

Overall, CeSIOs and relevant campaigns use a variety of strategies, most of which were deployed by traditional influence operations in the past but now find themselves enhanced by cybertools. The following is a non-exhaustive but synthetic list of such strategies (Pamment et al., 2018):

- **Black propaganda** and the creation and dissemination of fake evidence through social media to spark social outrage.

- **Point and shriek** takes advantage of the extreme sensitivity of certain groups in contemporary society, in particular groups that are often also highly active on social media and well aware of the viral dynamics of the hybrid media space.

- **Flooding** is a strategy in which the information space is overloaded with conflicting information to hamper the assessment of information credibility.

- **Cheerleading** operates in the same manner as flooding but with a limited number of more or less spuriously substantiated *narratives,* pushed via multiple channels and amplified by *botnets,* in order to overload the target system's capacity to differentiate credible from non-credible information.

- **Raiding** is a coordinated attack on an information arena to crowd out and silence opinions and exhaust others through disruption. This can be achieved via a variety of tools, such as spammer bots, trolls or DDoS attacks.

- **Polarization** has been observed during the US election. This strategy aims at supporting two extremes of a specific issue to force mainstream opinions into one of the two. To achieve this, a wide array of tools can be used, from social and parasocial hacking to trolling, disinformation and memes.

3.3 Potential & Strategic Implications

As shown by the increasing use and research, cyber influence activities, whether cyber-enabled influence activities or cyberattacks in support of influence activities, have gained considerable traction in recent years, as both large and small actors have come to recognize their potential. This trend will surely continue in the future. More specifically, CIOs are particularly attractive as they represent (1) a good counterbalance to conventional power (at little cost yet large flexibility) with (2) low risks of detection and escalation but high potential results.

Indeed, as mentioned previously, the cost of entry and resources of CIOs, whether in terms of hardware, software or knowledge, is very low in comparison to traditional influence operations. Cyber Influence tools are easily available and affordable. In addition, a wide variety of them exist, many of which are inter-operable, allowing for great operational flexibility and fluidity. An actor is thus not only able to easily vary and adapt the frequency, scalability and intensity of their operations, but also to precisely tailor them to the required context and targets (Cronin & Crawford, 1999).

Cyber influence capabilities in particular present a number of interesting features for nation states' influence operations. Indeed, they are inherently versatile,

ubiquitous and uniquely secretive, allowing states to operate in the gray area between peace and war. They are also incredibly flexible in their use and can in certain cases even substitute conventional and unconventional capabilities. As such, they can be used for standalone or support operations. Potential applications include, among others, preparation for kinetic battle (e.g. during the 2008 Russo-Georgian war) or "intelligence, reconnaissance, surveillance and psychological operations, as well as for signaling deterrence, for discreet sabotage and for widespread disruption" (Blank, 2017). Besides, the same tools and exploits can be used for multiple purposes and be further improved over time (e.g. the Black-Energy series of Trojan software). In addition, cybertools present other advantages in that they can be turned on and off according to need (and context) and are mostly non-lethal (cf. international law implications), temporary and reversible, which further reduces the risk of escalation.

In turn, these factors and the rapid growth of communication technologies underpinned by social media have provided a great number of (new) actors (small non-state as well as state) with a way to (counter)balance conventional capabilities of conventionally powerful states and further their political and strategic interests without the use of force. This is especially true for small non-state actors which, given their size and internal processes, have relatively high operational agility compared to established bureaucracies when it comes to accessing and utilizing new technologies (Marcellino et al., 2017).

At the same time, cyber influence operations present a limited risk of escalation for state actors because they do not constitute a "use of force" under existing international law, which would trigger retaliation and self-defense. The only exception would be, according to the non-binding Tallinn Manual, high-end cyberattacks causing physical harm and destruction. As such, most CIO activities are conducted in the gray area between war and peace, and they are usually not prohibited under international law, which considers them as hybrid threats alongside other types of non-military threats such as disinformation and diplomatic, economic or military pressure. Similarly, many of the cyber-enabled influence activities used to exert political influence in democratic countries are legal (e.g. big data, dark ads, social bots).

This is particularly true as under customary international law a state can only be trialed for breaching its international obligations, for instance violating another state's sovereignty or the principle of non-intervention, if its responsibility as an actor can be confirmed. In other words, it is necessary to determine whether that state exercises "effective control" over the group or organization conducting the influence operations in question (Pernik, 2018). Cyberspace, however, makes it complex to do so.

The problem is thus threefold, namely one of detection, scrutiny and attribution.

Indeed, detecting middle to high-end cyberattacks in support of influence operations can be difficult. Attackers can often operate undetected over long periods of time, with the average time to detection of cyberattacks being 200 days (Pernik, 2018). Low-end cyberattacks, such as DDoS or social media hacks, are, however, by their nature much more visible. With regard to CeSIOs, such as social media and dark ads, their detection can be somewhat difficult, at least for the targeted audience. This is even more true as actors engaging in influence operations on social media can count on the – more or less subconscious – support of "useful idiots", i.e. users, who uncritically process and disseminate information further, thus amplifying the magnitude of the respective operation while blurring the traceability of such CIOs (Bonfanti, 2019; Lin & Kerr, 2019). One must however note that the new social media transparency guidelines enacted and enforced after the 2016 US elections have somewhat improved traceability, at least with regard to money trails.

On a strategic level, it is, however, problematic to determine the efficiency and direct/indirect cognitive effects these cyber influence operations have on populations and politics with any degree of certainty. As a result, analyzing their effects and their perpetrators' possible intentions (or plans), and understanding their intended messages is highly subjective and difficult to prove based on sound evidence, mostly because of secrecy (Pernik, 2018). Indeed, as Allcott & Gentzkow's study (2017) has shown, it is possible, though potentially difficult, to measure changes in opinion or behavior or shifts in government policy resulting from CSIOs from a methodological perspective. Nonetheless, given the ambiguities surrounding cyberattacks, a negligible cause-and-effect relationship between specific cyberattacks and shifts in public opinion can certainly be assumed (Pernik, 2018).

This lack of observable and tangible effects limits the available response options in turn. To date, there have only been out-of-domain responses to foreign CIOs in times of peace, and their effectiveness still needs to be proven. Such responses include, for instance, the diplomatic and economic sanctions enacted against Russia by the Obama administration after Russian interference in the 2016 elections. Moreover, when it comes to Western countries, the legality of and capabilities (e.g. resources, language and cultural knowledge) for possible in-domain responses remain highly debatable. In times of war or conflict, in contrast, greater escalation and stronger responses have been observed, with the US online counter-propaganda efforts against ISIS constituting a notable example.

For its part, information scrutiny and monitoring is made increasingly difficult by the widespread use of social media and their inherent designs, which tend to promote the dissemination of information without any regard for the review or traceability of sources. Memes, photos and videos are particularly good vectors, as they offer only fragmented information without ascertainable factual content or identifiable source but are widely shared by friends or promoted by social media algorithms. Furthermore, the fast-moving nature of social media and information technologies requires states (or interested parties) to assemble a wide array of (evolving) techniques and technologies to quickly identify, monitor, and counter adversaries' influence operations.

Meanwhile, the attribution of specific cyberattacks or influence operations often remains difficult, given the prevailing anonymous targeting in cyberspace, thus allowing for a certain degree of plausible deniability even where the source of an attack has been more or less established (Brangetto & Veenendaal, 2016). This is notably the case with online propagandists, who are able to hide behind pseudonyms and automated botnets, as well their freedom of opinion, when pilloried.

There are, however, a number of caveats to be taken into account when considering the potential of cyber influence operations: First, that TeCIOs can easily spiral out of their operators' control. The use of sophisticated malware can, for example, be a wild card, as once such malware is in the open, it is uncertain whether it will achieve the desired effect, and there is always the possibility that an operation may backfire. Adversaries may replicate, reverse-engineer or proliferate malware, for example, in order to use it against the original owner.

Second, the striking power of CIOs cannot be compared to that of nuclear weapons, for example. Indeed, the power these operations wield is primarily psychological in nature, and part of the target population may therefore be immune to their effects. This is particularly the case where the rule of law is underpinned by strong institutions and traditions (Lin & Kerr, 2019).

Third, the effects of cyber operations are difficult to foresee and limit to specific targets, with the exception of highly sophisticated cases (e.g. Stuxnet). The level of downstream escalation (e.g. political or diplomatic) is always uncertain. Once an attack is launched, it can result in unintended consequences, go viral, cause unexpected damage or even have the opposite effect in the long term, for example by raising awareness of the issue concerned.

Finally, the real medium to long-term strategic impact of CIOs is difficult to assess. Indeed, as mentioned earlier, their intent, effect and objectives are not only difficult to observe but also to measure. Furthermore, the chaotic/inconsistent and operational forces that seem to drive these operations raise the questions of (1) the necessity for strategic thinking in this regard, and, most importantly, (2) the associated costs.

4 Comparative analysis: American and Russian Cyber Influence Operations

The race for influence in cyberspace is attracting ever greater attention. This section therefore adopts a more empirical and qualitative approach towards CIOs. Based on the framework described in the previous chapter, it thus compares the use, scope and objectives of various instances of CIOs conducted by two key actors in this field, namely the United States of America (USA) and the Russian Federation (RUS). This analysis first outlines and summarizes the main results before discussing the trends that can be taken from them.

With that in mind, the analysis thus compares six cases of Russian CIOs and four by the USA (including its involvement in NATO operations), all of which are situated at different points on the scale ranging from peace to war. At the highest end of the scale, there are six wars, namely the 2008 Georgian war; the Ukrainian conflict since 2014; the NATO and US operations during the wars in Kosovo (1998), Afghanistan (2001–present), and Iraq (2003−2011); and the military intervention against the Islamic State of Iraq and Syria (ISIS) (around 2015). The analysis additionally includes two cases of geopolitical tensions in the 2007 Estonian cyber operations and the 2015/2016 Russo-Turkish crisis following the Sukhoi Su-24 shootdown and the assassination of the Russian ambassador. Lastly, it also includes two cases of election meddling, namely in the US and French presidential elections of 2016 and 2017 respectively. Many more cases could have been selected, particularly in the last two categories, but this would have gone beyond the scope of this report. The analysis concludes with general remarks concerning the norms of using CIOs in liberal and autocratic regimes.

4.1 Methodology

From a methodological standpoint, the USA and RUS were chosen because relevant literature identifies them as the two states with the most highly developed and mature information warfare and influence operation strategies and tactics. While the People's Republic of China and the United Kingdom have also developed similar capabilities, they are not examined here due mainly to a lack of open sources and the limited scope of this study. Meanwhile, there is an extensive body of literature (mainly from Western sources) on Russian and American information and influence warfare, which has focused increasingly on cyber influence operations since the 2016 US presidential election and the various elections in Europe the following year. As a result, there are a number of open-source documents in the form of testimonies and reports by various institutions, on which this analysis and comparison is based. This method, however, entails a number of caveats, notably concerning the veracity and accuracy of these sources, which can never be fully guaranteed. Moreover, a certain bias regarding Russian operations must be kept in mind, as most of the literature comes from the West, whereas Western influence operations are only openly described and studied in a limited fashion and only in what is considered a legitimate context, namely war. A final but important caveat is that the comparison is based on political attribution, which is not always confirmed (including technically).

4.2 Presentation of Results and Discussion

Table 1.2 presents the results of the comparative analysis. The sources used for this table are listed in the annex. Relevant observations are presented in three parts based on the context of each CIO, namely conflicts and political tensions during and outside of election periods.

Conflicts

Open conflicts are prone to the deployment of CIOs. Among the conflicts examined, the Ukrainian conflict and the military intervention against ISIS stand out as those in which the broadest range of operations were conducted, including tools and techniques pertaining to both types of CIOs. However, these did not take place in isolation from the remaining approach taken by security forces in either of these conflicts, which entailed a military and tactical operative dynamic on the ground as well as in cyberspace.

The Ukrainian conflict involved the most extensive hybrid warfare operations with a combination of a wide array of tools, ranging from massive propaganda efforts (notably on social media) to highly sophisticated hacks (i.e. the 2015 attack against the Ukrainian power

grid) and the use of troll farms. Most of Russia's cyber operations (e.g. operation Armageddon) were highly coordinated and systematic and largely coincided with Russian military strategic interests in the region. The various CIOs in this conflict targeted a highly diverse group of actors, from enemy military personnel and the general population to media outlets and state institutions alongside international institutions such as NATO. Accordingly, they served a great variety of objectives, both nationally and internationally, depending on the targets. This notably included demoralizing enemy troops; encouraging allied forces; instilling distrust and skepticism toward the Ukrainian government; controlling a given narrative; and discrediting political and military figures. In addition, this conflict is the only known case in which a highly sophisticated cyberattack was conducted (against the Ukrainian electricity grid). Furthermore, it is also the only case in which doxing was reported (e.g. Catherine Ashton's telephone recording or the American ambassador's correspondence, to cite just a few), as well as one where narratives were manipulated to deny specific actions, such as the presence of Russian troops in Donbass or the downing of flight MH17 in 2014.

The military intervention against ISIS, in contrast, was a game changer for the USA as far as CIOs are concerned. There is wide agreement that ISIS's omnipresence on and capacity to act via social media (e.g. for propaganda, recruiting, raising funds, etc.) was a wake-up call for the USA to reclaim the information space. As a result, the USA developed various responses, including CIOs[15], notably CeSIOs focusing on social media messaging, such as the "think again, turn away" campaign. The USA further runs activities in various agencies across the state, including the US Department of Defense's (DoD) WebOps (part of CENTCOM), which focus on disrupting and countering ISIS propaganda; exposing ISIS hypocrisy and crimes, notably through the use of defectors to prevent recruitment; and mobilizing ISIS opponents (Parrish, 2016). Alongside these, the Department of State disseminates its messages and narratives through its network of unidentified actors and individuals (e.g. foreign governments or leaders of Muslim communities) to reach a wider audience (Tucker, 2016). In contrast to the Ukrainian conflict, CeTIOs such as DDoS, defacement and doxing were used relatively less frequently, or at least have not been openly reported. There were cases of hacks, including the 2016 Operation Glowing Symphony, which served a range of purposes from destroying propaganda material to instilling a sense of insecurity, and deceiving and forcing individuals to expose their positions (before being targeted by drones) (Cohen & Bar'el, 2017). The long-term effectiveness of these operations has, however, been

widely debated. As in the Ukrainian conflict, CIOs targeted a broad range of actors at multiple levels, from ISIS combatants and propagandists to groups at risk of falling for ISIS propaganda.

On a more general note, CIOs conducted by Russia and the USA differ in terms of the actors performing them. Indeed, Russia seems to (or at least used to) collaborate with external actors for low-end cyberattacks. This was notably the case first in Estonia in 2007, and then in Georgia a year later. In both cases, links could be established to the criminal/mafioso organization the Russian Business Network (aka. R.B.N.) (Blank, 2017). In the Georgian conflict, relevant activities where closely coordinated with Russian military operations, with times, tools and targets being listed on hacker forums. CIOs served as first strikes to degrade the Georgian government's ability to counter the Russian invasion by disrupting communications between it and the Georgian people, stopping a large number of financial transactions, and causing widespread confusion (Blank, 2017). The involvement of Russian patriotic hackers called the Nashi Youth Movement has also been reported (Baezner & Robin, 2018). While this group was officially disbanded in 2012, it is suspected that former members have continued to perpetrate cyber-activities against what they perceive to be enemies of Moscow, notably in Ukraine (Denning, 2011).

Georgia was therefore Russia's first attempt to combine kinetic and cyberattacks against command-and-control and weapons systems on the one hand, and information psychological attacks against media, communications, and perceptions on the other (Blank, 2017). In Ukraine, it is suspected that the Internet Research Agency (IRA), an organization with alleged links to the Kremlin, took up the RBN's activities alongside social media-related CeIOs (e.g. trolling, bots, misinformation, etc.). Sophisticated hacks have, however, been attributed to pro-Russian hacker groups (CyberBerkut), who have not been proven to have direct links to the Russian state but are suspected to be the Russian cyberespionage group APT28 (Bartholomew & Guerrero-Saade, 2016). The implication of military units is not disclosed, but highly likely.

In contrast, the US tends to rely mostly on its diplomatic, military and domestic personnel to perform CIOs. As mentioned earlier, these include the DoD's US cyber command and CENTCOM, the DHS's Countering Violent Extremism task force and the DoD's Center for Strategic Counterterrorism Communications (from 2011 to 2016). The US has also been known to outsource some of its activities to contractors. This is for example the case with Operation Earnest Voice, an astroturfing campaign operated by CENTCOM but developed by the web security company Ntrepid. The campaign is aimed at using sockpuppets to spread pro-American propaganda on social

---

15   Many other actors, e.g. France, Israel and the EU, have set up similar semantic analysis and counterpropaganda programs.

Table 2: Comparison of US and Russian CIOs (author's design)

Legend: **x** reported **o** probable/uncertain	Kosovo (1999)	Iraq (2001–2011)	Afghanistan (since 2003)	Estonia (2007)	Georgia (2008)	Ukraine (since 2013)	Turkey (2015/16)	ISIS (since 2015)	US elections (2016)	FR elections (2017)
Point of view	*USA*	*USA*	*USA*	*RUS*	*RUS*	*RUS*	*RUS**	*USA*	*RUS*	*RUS**
CeTIO										
Technical sophistication	med.	med.	med.	med.	med.	high	low	med.	med.	med.
DDos/DoS				x	x	x		o	o	
Defacement			o	x	x	x		o	o	
Doxing						x			x	x
Hacks	o	x	x	x	o	x		x	x	x
Highly sophisticated hacks						x				
CeSIO										
Cognitive hacking						x	o		x	o
Social hacking		x	x			x	x	x	x	x
Parasocial hacking		o	o			x		x	x	x
Disinformation	o	x	x		x	x	x	x	x	x
Forging & leaking						x			x	o
Potemkin		x	o			x	x		x	x
Deceptive ID		x	x			x	x	x	x	o
Bots/botnets/sockpuppets		x	x	x	x	x	x	x	x	x
Trolling & flaming					x	x	x	x	x	x
Humor & memes						x			x	x
Targeting										
Population		x	x	x	x	x	x	x	x	x
Military personnel	o	x	x		o	x		x		
Policy-makers/personalities		x	o	x	x	x	x	x	x	x
Other communities/groups					x	x		x	x	x
Individuals		x	x			x	o	x	x	o
Objectives										
Disrupt activities – sense of insecurity	o	x	x	x	x	x	x	x	x	x
Control/reinforce/redirect narrative		x	x		x	x	x	x	x	x
Undermine trust in institutions/media/ allies		x		x	x	x	x	o	x	x
Demoralize/encourage			x			x		x		
Sow division/polarize						x	x		x	x
Nudge policy				x		x			x	
Discredit/support individuals		x				x	x		x	x

networking sites based outside of the US, notably in Pakistan, Afghanistan and Iraq (Fielding & Cobain, 2011).

A comparison of targets and objectives of CIOs shows that military personnel is most commonly targeted during conflicts, whether by cyber-enabled tools or cyberattacks, with operations serving a range of purposes, including demoralization, the creation of uncertainty, deception, and motivation. One example is the dissemination on social media of videos shaming captured Ukrainian soldiers. Furthermore, in all of the studied cases, the population at large is also commonly targeted by propaganda and various disinformation campaigns, whether in order to push, repress or counter various narratives. Specific individuals (e.g. politicians, leaders, propagandists, etc.) of strategic interest are frequently targeted by cyberattacks for disruption, intelligence or pressure purposes, as are various institutions (e.g. financial, government, media), which are prime targets for DDoS attacks that cause operational and communicational paralysis and undermine the population's trust in these institutions, as was the case in Georgia. Lastly, lone hackers and groups have also been targeted (i.e. In hacker wars). While the aims of such attacks tend to be tactical and strategic in nature, they still have some cognitive effects (e.g. disruption or demoralization), as has been observed in Georgia, Ukraine, and against ISIS.

In terms of tools and techniques, the comparison shows that disinformation and propaganda are widely used by all actors to disrupt and control their narratives. While some channels vary, the US and Russia mostly use the same ones but at a different scale. These include, among others, online news outlets (i.e. Potemkin news), social media and sockpuppets amplified by bots. While Russia's use of propagandist online news platforms (e.g. Sputnik or RTnews) is well documented, it has also been reported (Cary, 2015) that the US Departments of Defense and State have published, supported and in some cases (i.e. in Afghanistan) co-opted a number of media to support their narratives. Online, both states use social media and bots to amplify their messages, but while the US officially/publicly only operates several hundred state-related accounts on various platforms, it can be reasonably expected that Russia, through its troll farms and the IRA, operates more. The extent to which sockpuppets are used by both sides remains unclear, but it has been shown that both use them relatively extensively (e.g. as part of Operation Earnest Voice and in Ukraine). Meanwhile, memes and humor appear to be CeSIO tools used by Russia alone for propaganda purposes, as the US does not seem to have seized memetic warfare as yet. With regard to the use of cyber capabilities by the US, low-end cyberattacks, such as DDoS and defacement, have so far not yet been used (or reported). This contrasts with the Russian *modus operandi,* which involved the wide use of these tools in both Georgia and Ukraine. Meanwhile,

both states have been exercising some restraint in the use of highly sophisticated cyberattacks against critical infrastructure. The only known cases (in the context of war, which excludes Stuxnet) remain the 2015 and 2016 cyberattacks against the Ukrainian power grid allegedly conducted by the Kremlin-linked group CyberBerkut. On the US side, the use of high-end cyber capabilities to disrupt critical infrastructures or military systems has long been a contentious issue. During the Libyan civil war, such an attack was considered against the Gaddafi government's air defense system but was never approved due to concerns about setting a precedent (Schmitt & Schanker, 2011). A similar argument was put forward by NATO during the Kosovo mission to support their official policy of not responding militarily in cyberspace despite having own infrastructure crippled by cyberattacks and propaganda campaigns.

A final observation to be made is that the US seems to have been relatively slow to adopt internet-based influence operations or PSYOPS compared to Russia's use of CIOs, at least in the first decade of this century. Indeed, Russia understood quite quickly after the second Chechen war and the Georgian war that control over information in cyberspace was critical for the effective execution of its military operations (Giles, 2016). This led to an experimentation with various tools and techniques, notably during the Snow Revolution in 2011, which were then later used in Ukraine. Meanwhile, according to a RAND report (Munoz, 2012), internet-based PSYOPS were not really considered in Afghanistan or were at least deemed too ineffective against the Taliban. This must, however, be seen in the context of the Iraq and Afghanistan wars, in which the use of cybertools was evidently unsuitable, given both countries' low internet penetration of only around 5% each in 2011 (World Bank & International Telecommunication Union, 2019). However, a transition of certain PSYOPS to the online sphere could still be observed, for example via the *radio in a box* (RIAB) program or newspapers going online. While this transition might have not materialized in these cases, DoD strategists have been talking of seizing the opportunities afforded by the internet and information technologies to improve the range and efficiency of PSYOPS and propaganda since at least 2003, when they published the Information Operations Roadmap – aka. Rumsfeld's Roadmap to Propaganda (US DoD, 2003). That document specifically aimed to provide the DoD with a plan for advancing information operations as a core military competency by expanding and coordinating both military PSYOPs and public diplomacy operations (US DoD, 2003). It underlined the need for rapid, wide-spread information operations to combat, deter and influence adversaries.

Political tensions: election periods

A second type of context in which CIOs are employed are during periods of tension between states, i.e. in the gray area between war and peace. In these, cyber influence campaigns form part of the broader political and diplomatic dynamic and are often intertwined with some more offensive components. With regard to the examples studied, this was notably the case with Russia's influence campaigns during the US and French presidential elections in 2016 and 2017 respectively. However, these are not the only cases, with relevant literature citing a large number of others, for example in the recent British, Finnish, German, Austrian and Dutch elections to name only a few (Baezner, 2017). On the US side, in contrast, there appear to be few or even no open sources identifying similar cyber-enabled campaigns during foreign elections, despite a long list of historical precedents of foreign election intervention, with the US having intervened in 81 elections around the world between 1946 and 2000 (Levin, 2016). However, if one had to make an educated guess, it could be safely assumed that such activities would not have stopped suddenly at the turn of the millennium once the digital age had arrived.

With regard to the two cases examined, a number of observations can be made. First, the level of technical sophistication of the cyberattacks against the Democratic National Convention (DNC) and the Clinton and Macron campaigns is consistently at the medium end. While it is known that APT28 has used some moderately sophisticated malware (i.e. X-agent) to infiltrate, remain hidden, and exfiltrate data, there is no evidence that the attack resulting in the Macron leaks unfolded in the same way. As such, these hacks, and the subsequent doxing, are the only recorded (and attributed) types of CeTIOs in terms of election meddling. Indeed, while some DDoS attacks (using the Mirai botnet) and website defacements were mentioned in the news, notably against Trump's and Clinton's campaign websites, these have not been traced back to any Russian operations. This absence of DDoS could be due to the inherently covert nature of cyber influence campaigns, which is in conflict with the high visibility of DDoS attacks and defacements and shines a spotlight on the victim's vulnerabilities. More importantly, though, these types of attacks would have diverted public attention and media resources from other divisive issues that were being pushed via social media influence operations for example.

In addition to these attacks, there have been reports of sophisticated hacks of electoral materials in the US, where specifically the voting systems of 39 states were hit. In some cases the attackers gained access to voter data, which they tried to alter and delete. In other cases they accessed campaign finance databases (Riley & Robertson, 2017). A second case was also observed in Ukraine in 2014, where CyberBerkut hacked its way into the Ukrainian Central Election Commission and changed the election results to portray the ultra-right candidate Dmytro Yarosh as the winner. While the operations were averted in both cases, *in extremis* in the Ukrainian case, the operations were effective even without altering voting outcomes. In fact, efforts to delete voter registration information or slow down election counts were made in order to undermine confidence in election processes and institutions.

With regard to CeSIOs, the use of the full spectrum of tools and techniques has been identified in both cases, from mass disinformation on social media amplified by bots, to sockpuppets and Kremlin-affiliated news alongside trolling and flaming. The two cases also present similar objectives and targets, tailored to each context, which include polarization, disruption, undermining trust, controlling narratives, supporting specific candidates, among others. The short timespan of only a few months that separated these elections was most likely the reason why no new techniques were deployed. However, there was a notable difference in the scale, reach and efforts – but not impacts – of these two operations. Indeed, according to a report on the Internet Research Agency (DiResta et al., 2018), the scale of their operations in America was unprecedented, reaching over 126 million people on Facebook, 20 million users on Instagram, and 1.4 million on Twitter, while uploading over 1000 videos on YouTube. The same report estimates the cost of this campaign to have been at least US$25 million. No definitive estimate has been made of the costs of interfering in the French elections, but it is suspected to be less. It is worth mentioning that the EU and France took a number of measures to mitigate foreign influence operations in the wake of the US elections. These included the following, among others: awareness-raising workshops for candidates; a ban on Russian TV outlets; pressure on Facebook to close automated accounts; the planting of fake documents to confuse hackers; and the abandonment of electronic voting for citizens living abroad (Baezner, 2017). Another difference can be seen in the reliance on domestic actors for trolling and disinformation. In the French case, a number of far-right groups not only reused Russian propaganda and contents but also exchanged know-how and materials with similar groups abroad (Baezner, 2017).

Political tensions: non-election periods

CIOs have been used in non-election periods, for example in Estonia in 2007 and in Turkey between 2015 and 2016. Similar to election meddling, these cyber influence campaigns again form part of broader political and diplomatic efforts. In Estonia, the campaign was linked to Russia's

energy diplomacy and agenda in northern Europe, while in Turkey it was associated with Russia's involvement and interests in the Syrian civil war. A comparison identifies clear differences between the two cases in terms of targets, tools and objectives, which arise due to the very different contexts in which the campaigns were conducted.

The operations in Turkey, for instance, involved mostly CeSIOs amplified via social media, ranging from disinformation (e.g. anti-American conspiracy theories or false authorship) to narrative laundering by so-called experts in addition to trolling and flaming. As such, they were focused on reinforcing narratives, undermining NATO, and fomenting distrust and uncertainty against institutions and allies (Costello, 2018). The level of sophistication was low, and operations were mostly operated by proxies.

In the Estonian case, in contrast, which happened before the widespread use of social media, CIOs were largely technical in nature. They included mostly unsophisticated tools (i.e. DDoS and defacement) deployed by a criminal network with links to the Kremlin to disrupt day-to-day life in Estonia (i.e. government, finance, media), instill a sense of insecurity, and undermine trust in Estonian institutions. In addition, these attacks aimed at influencing politicians to consider Russian views and therefore resembled earlier (Soviet-era) destabilization and deterrence tactics towards governments deemed insufficiently friendly or compliant.

4.3 Additional Remarks

From a more general perspective, it is interesting to discuss the broader use, scope and types of cyber influence operations used by two different types of regimes, i.e. a liberal democracy (such as the US) and an autocratic state (such as Russia). It must, however, be noted that the extent to which relevant observations can be generalized to apply to other democratic and autocratic regimes is limited.

Democratic regime

In liberal democratic regimes, CIOs are highly normalized but constrained within a relatively narrow operational scope at all times, whether during peace, war or political tensions. They are strictly prohibited – or extensively limited – in times of peace, though. In addition, the use of propaganda by the government or state agencies against their own population or that of a friendly foreign state

has traditionally[16] been frowned upon and deemed unacceptable by the general public. The rules of engagement are thus highly codified and controlled by domestic laws, such as the US Smith-Mundt Act, which prohibits any form of influence operations by the Pentagon against US citizens and news outlets. Democratic governments are generally committed to adhering to the rule of law, laws of governmental responsibility and the principle of freedom of speech. They thus remain accountable to their population and sensitive to popular outrage, which can have repercussions in later elections.

Nonetheless, this does not mean that CIOs are not taking place in one form or another. However, they are conducted in a more transparent fashion and not labelled as such, with white propaganda, for example, having been adapted to modern information technologies. Today, all governments not only release most of their official statements online but also engage with and operate actively on social media to diffuse their own narrative. This is not only done on behalf of entities such as the US Department of State but also by and through top-level bureaucrats such as the President or Secretary of State, among others, and a network of individuals who amplify official messages (e.g. through retweets). Public diplomacy as well as public and civilian affairs are other domains which use cyberspace to "win the population's hearts and minds"[17]. Both aim at achieving popular support, whether abroad during military deployments or at home to foster support and understanding for current engagements.

Meanwhile, CIOs against enemies are both allowed and tolerated in liberal regimes but only at certain times (i.e. during conflicts or war) and within a limited geographical scope (i.e. within the battlespace). Moreover, their use is restricted to furthering strategic and tactical objectives rather than pursuing economic interests. These operations thus remain highly controlled within their doctrinal framework. Both the scope and use of information operations are codified and limited to the military and its agents with the support of the intelligence agencies, while foreign services conduct public diplomacy. As seen in section 2.2, the approach to IOs is highly compartmentalized.

Furthermore, in the current age of interconnectedness, even authorized cyber influence campaigns against hostile populations during times of war pose an issue for a democratic regime's domestic population. As became evident in 2002 in the context of Rumsfeld's controversial *Office for Strategic Influence* activities, there is nothing to stop US individuals or media from picking up, further disseminating or being affected by online

---

16   The Trump administration seems, however, to have become an exception.

17   Which is in itself a term used to describe psychological warfare.

propaganda, whether gray or black, or disinformation aimed at foreign populations (Carver, 2002). This has regularly led the public and regulators to demand more transparency, particularly in the wake of Snowden's revelations about mass internet surveillance by the US.

The contentious case of Rumsfeld's office and the political backlash that led to its dissolution highlight another feature of democratic regimes, namely the existence of checks and balances and corrective mechanisms to any (perceived) abuses of the normative framework pertaining to the use of CIOs.

Overall, while state-led CIOs are highly normalized, there tends to be greater tolerance for non-state-driven cyber influence, especially in the fields of politics and business. Indeed, there are now a plethora of companies promoting and selling their marketing, advertising, brand management, and public relations services to politicians, celebrities and other companies. These services provided include a number that verge on a legal gray area, such as buying likes or subscribers or exploiting legal psychographic data (i.e. Cambridge Analytica) for political targeting. Influence has become a commonly traded good, with many actors trying to get a slice of the pie and exploiting one technique or another. A perfect example of this type of commercialized online influence are social media influencers, i.e. individuals who, through their online presence on various social media such as Twitter, Facebook, or Instagram, have a critical mass of followers replicating the fashions, locations or attitudes (e.g. clothing, makeup, restaurants) promoted by these online personalities and their sponsors.

Autocratic regime

In contrast to democratic regimes, CIOs in autocratic regimes are not bound by the same norms and restrictions. Influence operations against domestic targets are considered not only acceptable by such regimes but also necessary to maintain the desired degree of social control over the population. In Russia, this was particularly notable during the anti-government and election protests in 2011–2012 (the Snow Revolution). During that time, Russia refined its CeSIOs to dominate, monitor and suppress online debate as well as divert the use of social media for facilitating organization (Giles, 2016). It developed increasingly sophisticated social media techniques, including sophisticated trolling and DDoS attacks on news websites, fake hashtag and Twitter campaigns (using bots), and social media operations closely coordinated with campaigns conducted in other media (Helmus et al., 2018). However, Russia is by no means the only autocratic state to use such techniques against its own population, with other examples including China and North Korea. All of these actors manipulate media without restraint,

aided by the relative homogeneity and stability of their leaderships, which greatly assists the dissemination of a singular message and narrative while allowing sufficient operational flexibility (Cohen & Bar'el, 2017).

Furthermore, such internal/domestic influence can be seen to spill over into external influence. Indeed, most of the CIO techniques – particularly those pertaining to social media – were first refined and tested domestically before being used for propaganda or disruption purposes abroad. This applies particularly to various Russian-speaking communities outside Russia, for example in eastern Ukraine, which were specifically targeted by pro-Russian propaganda through Russian media and social media (such as VKontakt) in the wake of the Ukrainian conflict.

Moreover, unlike democratic nations, autocratic states are not organized around the distinction between war and peace in their laws, regulations and societal institutions. This is particularly true for those who uphold a narrative of continuous struggle with another entity. Such a stance allows authoritarian states to develop institutions and competencies that are much more closely integrated at the operational level and navigate between different levels of tension with relative authority and ease, particularly around the level of low-intensity warfare just below the threshold of war (Lin & Kerr, 2019). As a result, while CIOs are also based on and regulated by doctrine, this doctrine is very different from the liberal democratic one. For example, Russia's very broad and holistic understanding of IW allows a much broader use and scope of relevant capabilities. The range of CIOs used is extensive and even includes highly sophisticated cyberattacks against voting systems and critical infrastructures, both of which are strictly off-limits for democracies.

Lastly, autocratic regimes are, again due to their organizations and institutions, both less vulnerable to CIOs and better equipped to respond to them than democracies. Indeed, as mentioned earlier, they are more flexible operationally, less restricted normatively, and have a greater scope of use but, above all, their exposure to potential attacks is smaller than in democracies. Indeed, democratic states' respect of the rule of law and freedom of speech, as well as the open and public nature of democratic societies (e.g. in terms of media etc.) and their election processes make them particularly vulnerable targets for CIOs.

5   Conclusion

The goals of this series of Trend Analyses is to provide practitioners and researchers in the field of cyberdefense with ways to understand important issues in cybersecurity and cyberdefense, and to enable the development of mechanisms to address those issues. In this edition, the main focus has been on cyber influence and its related activities.

In this regard, the US 2016 presidential election was a wake-up call for many practitioners and policymakers. Since then, the study of CIOs has received a great deal of attention, both in the literature and in the media. Accordingly, a plethora of terms and concepts have emerged (e.g. cyber-propaganda and cyber-persuasion), often without clear definition or frame of reference. This study therefore attempts to disentangle the conundrum around the many interrelated conceptual frameworks which influence in general, and cyber influence in particular, are attached to and based on. It further contextualizes and defines the underlying concepts of political warfare, psychological warfare and information warfare. The following paragraphs summarize the various conclusions of this study.

A conceptual and definitional conundrum

The first main conclusion of this study is that the conceptual framework around influence-related activities, and particularly around related terms in cyberspace (e.g. "cyber-propaganda", "information cyber operations" or "cyber-persuasion"), remains unclear and to some extent even incoherent with a certain amount of overlap. Indeed, while the use and application of influence in times of war and peace by states, private entities or individuals goes back to immemorial times, the concepts, names and classifications of these activities have constantly evolved over time and particularly over the last century, which saw the theorization of political, psychological and information warfare in various forms. The resulting conundrum renders any rational political and legislative/normative debate on the issue complex if not impossible. This is further complicated by the wide range of actors found in this domain and their different understandings of and doctrines on the issue. Many concepts and elements of cybersecurity therefore urgently require proper clarification through discussion and the agreement of definitions between all parties involved.

Similarities to and differences from traditional influence operations

The second main conclusion pertains directly to cyber influence operations, defined as "activities that are run in the cyberspace, leverage this space's distributed vulnerabilities (both technical and systemic), and rely on cyber-related tools and techniques to affect an audience's choices, ideas, opinions, emotions or motivations, and interfere with its decision making processes" (Bonfanti, 2019). It suggests that, despite the revolutionary varnish given to cyber influence operations, their targets, end objectives and strategies are mostly the same as in traditional influence operations: they still target the population at large as well as specific groups (e.g. policy-makers or military personnel) and individuals; and the end objective is still the exertion of power in one form or another until the target does something that it would not otherwise do, whether this is achieved through demoralizing, undermining trust, or subverting narratives and decision-making processes. As before, influence strategies still include the use of black propaganda, cheerleading and polarization.

Meanwhile, what differs is the addition of new tools for exerting influence and means to gather and treat information (e.g. AI) in preparation for applying these tools. These developments have greatly enhanced the scope and range of previously existing techniques and strategies. The study identifies two types of CIOs in this regard, namely *cyber-enabled technical influence operations* (CeTIOs) and *cyber-enabled social influence operations* (CeSIOs). The former rely on a repertoire of cyber capabilities of various degrees of sophistication (e.g. DDoS, hacks, or doxing) to influence targets, while the latter focus on exploiting targets' opinion-formation and decision-making processes through various techniques (e.g. dark ads, trolling, social bots, and memes).

This distinction is particularly important as the effects of CIOs must first be properly recognized before they can be addressed, countered or mitigated. As such, there can be no single solution, only solutions tailored to individual circumstances, which require not only a constantly evolving understanding of the possible uses of cyber technologies, but also a broader discussion and relevant efforts at the societal level.

Complex strategic implications

A third conclusion is that the operational space in which CIOs are performed, namely cyberspace, allows such operations to exploit the volume of information that is currently generated, distributed and consumed via new platforms and services. In this regard, cyberspace and its associated new technologies have acted as an equalizer,

liberator and enabler, as the relatively low cost of entry, the widespread availability of tools and possibility to circumvent traditional controls of information have allowed anyone to engage in CIOs. Cyberspace also acts as a powerful enabler due to the ease, speed and virality of information dissemination as well as the increasing reach, scale, penetration, precision and personalization of information targeting.

Accordingly, these elements, and the fact that CIOs present an effective counterbalance to conventional power (at little cost and great flexibility) with low risks of detection and escalation but high potential results, have made CIOs particularly attractive for a wide range of actors and will most probably continue to do so. However, availability and cost-effectiveness alone do not guarantee success, particularly as people are increasingly becoming aware of and literate in the issue.

Nonetheless, the medium and long-term strategic impacts and implications of such cyber influence operations remain difficult to assess due to the complexities of observing and measuring their intent, effect and efficiency. Furthermore, the at times chaotic and inconsistent operational forces that seem to drive such operations raise questions regarding (1) the need for strategic thinking in this regard and, most importantly, (2) of costs. Further research on these questions will therefore be needed.

Democratic vs. authoritarian use of CIOs

Finally, when one looks at and compares various confirmed cases of CIOs, notably those conducted by an authoritarian state such as Russia and a democracy such as the US, several observations can be made. The first is that the toolbox used by each state is highly dependent on the specific context and objectives to be achieved. DDoS attacks, for example, are good for disruption (e.g. in Estonia) but are overt and inadequate for the covert dissemination of disinformation (e.g. during the 2016 US election). Meanwhile, CIOs used in times of war, in times of political tensions and for interference in elections are at a different level of sophistication, with some instances of highly sophisticated cyberattacks having been deployed in the Ukrainian civil war, for example. Specifically, Ukraine can be seen as a testbed for any types and forms of CIOs targeting all types of actors.

Accordingly, CIOs have also evolved year after year, conflict after conflict, crisis after crisis in keeping with technological and societal advances. Indeed, both the US and Russia have learned continuously throughout their engagement with cyber operations, whether foreign or domestic, and are still learning and inventing new ways to exert and protect themselves from cyber influence. New forms and techniques of (counter) influence may very well be invented in the future, especially given the possibilities afforded by artificial intelligence and emotional hacking.

Furthermore, election meddling is far from new, with both the US and Russia having comprehensively engaged in this practice throughout the last century. Cyber-enabled election meddling, which exploits the latest tools and vulnerabilities of hyperconnected societies, is only the latest form this activity has morphed into. At this stage, CIOs during elections certainly seem to constitute the new normal, with all of the implications this entails.

Lastly, autocratic and democratic states do not use CIOs in the same manner, or at least portray their use of such operations differently. Namely, autocratic regimes have a greater operational scope and margin than democracies, as they do not subject themselves to the same norms as liberal democracies do, particularly when it comes to using CIOs against their own populations or allies or outside times of war. This, however, does not mean that democratic regimes do not conduct cyber influence operations. However, this is most likely done through official state channels in the forms of white propaganda, public diplomacy and civilian affairs, or through numerous non-state economic actors.

6   Glossary

Advanced Persistent Threat (APT): A threat that targets critical objectives to gain access to a computer system. Once inside a network, it tries to remain hidden and is usually difficult to remove when discovered (Command Five Pty Ltd, 2011; DellSecureWorks, 2014).

Attribution problem: Difficulty to determine with certainty the perpetrator of a cyberattack. Attackers are more difficult to identify because of their ability to cover tracks, perform spoof cyberattacks, or falsely flag other actors as perpetrators (Hay Newman, 2016).

Botnet or bot: Network of infected computers which can be accessed remotely and controlled centrally in order to launch coordinated attacks (Ghernaouti-Hélie, 2013, p. 427).

Cyberattacks: Deliberate activities in cyberspace that cause harm by compromising communications, information or other electronic systems, or the information that is stored, processed or transmitted in these systems (Brangetto and Veenendaal, 2016).

Cyber capabilities: Devices, computer programs or techniques designed to create degradation, disruption or destruction effects and manipulation of information, information systems and/or networks in or through cyberspace (Brangetto and Veenendaal, 2016)

Doxing: Release of stolen data on the Internet with the intent of harming the target (The Economist, 2014a).

Disinformation: false information spread deliberately to deceive (Schultz & Gordon, 1984).

Distributed Denial of Service (DDoS): The act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Fake News: Politically motivated, fabricated story presented as news (Teffer, 2017).

Gerasimov doctrine: Also called "non-linear warfare" or "hybrid warfare": a concept of war where all the actors are fighting each other, making alliances but also breaking them during battle. The actors only follow their own objectives and will use cyber, economic, military and psychological operations to achieve them (Miller, 2016; The Economist, 2014b).

Hacktivism: Use of hacking techniques for political or social activism (Ghernaouti-Hélie, 2013, p. 433).

Hack: Act of entering a system without authorization (Ghernaouti-Hélie, 2013, p. 433).

Integrity of data: Protecting data from modification or deletion by unauthorized parties, and ensuring that, when authorized persons make changes that should not have been made, the damage can be undone. Part of the CIA Triad of Confidentiality, Integrity and Availability of data (Perrin, 2008).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins & McCombie, 2012, p. 81).

Phishing: Technique used to trick a message recipient into providing confidential information like login credentials by making them believe that the message came from a legitimate organization (Ghernaouti-Hélie, 2013, p. 437).

Propaganda: the deliberate and systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist. (Jowett & O'Donnell, 2006)

Social Engineering: A non-technical strategy cyberattackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices (Lord, 2015).

Social bots: Bot is a shorter term for robot. It is an automated program that runs routine tasks on social media but can also define fake social media accounts that are used to repost messages or news and/or to spam (Chu et al., 2012; Hegelich, 2016).

Troll: A person submitting provocative statements or articles to an internet discussion in order to create discord and drag more people into it (Williams, 2012).

Troll farm or factory: A site running around the clock to produce trolling messages and posts (Volchek & Sindelar, 2015).

Virus: Malicious program with the capacity to multiply itself and to impair the infected system. Its purpose is also to spread to other networks (Ghernaouti-Hélie, 2013, p. 442).

Weaponized software: Programs and pieces of software that have been specifically designed to cause damage to their intended targets (Dewar, 2017).

Worm: Standalone, self-replicating program infecting and spreading to other computers through networks (Collins and McCombie, 2012, p. 81).

Website defacement: Cyberattack replacing website pages or elements by other pages or elements (Ghernaouti-Hélie, 2013, p. 442).

7   List of Abbreviations

AI	Artificial Intelligence
CeTIO	Cyber-enabled technical influence operation
CeSIO	Cyber-enabled social influence operation
CI	Cyber influence
CIO	Cyber influence operation
CNA	Computer network attack
CND	Computer network defense
CNE	Computer network exploitation
CNO	Computer network operation
CO	Cyberspace operation
DCO	Defensive cyber operation
DDoS	Distributed Denial of Service
DoS	Denial of Service
ICT	Information & Communications Technology
IO	Information operation
IP	Informatsionoye protivoborstvo (information confrontation)
IRA	Internet Research Agency
ISIS	Islamic State of Iraq and Syria
IW	Information warfare
OCO	Offensive cyber operation
PA	Public affairs
PD	Public diplomacy
PSYOP	Psychological operation
PSYWAR	Psychological warfare
SIO	Social influence operation
TIO	Technical influence operation

8   Bibliography

Allcott, H., Gentzkow, M., (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspective,* pp. 211−235.

Arquilla, J., Ronfeldt, D., (1997). *The Advent of Netwar,* in: Arquilla, J., Ronfeldt, D. (Eds.), In Athena's Camp. pp. 275−293.

Baezner, M., Robin, P., (2018). *Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict Version 2.* Center for Security Studies (CSS), ETH Zürich, Zürich.

Baezner, M., (2017). *Hotspot Analysis: Cyber and Information Warfare in election in Europe.* Center for Security Studies (CSS), ETH Zürich, Zürich.

Bartholomew, B., Guerrero-Saade, J.A., 2016. *Wave Your Flase Flags! Deception Tactics Muddying Attribution In Targeted Attacks.* Virus Bull. Conf. pp. 1−11.

Becker, H., (1949). The Nature and Consequences of Black Propaganda. *American Sociological Review.* pp. 225−235.

Bentzen, N., (2018). *Foreign influence operations in the EU.* European Parliament.

Blackstock, P.W., (1964). *The strategy of subversion: Manipulating the politics of other nations.* Chicago: Quadrangle Books.

Blank, S., (2017). *Cyber War and Information War à la Russe, in: Understanding Cyber Conflict: Fourteen Analogies.* George Perkovich & Ariel E. Levite, Washington, DC, pp. 81−98.

Bonfanti, M., (2019). An Intelligence-based approach to countering social media influence operations, in: *Romanian Intelligence Studies Review.* National Intelligence Academy, Bucharest.

Brangetto, P., Veenendaal, M.A., (2016). *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operation,* in: 2016 8th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn.

Bright, J., (2016). Explaining the emergence of echo chambers on social media: the role of ideology and extremism. *SSRN Electronic Journal.*

Cary, P., (2015). *The Pentagon and Independent Media—an Update.* Center for International Media Assistance.

Chesney, R., Citron, D.K., (2018). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *SSRN Electronic Journal.*

Cohen, D., Bar'el, O., (2017). *The Use of Cyberwarfare in Influence Operations.* Tel Aviv university.

Conway, M., (2003). *Cybercortical Warfare: The Case of Hizbollah.org.* Presented at the European Consortium for Political Research Joint Sessions of Workshops, Edinburgh, UK, p. 17.

Costello, K. (2018). *Russia's Use of Media and Information Operations in Turkey.* RAND Corporation: Santa Monica, CA.

Cronin, B., Crawford, H., (1999). Information Warfare: Its Application in Military and Civilian Contexts. *The Information Society,* pp. 257−263.

Damjanović, D.Z., (2017). Types of information warfare and examples of malicious programs of information warfare. *Military Technical Courier.* pp. 1044−1059.

Denning, D.E., (2011). Cyber Conflict as an Emergent Social Phenomenon, in: *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications.* Holt and Schell, pp. 170−186.

Derian, J.D., (2003). The Question of Information Technology in International Relations. *Journla of International studies.* pp. 441−456.

Dewar, R.S., (2017). *Trend Analysis: Cyberweapons: Capability, Intent and Context in Cyberdefense.* Center for Security Studies (CSS), ETH Zürich, Zürich.

DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J., Johnson, B., (2018). The Tactics & Tropes of the Internet Rsearch Agency. New knowledge.

Doob, L.W., (1949). The Strategies Of Psychological Warfare. *The Public Opinion Quarterly.* pp. 635−644.

Fielding, N., Cobain, I., (2011). *Revealed: US spy operation that manipulates social media.* The Guardian. Retrieved from https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

Giles, K., (2016). *Russia's "new" tools for confronting the West: continuity and innovation in Moscow's exercise of power.* Chatham House, London.

Gray, T., Martin, B., (2007). Backfires: White, Black and Grey. *Information Warfare,* pp. 7−16.

Herring, S., (2002). Searching for Safety Online: Managing 'Trolling' in a Feminist Forum. *The Information Society.* pp. 371−384.

Huhtinen, A.-M., (2007). Different Types of Information Warfare. in: *Electronic Government: Concepts, Methodologies, Tools, and Applications.* pp. 291−297.

Hulcoop, A., Scott-Railton, J., Tanchak, P., Brooks, M., Deibert, R., (2017). *Tainted leaks: Disinformation and Phishing With a Russian Nexus.* Citizen Lab. Retrieved from https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish.

Joint Chiefs of Staff, (2018). *Joint Publication 3−12 Cyberspace Operations.*

Joint Chiefs of Staff, (2014). *Joint Publication 3−13 Information Operations.*

Jowett, G.S., O'Donnell, V., (2006). *Propaganda and Persuasion,* Sage,. ed. Thousand Oaks.

Kiyuna, (2015). *Cyberwarfare sourcebook.*

Levin, D.H., (2016). When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results. *International Sudies Quarterly,* pp. 189−202.

Libicki, M.C., (2007). *Conquest in cyberspace: national security and information warfare.* Cambridge University Press.

Libicki, M.C., (1995). *What Is Information Warfare?* National Defense University Press.

Lord, N., (2015). *What is Social Engineering? Defining and Avoiding Common Social Engineering Threats.* Digital Guardian. Retrieved from https://digital-guardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats.

Magnier, M., (2013). *Hindu Girl's Complaint Mushrooms into Deadly Indian Riots.* Los Angeles Times. Retrieved from http://articles.latimes.com/2013/sep/09/world/la-fg-india-communal-20130910.

Marcellino, W., Smith, M.L., Paul, C., Skrabala, L., (2017). *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations.* RAND corporation, Santa Monica.

Marlin, R.R.A., (1989). Propaganda and the Ethics of Persuasion. *International Journal of Moral and Social Studies.* pp. 37−72.

Michael, K., (2017). Bots Trending Now: Disinformation and Calculated Manipulation of the Masses. *IEEE Technology and Society magazine.* pp. 6−11.

Moreau, E., (2017). *Internet Trolls and the Many Ways They Try to Ruin Your Day.* Lifewire. Retrieved from https://www.lifewire.com/types-of-internet-trolls-3485894.

Munoz, A., (2012). *U.S. Military Information Operations in Afghanistan.* RAND Corporation, Santa Monica.

NATO, (2017). *StratCom Laughs. In Search of an Analytical Framework.* NATO Strategic Communications Centre of Excellence: Riga.

NATO, (2016). *Internet Trolling as a Hybrid Warfare Tool: The Case of Latvia.* NATO Strategic Communications Centre of Excellence: Riga.

Nichiporuk, B., (1999). *U.S. Military opportunities: Information-warfare concepts of operations, in: Strategic Appraisal: United States Air and Space Power in the 21st Century.* Rand Corporation: Santa Monica.

Palmertz, B., (2017). *Theoretical foundations of influence operations: a review of relevant psychological research.* Center for Asymmetric Threat Studies (CATS), Swedish National Defence College.

Pamment, P., Nothhaft, H., Agardh-Twetman, H., Fjällhed, A., (2018). *Countering Information Influence Activities: The State of the Art*. Lund University: Lund.

Parrish, K., (2016). *Centcom Counters ISIL Propaganda* DoD. Retrieved from https://dod.defense.gov/News/Article/Article/827761/centcom-counters-isil-propaganda.

Paul, C., Matthews, M., (2016). *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. RAND Corporation: Santa Monica, CA.

Pernik, P., (2018). *Hacking for influence: Foreign Influence Activities and Cyber-attacks*. International Center for Defense and security: Estonia.

Perrin, C., (2008). *The CIA Triad. Tech security*. Retrieved from http://www.techrepublic.com/blog/it-security/the-cia-triad.

Riley, M., Robertson, J., (2017). *Russian Hacks on U.S. Voting System Wider Than Previously Known*. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

Schleifer, R., (2014). Propaganda, PSYOP, and Political Marketing: The Hamas Campaign as a Case Point. *Journal of Political Marketing,* pp. 152−173.

Schmidt-Felzmann, A., (2017). More than "just" disinformation. Russia's information operations in the Nordic region, in: *Information Warfare. New Security Challenge for Europe*. Tomas Cizik, Bratislava, pp. 32−67.

Schmitt, E., Schanker, T., (2011). *U.S. Debated Cyberwarfare in Attack Plan on Libya*. N. Y. Times. Retrieved from https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html

Schwartau, W., (1994). *Information Warfare: Chaos on the Electronic Superhighway*. Thunder's Mouth Press, USA.

Szafranski, R., (1997). Neocortical Warfare? The Acme of Skill, in: Arquilla, J., Ronfeldt, D. (Eds.), *In Athena's Camp*. pp. 395−416.

Szunyogh, B., (1955). *Psychological warfare; an introduction to ideological propaganda and the techniques of psychological warfare,* William-Frederikc Press. ed. United States.

The World Bank, International Telecommunication Union, (2019). *World Telecommunication/ICT Development Report and database*.

Tom Carver, (2002). *Pentagon plans propaganda war*. BBC News. Retrieved from http://news.bbc.co.uk/2/hi/americas/1830500.stm.

Tucker, P., (2016). The Same Culprits That Targeted Election Boards Might Have Also Targeted Ukraine. Defense one Retrieved from h https://www.defenseone.com/threats/2016/09/same-culprits-targeted-us-election-boards-might-have-also-targeted-ukraine/131277.

US DoD, (2003). *Information Operations Roadmap*.

Vosoughi, S., Roy, D., Aral, S., (2018). The spread of true and false news online. *Science,* pp. 1146−1151.

Walton, D., (1997). What is propaganda and what exactly is wrong with it? *Public Affairs Quarterly,* pp. 383−413.

Wilson, C., (2006). *Information Operations and Cyberwar: Capabilities and Related Policy Issues*. Congressional Research Service: Washington.

8.1 Comparative table sources

Baezner, M., & Robin, P. (2017). *Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict*. Retrieved from http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-01.pdf.

Blank, S. (2017). Cyber War and Information War à la Russe. In *Understanding Cyber Conflict: Fourteen Analogies*. Washington, DC, Georgetown University Press, pp. 81−98,.

Bodine-Baron, E., Helmus, T., Radin, A., Treyger, E. (2018). *Countering Russian Social Media Influence*. RAND Corporation.

Boyte, K. J. (2017). A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare. *International Journal of Cyber Warfare and Terrorism,* pp. 54–69.

Bronk, C., & Anderson, G. S. (2017). Encounter Battle: Engaging ISIL in Cyberspace. *The Cyber Defense Review,* p. 93–108.

Cary, P. (2015). *The Pentagon and Independent Media— an Update.* Center for International Media Assistance, Washington, D.C.

Čižik, T., Schmidt-Felzmann, A., Gvineria, S., Šukytė, Do., & Pashkov, M. (2017). *Information Warfare – New Security Challenge for Europe.* NATO Public Diplomacy Division, Bratislava.

Cohen, D., & Bar'el, O. (2017). *The Use of Cyberwarfare in Influence Operations.* Yuval Ne'eman Workshop for Science, Technology and Security.

DiResta, R., Shaffer, K., Ruppel, B., Sullivan, S., Matney, R., Fox, R., Albright, J., Johnson, B. (2018). *The Tactics & Tropes of the Internet Research Agency.* New knowledge.

Dunne, J. (2003). *Information Technology and the War on Iraq.* Scss. Retrieved from https://www.scss.tcd.ie/ tangney/ComputersAndSociety/2003/Paper3/ jd.html.

Iasiello, E. (2017). Russia's Improved Information Opera- tions: From Georgia to Crimea. *Parameters, 47*(3), pp. 54–63.

Fielding, N., Cobain, I. (2011). *Revealed: US spy operation that manipulates social media.* The Guardian. Retrieved from https://www.theguardian.com/ technology/2011/mar/17/ us-spy-operation-social-networks.

Gazula, M. B. (2017). *Cyber Warfare Conflict Analysis and Case Studies.* Cybersecurity Interdisciplinary Systems Laboratory.

Geers, K. (2015). *Cyber war in perspective: Russian aggression against Ukraine.* NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Giles, K. (2016). *Russia's « new » tools for confronting the West: continuity and innovation in Moscow's exercise of power.* Chatham House. Retrieved from https://www.chathamhouse.org/sites/files/ chathamhouse/publications/research/2016-03- 21-russias-new-tools-giles.pdf.

Harris, S. (2009). *The Cyberwar Plan.* National Journal.

Hollis, D. M. (2011). Cyberwar Case Study: Georgia 2008. *Journal Article, 6*(10).

Mammadova, J. (2018). *Where the East Meets the West: How Western Internet and Modern Communica- tions Technology Helped Soviet-style Propaganda in Donbass.* ICIT.

Parrish, K. (2016). Centcom Counters ISIL Propaganda. DoD. Retrieved from https://dod.defense.gov/ News/Article/Article/827761/ centcom-counters-isil-propaganda.

Costello, K. (2018). *Russia's Use of Media and Information Operations in Turkey.* RAND Corporation.

Kurowska, X., & Reshetnikov, A. (2018). Russia's trolling complex at home and abroad. In *Hacks, Leaks and disruption Russian cyber strategies.* European Union Institute for Security Studies. Paris: Popescu, N. & Secrieru, S.

Michael Connell, & Sarah Vogler. (2017, mars). *Russia's Approach to Cyber Warfare.* CNA.

Milosevic, N. (2014). Case of the cyber war: Kosovo conflict. Retrieved from: http://inspiratron.org/ blog/2014/07/01/ case-cyber-war-kosovo-conflict.

Mueller, R.S., (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* U.S. Department of Justice: Washington D.C.

Munoz, A. (2012). *U.S. Military Information Operations in Afghanistan.* Retrieved from http://www.jstor. org/stable/10.7249/mg1060mcia.

Munoz, A., & Dick, E. (2015). *Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness.* RAND corporation. Retrieved from https://www.rand.org/pubs/ perspectives/PE128.html.

National Intelligence Council. (2017). *Assessing Russian Activities and Intentions in Recent US Elections* National Intelligence Council. Retrieved from: https://www.dni.gov/files/documents/ ICA_2017_01.pdf.

Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. RAND Corporation.

Payton, T. (2010). *Cyber Warfare and the Conflict in Iraq*. Infosec island. Retrieved from http://www. infosecisland.com/blogview/6750-Cyber-War- fare-and-the-Conflict-in-Iraq.html.

Pernik, P. (2018). *Hacking for influence: Foreign Influence Activities and Cyber-attacks*. International Centre for Defence and Security.

Rob Taylor. (2012, avril 27). *Taliban website hacked as Afghan cyber war heats up*. Reuters. Retrieved from https://www.reuters.com/article/net-us- afghanistan-taliban-hacking/ taliban-website-hacked-as-afghan-cyber-war- heats-up-idUSBRE83Q09I20120427.

Bradshaw, S. & Howard, P. (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Computational Propaganda Research Project.

Sanger, D. E. (2016). *U.S. Cyberattacks Target ISIS in a New Line of Combat*. The New York Times. Retrieved from https://www.nytimes.com/2016/04/25/us/ politics/us-directs-cyberweapons-at-isis-for-first- time.html.

Sanger, D. E., & Schmitt, E. (2017). *U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disap- pointment Against ISIS*. The New York Times. Retrieved from https://www.nytimes. com/2017/06/12/world/middleeast/isis-cyber. html.

Schmitt, E., Shanker, T. (2011). *U.S. Debated Cyberwarfare in Attack Plan on Libya*. The New York Times. Retrieved from https://www.nytimes. com/2011/10/18/world/africa/cyber-warfare- against-libya-was-debated-by-us.html.

Suebsang, A. (2014). *The State Department Is Actively Trolling Terrorists on Twitter*. MotherJones. Retrieved from https://www.motherjones.com/ politics/2014/03/ state-department-cscc-troll-terrorists-twitter- think-again-turn-away/^.

Wilson, C. (2006). *Information Operations and Cyberwar: Capabilities and Related Policy Issues*. Congressio- nal Research Service.

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.