Siiri Lassila

THE USE OF INFORMATION OPERATION ACTIVITIES IN FOREIGN ELECTORAL INTERFERENCE

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

ABSTRACT

Lassila, Siiri
The Use of Information Operation Activities in Foreign Electoral Interference
Jyväskylä: University of Jyväskylä, 2019, 94 p.
Information Systems, Bachelor’s Thesis
Supervisor(s): Clements, Kati

This Bachelor’s Thesis is a literature review that is based mostly on scholarly articles and books and some military and governmental sources. Its purpose is first to explain what is information warfare and foreign electoral interference. It will be then shown how information warfare tactics can be used to intervene in the elections of a foreign nation via a case study of the US 2016 Presidential Election in which the Russian Government intervened. The thesis showed that the Russian government intervened in the election by an extensive social media disinformation campaign that involved the use of trolls, bots, disinformation, ”active measures” and purchasing of political advertisements as well as computer network exploitation attacks on systems containing sensitive information and then the leaking of that information. These measures have also been used in other elections in Europe and can quite likely be used in future elections.

Keywords: information operations, information warfare, politics, foreign electoral interference, political manipulation, Russian information warfare, USA 2016 Presidential Election

TIIVISTELMÄ

Lassila, Siiri
The Use of Information Operation Activities in Foreign Electoral Interference
Jyväskylä: Jyväskylän Yliopisto, 2019, 94 p.
Tietojärjestelmätiede, Kandidaatintutkinto
Ohjaaja(t): Clements, Kati

Tämä tutkielma on kirjallisuuskatsaus, joka perustuu suurilta osin tieteelliseen kirjallisuuteen ja joihinkin armeija ja hallinnollisiin lähteisiin. Tämän tutkielman tarkoitus on ensin selittää, mitä ovat informaatiosodankäynti ja vaalihäirintä ovat. Sen jälkeen tutkielma näyttää kuinka informaatiosodankäyntiin liittyviä aktiviteetteja voidaan käyttää vaalihäirinnässä käyttämällä esimerkkinä USA:n 2016 presidentinvaaleja, johon Venäjän hallitus kohdisti vaalihäirintää. Tutkimus näytti, että venäläiset häiritsivät vaaleja laajamittaisella harhatietokampanjalla, johon kuului trollien, bottien, harhatiedon, aktiivisten toimenpiteiden (”active measures”) käyttäminen ja poliittisten mainosten ostaminen, sekä kyberhyökkäykset informaatiojärjestelmiä vastaan, jotka sisälsivät arkaluontoista informaatiota, ja tuon informaation vuotamista. Näitä keinoja on käytetty myös muissa vaaleissa Euroopassa ja niiden käyttämistä tullaan luultavasti jatkamaan myös tulevissa vaaleissa.

Avainsanat: informaatiosodankäynti, informaatio-operaatio, politiikka, vaalihäirintä, venäläinen informaatiosodankäynti, USA 2016 presidentinvaalit

FIGURES

TABLES

SISÄLLYS

1 INTRODUCTION

In 1995, there was already a growing feeling within the U.S. Defense Department that the role of information would become more crucial, both in national security and especially in future warfare (Libicki, 1995). Armistead (2004) saw information as the most critical element of power because individuals can transfer the power of information. The new information environment has enabled for even ordinary citizens to utilise the power of information through inventions such as the Internet and smartphones, which was necessarily not the case a few decades ago before the information revolution. (Armistead 2004; NATO, 2009).

We now live in an environment that is increasingly dependent on information and information systems (NATO, 2009). The change in information environment has revolutionised the power paradigm of information (Armistead 2004), and it has ushered in a new era of computer-based decision-making in all areas of life, including in the military (NATO, 2009). This dependence is both an opportunity and a weakness that can be exploited. (NATO, 2009).

Information on the internet can be spread with a speed that would have been inconceivable decades ago, and it can be easily manipulated (NATO, 2009). The information people see every day on the Internet may not always be accurate. Most people absorb and give credence to information every day without necessarily knowing its validity or its source (NATO, 2009), and false information in social media has been shown to impact people's judgement (Pennycook, Cannon & Rand, 2018). There are no regulations or restrictions in place that would prevent an adversary from spreading false information to further their own agenda or use the Internet as a source of intelligence or even as a channel for attacks upon friendly systems. (NATO, 2009).

During the years 1946 and 2000, the United States and Russia intervened in every nine of nation-level elections (Levin, 2016). Research has found that electoral intervention can systematically affect the election results in favour of the candidate supported by the intervening party (Levin, 2016). This is a concern given that national-level elections have a significant effect on the politics of the country (Levin, 2016) and although researchers have argued that in some cases such intervention can be justified by concerns about human rights, it fundamentally violates the democratic rights of citizens to use their vote (Fabre, 2018) and does not lead to democratisation as the United States has claimed in defence of their interference actions in the past (Levin, 2019b).

Combining these two things with a world where military interventions are increasingly more costly, likely leading to electoral intervention becoming ever more important tool of interference (Levin, 2016) and where many people, for example, 62% adults in the United States, get their news from the internet and social media where fake news is pervasive (Allcot & Gentzkow, 2017) leads to a concern about the use of information operation tactics in electoral interference. Already Russia has proven that it is willing to use such measures to subvert the democratic elections of other countries, with recent information operations taking place in the elections of Ukraine, the United States, and France (Polyakova & Boyer, 2018). But not only Russia is interested in using new technology to its advantage to undermine other nations, but various state and non-state actors are also as well (Polyakova & Boyer, 2018), including terrorist organisations (Theohary & Rollins, 2011). In fact, there have been a number of incidents in recent years where information warfare tactics have been used as an extension of politics, but there has been difficulty in attributing them and little in the way of retaliation since there are a number of challenges from a legal perspective. Current counter-measures are struggling to defend against such attacks. (Van Niekerk, 2018). Therefore, keeping all this in mind, it is vital to understand the different tools and activities these parties might use to interfere in elections to undermine democracy so one can recognise them and develop effective ways to counter them.

In literature relating to information warfare, one can find several definitions for what exactly it is and what it consists of. According to one description, information warfare is a subset of information operations and "a series of operations carried out during a conflict to reach or encourage specific objectives over one or more adversaries" (JP3-13, 1998). What most research agrees on is that information warfare has the manipulation, destruction, and protection of information at its core.

Similarly to information warfare, information operations also has varying definitions, depending on the organisation or the researcher. According to NATO's (2009) definition, information operations are coordinated military operations designed to affect the will, understanding, and capabilities of adversaries or potential adversaries. Information operations consist of information activities that's purpose is to modify information or information systems (NATO, 2009).

Foreign electoral interference is when one or more foreign power intentionally intervenes in crucial nation-level elections of another country by using either covert or overt means to support or smear one of the contesting parties in a way that will increase the chances of the party on whose behalf the intervention is happening. (Levin, 2016).

The research questions are:

- What are information operations?
- What is foreign electoral interference?
- How can information operation tactics be used to influence the elections of a foreign nation?

This thesis is a literature review of mostly military sources and scholarly books and articles. The sources were found using four information databases: JYDOK, Scopus, ProQuest, and Google Scholar. The search terms used included such phrases as "information warfare", "cyberwarfare" "information operations", "informaatio-operaatiot", "vaikuttaminen", influencing", "politics", "politiikka", "fact-checking", "fake news", "foreign electoral interference", "electoral interference", "voter manipulation", "USA" and "Russia". A few sources were found by reading through the sources of a previous Bachelor's Thesis on a similar topic and looking through the sources of the studies used in the writing of this thesis.

The second chapter of this thesis will explain what information warfare/operations are and what are the common objectives and tactics. The third chapter will be about elections, democratic electoral systems, and electoral interference. The fourth chapter is dedicated to exploring how information warfare tactics can be used to influence the politics of a foreign nation via a case study of the 2016 US Presidential elections. The fifth and final section of the study is for summarising the findings of the thesis and suggesting further research questions.

2 INFORMATION WARFARE: DIFFERENT PERSPECTIVES

As mentioned previously, the definition of Information Warfare and Information Operations and what they consist of vary in literature. Both Information Warfare (IW) and Information Operations (IO) are highly militaristic terms, so most sources that were used are government and military sources. What is included and not included to be a part of Information Warfare varies between different military organisations. The definitions gathered here are mostly from the perspectives of the USA, NATO, and Russia. Russia's characterisation of Information Warfare is much broader than the West's, so it will be discussed separately. The case study included in this thesis is an example of Russia's Information Warfare, so it was essential to include it as well as the Western's definition. In addition, most major foreign electoral interference campaigns have been conducted by either Russia or the United States (Levin, 2016).

2.1 Information Warfare

The term 'information warfare' was born in the 1990s in the United States after operation Desert Storm (Armistead, 2004; Ventre, 2016). Some aspects of information warfare, like deception and psychological operations, are as old as time, but the evolution of the information revolution has brought new elements to it in the form of hacker and cyber warfare. (Ventre, 2016). Digital information is now at the forefront of war (Ventre, 2016).

According to Ventre (2016), Winn Schawartau defined information warfare into three categories: personal information warfare (that targets individuals and privacy), commercial warfare (industrial espionage), and global information warfare (that is concerned with industries, countries and critical infrastructures). Therefore, information warfare is not exclusively limited to the military. In Schawartau's definition, information and information systems are both the weapon and the target, eliminating kinetic weapons entirely. Different techniques include breach of confidentiality, attacks against integrity, psychological operations and misinformation. (Ventre, 2016).

Al Campen, a U.S. Air Force Colonel, defined information warfare on how it differed from the past; by nations increasing dependency on information technology. Campen limited the scope of information warfare to data and software responsible for modifying, creating, storing, processing, and distributing it. In this definition, all forms of psychological operations, like leaflets, would not be a part of information warfare operation. (Ventre, 2016). James F. Dunnigan defined information warfare as attacking and defending the transmitting of information. (Ventre, 2016). Fred Cohen described information warfare as a conflict in which information is both the weapon, target, objective and method. (Ventre, 2016).

Martin C. Libicki defined information warfare as a series of activities aimed at modifying the enemy's flow of information while defending our own. (Ventre, 2016). In 1995, Libicki (1995) claimed that information warfare is not a separate warfare technique, but several distinct ones that each lay claim to the broader concept of information warfare. These techniques are: command and control warfare, intelligence warfare, electronic warfare, psychological operations, hacker warfare, economic information warfare and cyber warfare. (Libicki, 1995).

Larry Merritt, the technical director for the Air Force Information Warfare Center (AFIOWC), saw information warfare as all actions undertaken to affect or exploit the intelligence gathering capacity of an adversary to acquire a realistic image of the battlefield or the military command and operating capability of an opponent. Merritt's definition also included defensive capabilities like electronic warfare, computer network attacks, intelligence reconnaissance, and surveillance. (Ventre, 2016). Theohary and Rollins (2011) define Information Warfare as "the use of information technology and content to affect the cognition of an adversary or target audience."

The United States Army also has its own definitions of information warfare. However, the Army, Navy, and Air Force do not share a common doctrine, so the descriptions are somewhat different. (Ventre, 2016). The Air force defines information warfare as operations carried out to defend and attack information and information systems. Activities included are psychological operations, electronic warfare, deception, physical attacks, information attacks (basically computer network attack), information assurance, operations security, counter-intelligence, psychological counter-operations, counter-deception, and electronic protection (Ventre, 2016). A Joint Chiefs of Staff Publication (1998) committee described information warfare in 1998 as a subset of information operations that is a "series of operations carried out during a crisis or a conflict to reach or promote specific objectives over one or more specific adversaries." A 2001 entry in the Dictionary of the Department of Defence, only includes the term information warfare in a definition of the concept of information operations that is defined as actions that can be used to disturb the information and information systems of the adversary while defending our own and "those actions [that are] implemented in times of crisis or conflict constitute information warfare." (Ventre, 2016).

Overall, information is the key part of information warfare. Information is defined by Joint Publication (1998) as "facts, data, or instructions in any medium or form." Many of the definitions also define information warfare as actions taken to attack enemy systems while defending friendly systems.

2.2 Information Warfare vs Information Operations

Information warfare as a concept had largely disappeared from use in the US military circles by 2007 and was replaced by the concept of information operations. However, the concept of information warfare is still in use in countries like the United Kingdom, New Zealand, and Russia. (Ventre, 2016). According Armistead (2004), the critical difference between Information Warfare and Information Operations (IO) is that whereas information warfare is conducted during wartime, and concerns operation conduction, information operations is a strategic campaign that goes from peace to war to back to peace as shown in Figure 1. (Armistead, 2004). Information Warfare is, therefore, a subset of information operations, and the term would not be used for operations conducted during peacetime. (Ventre, 2016). IO can be used either during the war to affect the enemy's information infrastructure or during peacetime to prevent and minimise conflict, reducing the need for all-out information warfare (Armistead, 2004).

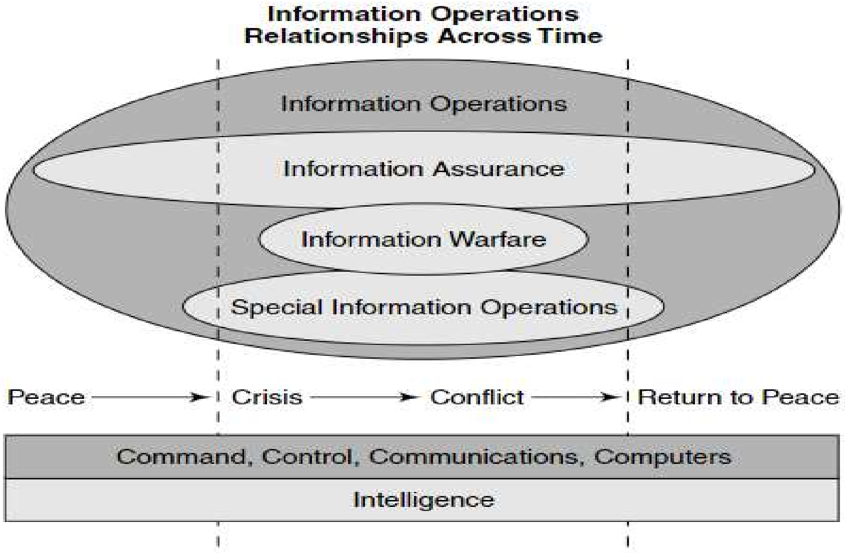


Figure 1: Information Operations Relationships Across Time. Reprinted from *Information operations: Warfare and the hard reality of soft power* by Leigh Armistead, 2004.

2.3 Information operations

Information Operations is more than mere war acted by computers. Originally it was born as an attempt by the U.S. military to develop a set of working tactics to exploit information in diplomatic and military contexts (Armistead 2004). IO is a supporting military capability that requires coordination with non-military agencies and the commercial industry, and its activities need to line-up with the national military strategy. It capitalises on the growing sophistication and dependency on information technology (JP3-13, 1998).

The United States' Department of Defence (DoD) defines Information Operations as "the integrated employment of information-related capabilities in concert with other lines of operations to influence, corrupt, disrupt or usurp the decision-making of adversaries and potential adversaries while protecting our own." (Theohary & Rollins, 2011). Joint Doctrine for Information Operations (JP3-13, 1998) of the United States army defines information operations as "actions take to affect enemy information and information systems while defending one's own" in order to affect information-based processes like decision-making and automated processes of critical infrastructures like electric power. IO activities apply at any phase and level of military operations and war. (JP3-13, 1998). NATO (2009) defines 'Info Ops' as a military function that "provides advice and coordination of military information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries, and other NAC approved parties in support of Alliance mission objectives." (NATO, 2009). Therefore, NATO also sees Information Operations as integrated coordination of activities instead of a separate function in its own right.

According to Armistead (2004), a common complaint about the definition of IO is that it is too broad, so, at the same time, it encompasses both everything and nothing. There are long-standing capabilities that are separate from the definition of IO, meaning that not all actions performed within those areas are necessarily part of an information operation and that they have broader applications than just IO, but that they are still elements of IO or they are related to it. (Armistead 2004; NATO 2009). These activities include, for example, Civil Affairs (CA), Computer Network Attacks (CNAs), Deception, Destruction, Electronic Warfare (EW), Operations Security (OpSec), Public Affairs (PA), Information Security and Psychological Operations (PSYOPS) (Armistead, 2004; NATO 2009). Integrating these activities and capabilities is integral to creating a cohesive IO strategy (JP3-13, 1998).

It is the purpose of IO to use these different capabilities in a coordinated fashion to produce the desired effect in the adversary's decision-making. (Armistead 2004). More often than not, not all these capabilities will be used in a good information campaign. Although physical destruction can be a part of information operation, for example, destroying the enemy's databanks, the basic idea of IO is that nations do not have to resort only to kinetic means.

(Armistead 2004). Information operations can take place in a variety of platforms, like what the United States' Department of Defence calls 'cyberspace.' Cyberspace exists within the information environment, and it consists of connected networks of information technology infrastructures, like the Internet and different computer systems. (Theohary & Rollins, 2011). The information environment consists of information, and those actors and systems that enable its use and where those systems and actors can observe and act upon the information. (NATO, 2009; JP3-13, 1998). These actors can be leaders, decision-makers, individuals, and organisations, and information systems include all systems and materials meant for the collection, storing, and sharing of information. (NATO, 2009).

Information Operations is tied to the concept of information superiority. Information superiority is defined by Armistead (2004) and Joint Publications (1998) as "the capability to collect, process, disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Therefore, it should come as no surprise that intelligence, its gathering, and its preparation is at the very foundation of information operations. According to Armistead (2004) intelligence is defined by U.S. Joint Operations as "information and knowledge about an adversary obtained through observation, investigation, analysis or understanding," as well as "the product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas."(Armistead, 2004). Intelligence should be timely, accurate, relevant, objective and detailed (JP3-13, 1998). Its relevance determines the intelligence value of information to ongoing military operations. It is crucial to successful planning, successful execution, and assessment of both defensive and offensive information campaigns. (Armistead 2004; JP3-13, 1998).

Although there are some differences between phrasing, both NATO, the US Army, and the DoD define information operations in the relatively same way: as a coordinated effort to influence the decision-making of their adversaries by targeting information and information systems while defending their own.

2.3.1 Information Operation objectives

The primary objective of IO is to affect the information environment in such a way that it will coerce or manipulate the adversary decision-makers into doing or not doing a particular action (Armistead, 2004) by affecting the **Will, Understanding,** and **Capability** of the adversary decision-makers (NATO, 2009). Information Operations objectives can be achieved either through lethal (e.g. kinetic attacks upon information infrastructure) or non-lethal means (e.g. deception), although a large part of IO activities are non-lethal (NATO, 2009).

Will is defined as the willingness to act on the part of the adversary. It can be weakened, for example, by undermining the authority and the cause of the leadership and cause discord between them and their support base, therefore, weakening their will and affecting their actions. In addition, protecting the will of the acting nation is also a part of information objectives. (NATO, 2009). **Understanding** of given situation is also vital to military operations, so Information Ops is interested in corrupting and degrading the information that contributes to the understanding and perception of the adversary and also protecting the understanding of the friendly decision-makers. (NATO, 2009). The aim is also to attack and defend those **Capabilities** such as communication infrastructure and propaganda systems that aid the decision-makers' will and understanding. (NATO, 2009).

To achieve its objectives, IO has many different tools to utilise, among them deception, psychological operations, and electronic warfare, that are used to target different targets like the ones that are shown in Figure 2 (Armistead 2004). Early identification of targets and their critical elements is essential for successful information operation and determining which capabilities will be the most effective. (JP3-13, 1998). However, as mentioned, IO is not only about attacking the enemy’s information system; it is also about defending one’s own. Therefore, Information Operation has two primary objectives: to protect and to attack. Common links between them are a dependency on information and the target sets involved (JP3-13, 1998).

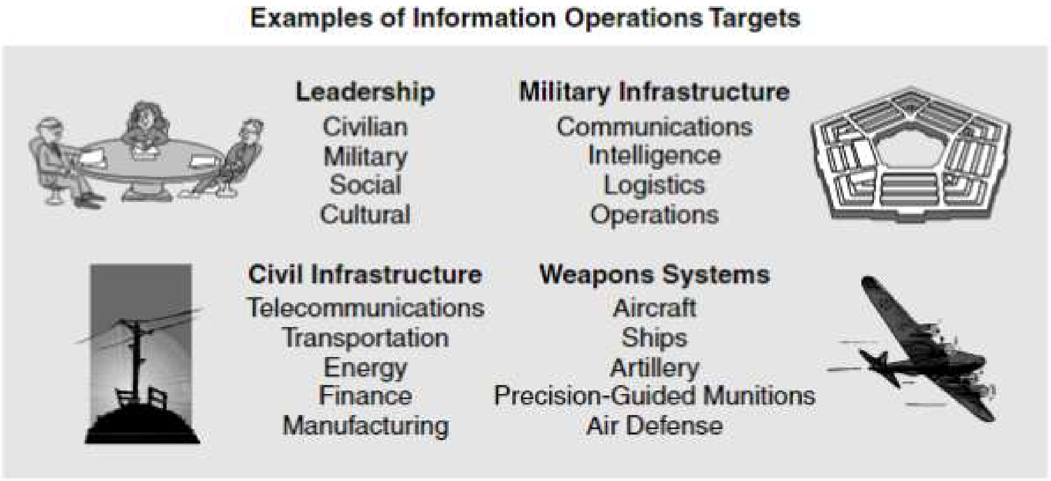


Figure 2: Examples of Information Operations targets. Reprinted from *Information operations: Warfare and the hard reality of soft power* by Leigh Armistead, 2004.

Defensive information operations are concerned with the protection and defending of friendly systems and information that military forces depend on to conduct operations and achieve objectives (Armistead, 2004; JP3-13, 1998). Those systems can include computers, satellites, broadcast media, phones, military technologies like weapon systems, and so on (Armistead, 2004). The sophisticated technologies of today have made it easier for adversaries to affect the military’s decision-making process, but defensive information operations are not concerned with just protecting information-based systems but also countering propaganda. (Armistead, 2004). Like all information operations, defensive information operation is a coordinated and integrated approach of policies, procedures, operations, personnel, and technology. Some techniques of defensive information operations include information assurance, OpSec, physical security, counter-deception, counterpropaganda, counterintelligence, electronic warfare, and special information operations. These activities are conducted on a continuous basis. Defensive information operation ensures access to information to friendly agents while denying its exploitation by enemy agents. (Armistead, 2004; JP3-13, 1998). There are two main goals: to minimise friendly mutual interference and to minimise IO system vulnerabilities to adversary efforts (Armistead, 2004). The weak link in defensive IO is the personnel; an untrained and unprepared insider can prove as significant a threat as an outside adversary and cripple critical information systems (Armistead, 2004). It is therefore vital for defensive information ops to have well-trained personnel.

An offensive information operation is concerned with targeting the adversary decision-maker and crippling their ability to make decisions (Armistead, 2004), yielding the actor enormous advantage (JP3-13, 1998). They can also be used to support defensive IO (JP3-13, 1998). Just like defensive info ops, it is an integrated use of offensive information operations capabilities, supported by intelligence to affect the decision-maker to achieve or promote specific, desired objectives. These capabilities consist of but are not limited to OpSec, deception, PsyOps, EW, kinetic attacks, special information operations, and possibly computer network attacks (CNA) (Armistead, 2004; JP3-13, 1998). Offensive IO has to have clear objectives that are in-line with the military strategy (JP3-13, 1998). Many of these are performed in the pre-hostilities phase of the conflict where they might have their most significant impact (JP3-13, 1998), and they can be both lethal and non-lethal (Armistead, 2004). IO is not something that can be done quickly or in a crisis mode. Therefore, there needs to be an intelligence preparation before any offensive IO effort. (Armistead, 2004). Offensive IO is conducted on every level of war, and the activities must be in-line with the overarching military objectives and follow domestic and international laws even if they do not take place at the same time as physical combat. (JP3-13, 1998). Offensive IO can be the main effort of a campaign, the supporting actor or a phase of a campaign or operation (JP3-13, 1998). Offensive IO operations can be conducted during peacetime to promote peace, deter crisis, control crisis escalation, or project power, for example by affecting the adversary’s course of action or degrading their capability to respond, with the goal of maintaining and returning to peace. (JP3-13, 1998).

2.3.2 Information operation activities

As mentioned previously, there are several activities that can be utilised to achieve Information Operations objectives. These vital activities, tools, and techniques can also exist separately from IO, as in not every time a particular activity is used it is part of an Information Operation. (NATO, 2009). It is their integration into cohesive IO strategy to reach stated objectives that make them part of an Information Operation (JP3-13, 1998). Some of these various activities were mentioned previously in this thesis, and they will now be elaborated on here. Those activities only mentioned in the Joint Staff publication (JP3-13, 1998) or the NATO (2009) publication have been left out to focus on the activities that are acknowledged by both.

NATO defines information activities as "actions designed to affect information or information systems" that also "include protective measures" (NATO, 2009). Information activities consist of three inter-related activity areas: activities designed to influence adversary perception, activities that focus on preserving and protecting friendly information and information systems, and activities that focus on targeting the data and information of adversaries. (NATO, 2009).

Operations Security (OpSec) is a process meant for protecting information critical to friendly military campaigns, including the friendly forces' dispositions, weaknesses, capabilities, and intentions, using either passive or active means (NATO, 2009). It also includes having a good understanding of adversary's ability to gather intelligence (JP3-13, 1998). By denying access to critical information from the adversary, the nation will affect their adversary's will, understanding, and capability (NATO, 2009), leaving them vulnerable to other offensive means and slowing down their decision-making (JP3-13, 1998).

Information Security (InfoSec) is a part of Operations Security. Its purpose is to protect stored, processed, or transmitted information and information systems against attacks that would lead to loss of confidentiality, integrity or availability. (NATO, 2009). Loss of integrity means that information loses its integrity through modification, loss of availability is when mission-critical systems are rendered unavailable, and loss of confidentiality is when confidential information is disclosed to non-authorised personnel or civilians. (Theohary & Rollins, 2011).

The purpose of **Psychological Operations** (PSYOPS) is to influence the perceptions, motives, reasoning, attitudes, and behaviour of targeted groups or individuals so that they act in a way that goes in line with the desired objectives of the influencing nation. (NATO, 2009; JP3-13, 1998). They are actions to convey selected information to foreign audiences (JP3-13, 1998). PSYOP messages can be transmitted through all types of media such as print, radio, television, aerial leaflets, the Internet and telephones. (NATO, 2009). For the successful execution of a PSYOPS, the choosing of right venue to transmit your message through is crucial (Armistead, 2004). PSYOPs can also be used to support military deception operations (JP3-13, 1998).

Deception's purpose is to mislead opponents through means of manipulation, distortion, or falsification (NATO, 2009) to make them commit desired actions (JP3-13, 1998). The emphasis of deception is not merely on misled thinking but the desired actions of the enemy (JP3-13, 1998). It targets intelligence systems in an effort to make enemy commanders form erroneous suppositions of the friendly forces' abilities and intentions, misappropriate intelligence assets or fail to employ combat and support units to their best advantage (JP3-13, 1998). It is a complex operation that is not considered an IO tool entirely, but using it in coordination with other IO activities can help in the achieving of IO objectives. It requires extensive knowledge of how the adversary thinks, lots of effort and a high level of security. Deception can be performed through both traditional means (e.g. show of force) and information means. (NATO, 2009).

Electronic Warfare (EW) includes any military action concerning the control or the use of the electromagnetic spectrum to attack the enemy through the use of electromagnetic waves (JP3-13, 1998). The electromagnetic spectrum is an infrastructure or conduit that facilitates the reception and transmission of information. (Armistead, 2004). EW has wide applications. It can be used to support other information activities like PSYOPS or deception or to gather information. It enables attacks on information technology, and it can also be used to protect friendly systems from assaults on the electromagnetic spectrum. Its effect can be either temporary or permanent. Electronic warfare can be used instead of kinetic warfare to avoid unnecessary force, which in turn leads to fewer casualties and collateral damage. (NATO, 2009). The three major subdivisions of EW that contribute to both offensive and defensive IO are electronic protection, electronic attack and electronic warfare support (JP3-13, 1998). Electronic attack is "the use of electromagnetic energy, directed energy or anti-radiation weapons to attack personnel, facilities, or equipment with the intent to degrade or destroy enemy combat capability" (Armistead, 2004). Electronic protection involves actions taken to protect friendly use of electronic spectrum against enemy EW attacks. Electronic warfare support is used to recognise immediate threats of EW. Both EP and EWS are used regularly during peacetime as well (JP3-13, 1998). There are cases when EW is not part of IO, for example, an attack on an unguided missile, which is not part of an information system. (Armistead, 2004).

Physical Destruction can also be used as a tool of information operations. It refers to the use of kinetic weapons against targets (JP3-13, 1998). It has two main aspects; first, through physical attacks on enemy information systems, it can compromise the information system of the adversary and therefore affect their understanding and ability to apply will. Second, the use of force will also have a strong psychological impact on the opponent and can act as deterrence or as a tool of coercion. However, the actor must consider the pros and cons of the use of physical force before acting since the use of too much force can have an adverse effect on public support. (NATO, 2009).

Computer Network Operations comprises of computer network attacks (CNA), computer network exploitation (CNE), and computer network defence (CND) (NATO, 2009). Computer network attacks degrade, deny, disturb and destroy information in adversary computers and computer networks (Armistead, 2004; JP3-13, 1998) by insertion of malicious code, or subtler manipulation of a data, changing the character, performance or display of the information contained in the network. CNA has been made easier by commercial software use in military systems. (NATO, 2009). Physical destruction of a computer also qualifies as CNA (Armistead, 2004). Computer network exploitation supports information operations by getting information from adversary computers and computer networks by gaining access through the exploitation of vulnerabilities. (NATO, 2009). The purpose of CND is to protect against CNA and CNE. It uses different techniques to monitor and protect computers and computer networks from attacks by detecting, identifying and responding to them by initiating a necessary action to protect the system. It is essential for maintaining decision-making capability. (NATO, 2009). The opportunity and effectiveness of CNO are entirely depended on the adversary's dependence on information technology (NATO, 2009).

2.4 Russia's Definition of Information Warfare

The previous segments were mostly about how the West defines the concepts of Information Warfare and Information Operations, but the Russian definition is somewhat different and broader than the Western ones. In the Russian construct, Information Warfare is not only a tactical warfare activity; it is an ongoing activity during both war and peacetime, and it is not just confined to the pre- and post-conflict stages of a war like Information Operations is (Giles, 2016). Therefore, there doesn't have to be a kinetic war going on for Russia to wage information warfare. In fact, Russian's recent activity and its news coverage suggest that they already consider themselves to be at war with the West (Giles, 2016).

In Russia, information warfare is a broad concept that covers a wide range of activities to use information as "a tool, or as a target, or as a domain of operations" (Giles, 2016). Some channels and methods used by Russia to wage information warfare include computers, satellites, smartphones, real or fake news media, statements by leaders and celebrities, online troll campaigns, text messages, YouTube videos, or direct approaches to individual human targets (Giles, 2016). These methods are used to steal, plant, interdict, manipulate, distort or destroy information (Giles, 2016). It is seen as a way to avoid the need for armed conflict to reach political and strategic goals (Giles, 2016).

The concept of information warfare includes systems, methods, and tasks, including computer network operations, PsyOPS, strategic communications, Influence, intelligence, counterintelligence, disinformation, electronic warfare, and physical destruction. (Giles, 2016). As with the Western Information Operations, the purpose of the coordinated use of these tasks is to influence the perception and behaviour of an adversary, but Russia also adds "population and international community on all levels" to the list of targets (Giles, 2016).

Russia sees information warfare as the starting point of a new type of war that is sometimes referred to as hybrid warfare, which will be waged through mass media and global computer networks (Giles, 2016). It is a way to incapacitate the enemy state before they are even aware that conflict has started and means that Russia can avoid armed conflict altogether or even replace it with information warfare. (Giles, 2016). They see their broad application of information warfare (information superiority) as an advantage in hybrid warfare. (Giles, 2016).

One crucial distinction between the Russian and Western definitions is that "cyber" attacks (CNO) or activities do not exist as a separate function but belong to the same tools as other information warfare techniques as propaganda and other activities; it is a subset of information warfare instead of an activity in its own right. (Giles, 2016). In fact, the Russians use the term cyber only in the context of discussion the Western information warfare terminology (Giles, 2016). In the Russian concept, the targeted information can be anywhere, in media, in information systems or inside someone's head; therefore, cyberattacks are conceptually seen to be no different from psychological attacks (e.g., propaganda). (Giles, 2016). The division between various activities has instead historically been divided into two main categories; **information-technical** and **information-psychological** (Giles, 2016). Information-psychological is the type of information warfare that is in effect continuously, and it aims to affect the enemy armed forces and the population (enemy and friendly alike), whereas information-technical is the type of information warfare that is waged during the active conflict to affect information systems. (Giles, 2016). It should be noted that cyberattacks do not belong only to the information-technical category; as an integral part of information warfare, they are also utilised in information-psychological operations, and they can be used efficiently in peacetime as well as during wartime. (Giles, 2016). Cyberattacks can be used in information campaigns whether or not they have little to no real impact; even when there is no damage, they can be used to stir panic and distrust in authorities (Giles, 2016). Threats of kinetic attacks, including nuclear options, can be used in psychological attacks as well in the same way (Giles, 2016). Whereas in the West non-kinetic, mainly psychological means have traditionally been seen as a supportive function to kinetic means, Russia sees both versions of warfare, non-kinetic and kinetic, as interchangeable and mutually supporting. (Giles, 2016).

Some Russian experts have drawn a distinction between **wartime** and **peacetime information warfare**. In peacetime, information warfare consists mostly of "covert activities, reconnaissance, espionage, building capabilities, and degrading those of the adversary and manoeuvring for advantage in information space" (Giles, 2016). In contrast, wartime activities are aggressive and overt and aim to achieve "political or diplomatic ends, by influencing the leadership and public opinion of foreign states, as well as international and regional organisations" by "discrediting adversary leadership, intimidating military personnel and civilians, falsification of events, disinformation, hacking attacks and so on". (Giles, 2016). By this definition and by looking at Russia's recent activities, it is implied that Russia already considers itself to be in a state of active warfare (Giles, 2016).

Traditionally Russians have looked father than their Western counterparts in achieving their objectives (Giles, 2016). The practice of choosing the desired goal and working backwards from it to the present situation to select a preferred course of action is called in the Western literature **Reflexive Control**, and recently in Russian literature, **Perception Control**. (Giles, 2016). Perception Control aims to influence individual and mass (public) consciousness by altering their perception in a way that they will make decisions and choose actions that are favourable to Russian objectives. The preferred goal can also be achieved by a series of decisions where the adversary will disregard the option that would be favourable to them until eventually, they are forced to choose between bad and worse, both of which are favourable to Russian objectives. (Giles, 2016). Reflexive control works in a way that the opponent is by means of disinformation, propaganda, counter-propaganda, pressure of force, distorting their perception of a given situation or their decision-making process, shaping their objectives or choosing the right moment for a decision to force them to logically arrive at the conclusion that is favourable to Russian outcomes. (Giles, 2016). Reflexive control is far more comprehensive than the Western practice of deception since instead of just misinformation, it is a sophisticated program that targets the factors affecting decision-making through multiple directions. (Giles, 2016).

Russia secures its own information space by limiting their own populations' access to foreign media, making it harder for the West to counter the Russian state propaganda, and enforcing the image of the West as an aggressor. (Giles, 2016). After Putin rose to power the Russian government re-instated their control over the information their own population receives by limiting foreign ownership over news media, closing or constraining independent news outlets, having commercial control over Kremlin-friendly media, censoring school books to show only approved versions of history and criminalising historical facts that are inconvenient for the running narrative (Giles, 2016).

2.4.1 Russian disinformation campaigns

Russian disinformation campaigns are not necessarily aiming to establish false information as correct but confuse the target audience in such a way that they began to doubt the very concept of truth and objective facts. This is achieved on the part of Russia by dismissing, distorting, distracting and dismaying information (Richey, 2018; Giles, 2016; Polyakova & Boyer, 2018). This is seen as an effective way to neutralising enemy efforts to counter Russian propaganda; if no one knows the truth or believes in objective facts, it's not simple to expose what are and are not lies, especially since Russia usually has multiple, even contradictory narratives at the same time (Giles, 2016). Generally, Russian disinformation has four objectives within the context of hybrid warfare: dissuading political rivals from challenging Russian kinetic action by painting image of them as a powerful state capable of defending itself and damaging its opponents, generating cynicism about politics and international laws and popularising Russian policy agendas to erode trust within the international community, legitimising "facts on the ground" to use human rights and defensibility of borders and right to self-determination as an excuse to intervene in other countries, and causing discord within allied states that are against Russia (Richey, 2018).

Russian's disinformation campaign has been made easier by what is called "post-fact" or "post-truth" era that has evolved in the Western political life via the election of Donald Trump, a man who regularly tells lies (Kessler, Rizzo & Kelly, 2019) and calls mass-media "fake news" and "enemy of the people" (Smith, 2019) and the Brexit campaign to leave the European Union in the United Kingdom (Giles, 2016). Russian disinformation campaigns also take advantage of mass media. RT and Sputnik (Russian propaganda news sites) are only the tip of the iceberg; Russian disinformation campaign is a 400M USD annually-costing, multi-lingual, international and domestic effort, that includes state-backed media and the use of social media trolls as well as fake news and the use of forged documents (Richey, 2018; Giles, 2016). The evolution of the internet has meant that placing disinformation on reputable news sites has proven vastly cheaper, simpler, and permanent than it was possible in previous decades (Giles, 2016).

Russians take advantage of the fact that western elected representatives receive their news from the same sources as civilians (Giles, 2016). The mass media, as it is today, has made it easier to use as a weapon. It can easily stir up chaos and confusion in military and government management and instil ideas of "violence, treachery, and immorality" into the public and demoralise them (Giles, 2016) and be used as a tool to slander adversaries and their supporters (Richey, 2018). Even responsible news media may inadvertently support Russian objectives by framing a story in a way that supports the Russian narratives (Giles, 2016). Even if disinformation doesn't spread to policymaking, only in mass and social media, it can change the social environment to be more favourable to Russian objectives and narratives (Giles, 2016). This can lead to lesser resistance against actions taken by Russia to Russia, even winning public support, therefore, increasing Russian's chances for success and reduce the damage caused by an adverse reaction by the international community. (Giles, 2016).

Trolls, fictitious online persona, or previously established real online persona taken over by human agents, and **bots**, automated social media accounts, also play a part in Russian's information campaigns (Giles, 2016). These accounts can pose as credible information sources to distribute disinformation from fake news sites, work to suppress any debate that goes against the Russian narratives or create confusion and discord between other internet users by provoking arguments (Giles, 2016) and amplify divisive and/or misleading content online (Polyakova & Boyer, 2018). Trolls and bots are also used to harass reporters and others to suppress their work that is unfavourable Russia. The work of trolls is often supported by misguided individuals from the target countries who support their work for various personal and political reasons, reflecting the Russian practice of taking advantage of existing political divides and social trends. (Giles, 2016).

Cyberattacks can be used in the service of disinformation campaigns. Among other things, Russia uses spearphishing, denial of service attacks and credential reuse to steal confidential and personal information that's leaked and used to spin a disinformation campaign to damage targeted individuals or institutions. Spearphishing is an electronic attack that usually uses false emails from seemingly trustworthy sources to steal sensitive information like account credentials or financial information from the target of the attack. Denial of Service attack is an electronic attack that attempts to block users from accessing particular services by overwhelming the server by false requests. Credential reuse is the using of stolen credentials to target other targets. The goals of these attacks can be to discredit electoral candidates, spin narratives or to sow distrust in political institutions by revealing damaging information. These sorts of attacks fall below the line of "cyberattacks of significant consequence" which usually means there is little retaliation on the target's part. (Polyakova & Boyer, 2018).

The aim of **subversion and destabilisation campaigns** is the long-term weakening and undermining of adversary societies overall to increase Russian's strength, without there necessarily needing to be a specific short-term goal. (Giles, 2016). These subversion campaigns carry with them revived aspects of subversion campaigns from the Cold War era that have been modernized to work on the age after the information revolution. (Giles, 2016). These campaigns are sometimes misleadingly referred to as "**active measures**" (Giles, 2016). Subversion campaigns aim to involve all public institutions it intends to attack in a disturbed attack in an effort to strike damaging blows to the enemy country's social system, from mass media to religious and cultural institutions to nongovernment organisations and individual scholars (Giles, 2016). The claimed aim of these efforts is to promote democracy and respect for human rights but, in truth, freedom of expression and democratic principles are exploited to help spread disinformation (Giles, 2016) and support (often) radical political parties to erode trust in political leadership (Richey, 2018). Russians use the values of Western societies against themselves, and instead of creating social trends, issues, or divides, they merely exploit them, as has been their habit since the Cold War (Giles, 2016). In Europe, these issues tend to be about national sovereignty and immigration, Islam, terrorism, and the EU as a globalist and elitist body, and in America, they are racial tensions, the criminal justice system, immigration, and class divisions (Polyakova & Boyer, 2018). The objectives of distributed attack are to influence the policies of the foreign nation, undermine the confidence the public has on the people and the institutions in power, disturb the relations between countries, and to discredit and weaken both the governmental and non-governmental opponents. (Giles, 2016). The key element of subversion campaigns is to spread misinformation among the population to discredit the leadership and undermine their authority (Giles, 2016).

3 ELECTIONS

> A formal and organized choice by vote of a person for a political office or other position.
>
> - Elections in Lexico

National-level elections that nowadays occur in half of the countries in the world are crucial to the politics of the nation because they usually involve a change in the political make-up of a country. The main-decision makers and parties change, which in turn leads to change in the policies, both domestic and international, that shape the future of the country. Elections can also affect a country's propensity for conflict, both within the country and outside of it, with other countries. Even in regimes that are not democratic, competitive elections may affect both international and domestic politics, sometimes even leading to the fall of the autocratic regime. (Levin, 2016). Elections, therefore, have a significant effect on the politics of the country.

Although elections are often associated with democracies, the presence of an election does not necessarily correlate to the governing system's democracy. (Schmitter & Karl, 1991). Historically, elections have been as much a tool of democratic governance as a means of authoritarian manipulation and control. In order to count as democratic, elections must work under conditions of freedom and equality by offering a choice of political authorities to free and equal citizens who are free to formulate their own political beliefs, signify them and have them weighed equally. Democratic elections also have to be irreversible. (Schedler, 2002). The fallacy of equating democracy with elections is called "electoralism." (Schmitter & Karl, 1991). However, since an increasing number of countries in the world are democracies (Levin, 2016; Klingemann, 2009) and the country the case study in this thesis focuses on is a democracy, this chapter will focus on democratic electoral systems.

3.1 Democratic electoral systems

By the year 2000, the majority of the world's countries had become electoral democracies when only a century before, only 25 states had restrictive democratic practices, and no country had universal suffragette. In just a century, democracies have become the norm instead of the exception. (Klingemann, 2009).

Democracy is not just a single collection of unique institutions; there are many types of democracy. Broadly, it is a system of governance where the representatives are chosen with regularly held, and fairly and honestly conducted elections. (Schmitter & Karl, 1991). In elections performed in democracies, coercion is relatively uncommon, and practically all adults are allowed to both vote and run for office in the elections (Schmitter & Karl, 1991).

There are two major types of democracy: majoritarian democracy, where leaders and representatives are decided by the majority, and consensus democracy, where leaders and representatives are chosen by as many people as possible. (Lijphart, 2012). Consensus democracy is also called "negotiation democracy," for it is characterised by compromise, bargaining, and inclusiveness, whereas majoritarian democracy is characterised by exclusiveness, competition, and adversity (Lijphart, 2012). The other difference between the majoritarian and consensus democracy models is that where majoritarian democracy centralises the power into the hands of a bare majority, a consensus democracy tries to share, disperse and limit that power in various ways. (Lijphart, 2012).

The single-member district plurality or majority system is the most common electoral system in majoritarian democracies. It is sometimes called "the winner-takes-all system" because the candidate(s) who get either the majority or plurality of the votes wins the election, and the others lose. This is why in a majoritarian system, the parties who get the most votes tend to be overrepresented, and the smaller parties get left with little to no seats, which leads to minorities not having a voice in government (Lijphart, 2012).

Countries with consensus democracy typically use proportional representation (PR) that aims to represent both majority and minority voices by translating the votes proportionally to seats in the government (Lijphart, 2012). For this reason, PR systems tend to be less disproportional than plurality and majority systems, except in presidential democracies, in which the president cannot be removed by the legislature except by means of impeachment (Lijphart, 2012). Countries are usually attached to their electoral systems, and changes from one to the other are rare (Lijphart, 2012).

Within these two electoral systems, there exists variation. Typically, electoral systems have seven attributes that differentiate them from each other, and those attributes are either proportional representation attributes or single-member majority attributes. These attributes are the electoral formula, district magnitude, electoral threshold, the total membership of the body to be elected, the influence of presidential elections on legislative elections, malapportionment, and interparty links. (Lijphart, 2012).

The electoral formula is the way an election is conducted and how the candidates are elected, and the votes allocated. Most electoral formulas belong in the category of plurality-majority formulas or proportional representation formulas, although there are some expectations (Lijphart, 2012). There are six main formulas; three majority-plurality formulas and three proportional representation formulas (Lijphart, 2012).

The first plurality-majority formula is the plurality formula, where the candidate who receives the most votes is elected. To be elected, the candidate needs the absolute majority of the ballots, which sometimes leads to run-off elections between candidates. This formula is often used in presidential elections. (Lijphart, 2012). The next formula is the majority-plurality formula, where the candidates are decided by the plurality of the votes if no one receives the majority (Lijphart, 2012). The third formula is called alternative vote that is used in some elections in Australia and Ireland. In this formula, voters list the candidates in order of their preference. Those candidates who receive an absolute majority in first preferences are elected, and those receive least votes are dropped and the votes in the ballots that had them as their first preference move to the candidate who is the voter's next preferred candidate. (Lijphart, 2012). The three proportional list formulas are called list PR, mixed-member proportional, and single transferable vote. In list PR, parties nominate a list of candidates and voters cast their ballots for a single party, and then the seats are allocated to the party lists in proportion to the number of votes they have collected (Lijphart, 2012). In mixed-member proportional single-member district representatives are selected by the plurality of the votes, and in the other non-single member districts, the representatives are elected by list PR. In this formula, each voter has two votes, one for a district candidate and one for the party list. (Lijphart, 2012). Single transferable vote formula differs from list PR by the fact that voters vote for individual candidates instead of party lists, and the voters are asked to rank off each candidate. When a candidate receives the minimum number of votes needed for election, their votes are transferred to the next preferred candidate, same if a candidate loses, their votes are transferred as well. These steps are repeated until all of the available seats are filled. (Lijphart, 2012).

The plurality method tends to favour two-party systems, whereas PR and two-ballot systems tend to encourage "multipartism." The effect of the plurality rule is that all but the two strongest parties are underrepresented because they tend not to have a chance at winning elections. This effect is heightened by the people's psychology; voters and candidates see it as waste of their time and vote to run or vote for a party that has little to no chance at winning which leads to voters voting for the "lesser of two evils" of the main parties instead of their actual preferred party. (Lijphart, 2012).

District magnitude does not tell the geographical size of the district or the number of voters in it. Instead, it determines the number of candidates to be elected in the district. Proportional voting and single-non-transferable vote electoral formulas require multi-member districts, whereas plurality and majority formulas can be applied in both single-member and multimember districts. (Lijphart, 2012). District magnitude has a substantial impact on the degree of disproportionality of the election and the number of political parties. Larger district magnitude in plurality and majority formulas means more significant disproportionality and works to the larger parties' advantage. In PR, larger districts lead to greater proportionality and work as an advantage for smaller parties, which why the considerable variation in district magnitudes in PR systems also leads to the variation of the proportionality of the election in PR systems. (Lijphart, 2012).

The electoral threshold is in use in countries that have large or nationwide electoral districts. They are put in place to make it harder for smaller parties to win the election since they have the advantage in PR systems with larger districts. This threshold is for representation and is often defined as the minimum number of seats won in lower-tier districts and/or a minimum percentage of the total national vote. (Lijphart, 2012).

The total membership of the body to be elected can also affect the proportionality of an election. The proportionality of the election increases, the more substantial the body to be elected is. The number is relatively meaningless for electoral bodies that have hundred or more members, but the proportionality of the election becomes affected with electoral bodies with fewer members than a hundred or if the total membership size does not correlate to the country's population size. (Lijphart, 2012).

In presidential systems, presidential elections can have a substantial effect in favour of larger parties on the outcome of legislative elections since usually only larger parties have a chance at winning them. This effect is stronger in presidential elections using the plurality rather than the majority formula and when the elections are held at the same time or shortly before legislative elections (Lijphart, 2012).

Malapportionment means that the voting population of a district is unequal. This, for example, means that in a multi-member district, the magnitude is not equal to the size of the voting population. Malapportionment occurs more often in majority and plurality systems with single-member districts and less in proportional representation systems that usually use large districts with varying magnitudes. Malapportionment does not occur at all in elections with nation-wide districts. (Lijphart, 2012).

Some list PR systems allow smaller parties to form interparty links, which means that they link their ballots so both parties' votes will be combined and will be used in the initial allocation of seats. This combined ballot might be advantageous to smaller parties to gain a few extra seats. Interparty links are usually referred to by the term apparentement. Apparentement tends to increase proportionality and make more effective parties (Lijphart, 2012).

3.2 United States electoral system

United States electoral system is a presidential plurality system. (Lijphart, 2012; Gueorguieva & Simon, 2009). Its federal legislature is two-chamber congress that consists of the Senate and the House of Representatives. There are presidential, national, state, and local level elections held in the United States. The elections are highly decentralised and are administered at state and local levels. Voting is not compulsory, and voter turnout for federal elections had fluctuated between 36 per cent to 63 per cent in the last decade. (Gueorguieva & Simon, 2009). The degree of disproportionality in US elections is 11.7 %, a number that is relatively low despite the plurality method used in congressional elections. (Lijphart, 2012).

The Senate has one hundred members, two from each of the 50 states regardless of population size, who are elected for a six-year term. The two senators from one state are never elected on the same election year. One-third of the Senate is elected every two years. (Gueorguieva & Simon, 2009).

The House of Representatives has 435 seats, a number that has been determined by law. Each state is entitled to at least one seat in the House, and the total number of the state's seats is determined by the population figures, which are derived from a census that is held once per decade. The representatives are chosen for a two-year term by a plurality vote in single-member districts. In addition to the 435 voting members, there are also non-voting delegates from unincorporated US territories like American Samoa. (Gueorguieva & Simon, 2009).

Instead of the plurality voting method, the President is elected through the Electoral College system, where each party selects a list of potential electors who vow to vote for the party's presidential candidate. The state's number of electoral votes equals the amount of the state's congressional representatives. The candidate who wins the plurality of the votes on each state is awarded the electoral votes from that state. (Gueorguieva & Simon, 2009)

There are different ways to vote in elections depending on the state the voter lives in. There is precinct voting that happens on the day of the election, where the ballots are cast in the precinct the voter is registered to, that occurs in every state (Gueorguieva & Simon, 2009). The vote is cast on a voting system for which the requirements are error correction on the part of the voter, manual auditing, accessibility, alternative languages, and maintaining voter privacy and ballot confidentiality (Gueorguieva & Simon, 2009). These machines used for voting have weak security and are full of easily exploitable loopholes. At the 2017 Defcon hacker conference, the participants managed to hack every single voting machine in use in America in less than two hours (Polyakova & Boyer, 2018). In Oregon and some local elections in California, a vote-by-mail is also an option. Some precincts also have vote centres where anyone can vote regardless of their home precinct. (Gueorguieva & Simon, 2009).

If a voter is not able to vote on the day of the election, half the states offer the option of early voting on the voting polls, that can be done without having to provide a reason for absence on the actual voting day. (Gueorguieva & Simon, 2009) All states offer absentee voting, where the ballot is cast by a mail-in paper before the election. Some states have more limitations on absentee voting than others where absentee voting can be done without providing a reason for the absence (Gueorguieva & Simon, 2009). Absentee voting is also offered for citizens living overseas or members of the military (Gueorguieva & Simon, 2009).

3.3 Foreign Electoral Interference

Foreign electoral interference is when one or more foreign power intentionally intervenes in crucial nation-level elections of another country by supporting or smearing one of the contesting parties in a way that will increase the chances of the opposing party by using either covert or overt means. (Levin, 2016). The methods range from providing funding to the preferred side's campaign to the creation of campaign materials to promises of aid or public threats to cut off foreign aid if the disfavoured candidate were to win or, in one case, drugging the opposing candidate before a major press conference. (Levin, 2016; Levin, 2019a). Intervention attempts are usually customised to fit the needs of the candidate the intervener is helping. (Levin, 2019a).

Between 1946 and 2000 alone, the United States and Russia (former USSR) intervened in the national-level executive elections of other countries 117 times, or in one of every nine elections (11,3%) (Levin, 2016; Levin, 2019a). The amount of intervened elections by region are shown in Figure 3. As can be seen, electoral intervention occurred in every region except for Oceania, and elections in Europe and Asia were more likely to be targeted than elections in other regions. Of these, Russia mostly intervened in Europe, and the US mainly intervened in Asia (Levin, 2019a). Electoral interventions were the favoured method of intervention of these two countries, with only 18 foreign-imposed regime changes and 53 military interventions occurring in the same time period (Levin, 2019a).

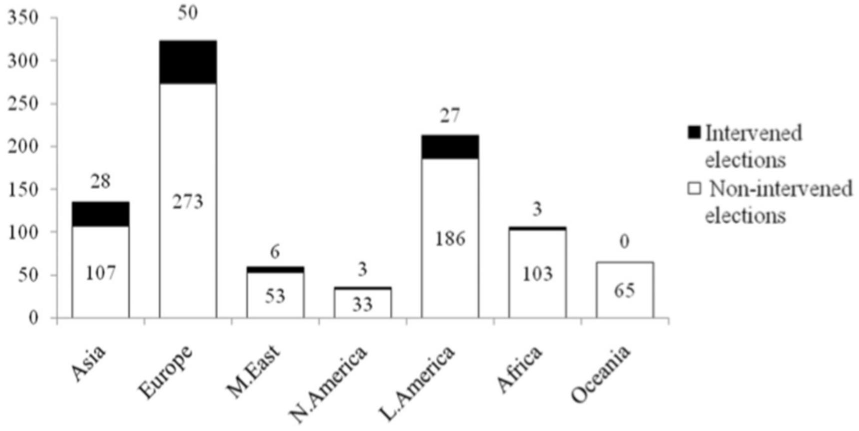
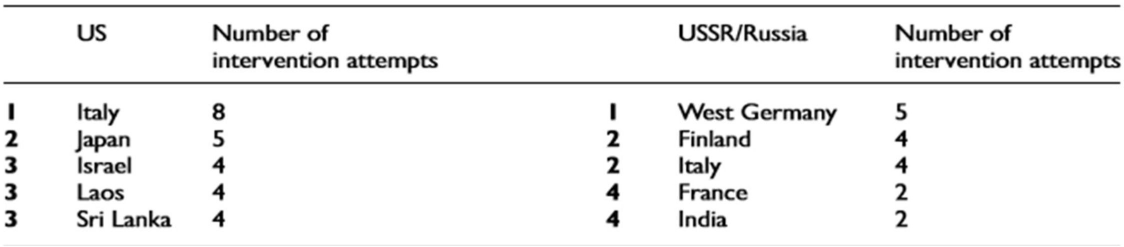


Figure 3: The amount of intervened and non-intervened elections by region. Reprinted from *Partisan electoral interventions by the great powers: Introducing the PEIG Dataset* by Dov H. Levin, 2019.

A total of 60 different countries were targeted. The top 5 countries most targeted by the US and Russia can be seen in Table 1. As can be seen, the targets varied in size and population number (Levin, 2019a). About half of the intervention cases (44.4%) were repeat interventions, as in subsequent interventions after a country has already intervened in one election, with 71% of them happening in consecutive elections (Levin, 2019a).

Table 1: Top 5 targets of electoral intervention by the US and Russia. Reprinted from *Partisan electoral interventions by the great powers: Introducing the PEIG Dataset* by Dov H. Levin, 2019.



	US	Number of intervention attempts		USSR/Russia	Number of intervention attempts
1	Italy	8	1	West Germany	5
2	Japan	5	2	Finland	4
3	Israel	4	2	Italy	4
3	Laos	4	4	France	2
3	Sri Lanka	4	4	India	2

Other nations beyond great powers like Russia and the USA can also intervene and have intervened in elections. For example, Iran intervened in the 2010 Iraqi elections, and Venezuela has intervened in elections in nearby Latin American countries (Levin, 2019a).

In order to be coded as electoral interference, the actions performed by the intervening nation need an affirmative answer to two questions: 1) was the act intentionally done to help or hinder one competing party? 2) did the act carry significant costs in terms of money invested or damage done to relations between the two nations? (Levin, 2019a).

In addition, for an electoral intervention to occur, usually, two concurrent conditions have to exist. First, the intervening party has to have a motive for intervention (Levin, 2016). Levin (2016) has found that electoral interference is effective in both democratic, partially democratic, or competitive authoritarian countries and that they are equally likely to occur in both partially democratic and full democratic countries (Levin, 2019a). Given that elections shape the course of international and national politics and that it can work in all these different forms of government, there exist many motives for great powers to intervene in the elections of other countries. (Levin, 2016). For example, the target nation's candidate or political party may present a threat to the interests of the intervening country, and other forms of diplomatic solutions seem too costly or ineffective to turn the candidate(s) around in their favour. (Levin, 2016). Second, a domestic actor must consent to and be willing to cooperate with the agents of the intervening nation. Without the information the internal actor provides, the chances of electoral intervention succeeding may be seen as too low to justify intervention. If either of these factors is missing, the electoral intervention will not occur. (Levin, 2016).

Other conditions often also need to be met for the intervener to consider electoral intervention. Although incumbents and challengers are almost equally likely to receive interference on their behalf (Levin, 2019a) if it is felt that a candidate has high changed to win without aid, intervention is obviously not needed, and the candidate is more likely to reject assistance in that situation because it would make them indebted to the intervening nation, restricting their freedom to enact policy and potentially alienate their support base by accepting help from a threating foreign government. On the other end, if a candidate's chances to win an election are too low, the intervening nation may consider it a waste of effort and will not support them. In this case, other measures of intervention may be used post-election, for example, violent removal. (Levin, 2016). Electoral interference itself is non-violent (Levin, 2016).

There are two forms of foreign electoral interference: covert and overt. Both have different risks, costs and benefits. (Levin, 2016). Usually, overt intervention methods are more effective than covert interventions, and they allow for a more extensive scale of manipulation (Levin, 2016). Overt intervention is when at least some of the details of the intervention were known to the target voters, and they knew that the intervention was done for this purpose (Levin, 2016). Electoral intervention is usually performed by great powers because they have more resources to put into it. A nation with the resources of a great power can promise or threaten the target nation with these resources, offering them in return for the preferred outcome or threatening their loss if the preferred outcome does not come true. (Levin, 2016). However, these sorts of overt interferences also carry with them a risk of backlash if the voting population of the target nation is not receptive to intervention and turns against the preferred candidate because of it. (Levin, 2016). On the other hand, covert missions are not as likely to face backlash, because they are by nature secretive (an intervention is coded as covert when the intervention was done in secret, and the intervention was not known to the populace), but what they gain in that area they lose in effectiveness. (Levin, 2016). The need for secrecy places limitations on the covert mission. The intervening country needs to provide enough help to the preferred candidate that they will win with means that are limited due to the clandestine nature of the mission. Due to the limited means, the chances of failure are higher than for overt missions. (Levin, 2016). Covert interventions are more common, with 64.1% of the interventions done by the US and Russia having been covert in nature (Levin, 2019a).

According to Levin (2016), electoral intervention systematically increases the chances of the aided candidate (Levin, 2016). In his study, he found that on average, an electoral intervention will increase the vote share in favour of the supported side by 3 per cent. Although it might not sound high, that per cent number would already have swung the vote in seven U.S. presidential elections since 1960 (Levin, 2016), and it has been enough to frequently determine the winner (Levin, 2019a). And although many foreign electoral interference missions in the past have failed (e.g., Soviet intervention in India's parliamentary election in 1977) and the supported candidates have lost, or the intervention has provided too little results, many more have succeeded (e.g. Soviet intervention in West Germany Parliamentary elections in 1972, US intervention in 1992 Israeli parliamentary elections) and won elections in the supported candidate/party's favour. (Levin, 2016). Therefore, the effect of foreign electoral interference is not insignificant and can affect a country's political landscape in a significant way.

4 The Use of Information Operation Tactics in Foreign Electoral Interference

4.1 Case Study: USA 2016 Presidential Election

4.1.1 Electoral Intervention?

First, to investigate if the Russian campaign can be coded as electoral interference by answering the questions put forward by Levin (2019a). 1) Were the acts intentionally done to help one of the candidates? According to the investigation by Robert Mueller (2019), the information efforts clearly favoured Donald Trump and undermined Hillary Clinton. 2) Did the actions carry a significant cost? The interference campaign resulted in sanctions placed against Russia (Mueller, 2019), and Russians invest yearly 400M USD into disinformation campaigns (Richey, 2018). Therefore, both conditions are fulfilled.

Second, to investigate if conditions suggested by Levin (2016) existed for the Russian campaign in USA 2016 Elections to occur, by establishing if there existed motivation and if a domestic actor was willing to cooperate with Russian agents. In 2011, Hillary Clinton criticised Russia's elections as "neither free nor fair" leading to Putin then accusing her of trying to influence Russia's internal political affairs. This possibly affected his decision to intervene in the 2016 Election (Ziegler, 2018; Hamilton, 2019). Clinton has consistently advocated for an activist, transformational foreign policy that poses a risk to Russian objectives, in contrast to Trump's approach that is transactional and isolationist and far less threatening to Russia (Ziegler, 2018). Therefore, motivation for interference existed on Russia's part. Second, there were various links between the Trump campaign and the Russian Agency running the information operation, although there was no sufficient evidence to place charges against them (Mueller, 2019). For example, Trump's foreign policy advisor George Papadopoulos attempted to arrange a meeting between Russian agents and the Trump campaign. (Mueller, 2019). Therefore, there existed some cooperation on the part of domestic actors to work with Russian agents and both conditions of electoral interference are fulfilled.

4.1.2 Overview

Evidence of Russia interfering in the 2016 US Presidential Elections started surfacing in mid-2016. This interference was "systematic and expansive" in fashion (Mueller, 2019). The campaign started as early as 2014 when the Russian Internet Research Agency sent agents to an intelligence-gathering mission to the United States. This led to a generalised program to undermine the US electoral system that, in time, evolved into a targeted operation that aimed to get Donald Trump elected. (Mueller, 2019).

A significant portion of the influence operation was executed through a social media campaign (Dutt, Deb & Ferrara, 2018), that favoured candidate Trump and disfavoured candidate Clinton, in addition to hacking operations targeting the Clinton campaign that led to the releases of stolen documents. (Mueller, 2019). The Russian government also attempted to involve people that worked for President Trump's campaign in the operation. (Mueller, 2019). The operation was unusual in the sense that usually evidence of covert interference operations surfaces only years after the fact, but in this case, evidence started already coming out during and shortly after the campaign. (Levin, 2018).

The Russian attempt to interfere in the elections lead to sanctions placed against them by the US government in December 2016, and several investigations into the matter were in process by early 2017 that eventually lead to the hiring of Special Counsel Robert S. Mueller, III to investigate the matter further, including any links or coordination between the Russian Government and the Trump Campaign (Mueller, 2019) since Campaign Finance laws forbid foreign governments or individuals from participating or influencing the election (Dutt et al., 2018).

There is some difference in opinion whether the Russian interference in US 2016 Election had any impact on the outcome of the election, with some saying that the effect was minimal (Berghel, 2017) and marginal (Ziegler, 2018) and others claiming that it "contributed decisively" to Donald Trump's victory (Richey, 2018). However, it has eroded the public's confidence in the legitimacy of the American electoral process, with the majority of Americans now questioning it, undermined trust in political leadership and widened the gap of suspicion between the political parties. (Ziegler, 2018; Gaughan, 2017). So, even if the Russian efforts did not win the election, they still achieved their desired outcome, and achieved objectives of their destabilisation and subversion campaigns.

4.1.3 Russian Social Media Campaign

The social media campaign was carried out by the Internet Research Agency (IRA). The IRA is based in St. Petersburg, Russia. It received funding from Yevgeniy Prigozhin, who has ties to the Russian President Vladimir Putin, and his companies, Concord Management and Consulting LLC and Concord Catering. (Mueller, 2019).

The campaign started in 2014 with the aim of spreading political and social discord in the United States (Mueller, 2019). These operations were aimed at broad audiences and constituted of "active measures" (subversion and destabilisation campaigns that were discussed previously). (Mueller, 2019). In mid-2014, IRA employees travelled to the US on an intelligence-gathering mission to obtain information and photographs to be used in their social media posts (Mueller, 2019). The IRA used social media sites such as Facebook and Twitter, where they established fake social media accounts and groups pages that spread false information that was beneficial to Donald Trump's campaign and harmful to Hillary Clinton. (Mueller, 2019). The IRA also bought political advertisements on social media in the names of people and groups residing in the United States and organised rallies to support Trump (Mueller, 2019). The organisers of those rallies contacted Trump supporters and campaign personnel to hold the rallies. (Mueller, 2019).

The IRA run social media accounts addressed divisive US political issues and falsely claimed to be run by activists and people from all across the political spectrum. (Mueller, 2019). The accounts were initially false accounts created for US persons but by early 2015 they more commonly posed to be accounts of fake US political and social organisations that claimed to be associated with movements and organisations like the Tennessee Republican Party, the Tea Party, the Black Lives Matter and LGBT+ rights movement. (Mueller, 2019).

These accounts posted harmful information about several candidates in the running for President, but by February 2016, internal IRA documents advised that their efforts should be focused on supporting President Trump and candidate Sanders while undermining candidate Clinton and the others. By mid-2016, IRA was exclusively focused on supporting Trump and disparaging Clinton. (Mueller, 2019). IRA also posted criticism of Clinton even before she had officially announced her candidacy (Mueller, 2019). The accounts were run by dozens of IRA employees that the IRA referred to as "specialists." In 2014 the US campaign social media specialist for Facebook, Youtube, and Twitter. Specialist focusing on Tumblr and Instagram were hired later. (Mueller, 2019).

These social media sites had a vast reach; by the end of the election, the IRA could reach millions of people by their social media accounts. (Mueller, 2019). A Facebook representative testified in 2017 that they had identified 470 IRA controlled accounts that had made around 80,000 posts during the election season that had reached at least 29 million people, but the number, according to Facebook, could be as high as 126 million people. (Mueller, 2019). Multiple of the Instagram accounts and Facebook groups had hundreds of thousands of US followers. In Twitter, their follower count was in many separate accounts in tens of thousands, including various US political figures (among them President Trump's son, Donald Trump Jr.) that retweeted their content. (Mueller, 2019). Twitter announced in 2018 that it had identified almost four thousand IRA run Twitter accounts that approximately 1.4 million people had been in contact with (Mueller, 2019).

The IRA twitter operation consisted of two strategies. The IRA personnel-run twitter accounts that generated original content and communicated with other Twitter users (trolls), and a network of automated Twitter accounts (bots) were used to amplify existing content (Mueller, 2019). These types of bot campaigns are sometimes referred to as astroturf or Twitter bombs and can be used to polarise political conversations and spread misinformation and further enhance it. (Bessi & Ferrara, 2016).

Troll accounts are accounts with the primary goal of manipulating public opinion with a clear intent to deceive and create conflict (Badawy, Ferrara & Lerman, 2018). The IRA used the 2,752 now-deactivated troll accounts, who operated mainly in the South of the United States, (Badawy et al., 2018) to try and influence the voters and provoke reactions; indeed, many of their tweets gained popularity. (Mueller, 2019). US media outlets also posted IRA accounts' tweets in news articles, thinking them to be tweets by US citizens. (Mueller, 2019). Out of the 2752 troll accounts, more than double were conservative in both the number of overall trolls and the number of trolls who produced original content. In the year before the election, these accounts produced more than half a million tweets. (Badawy, Addawood, Lerman & Ferrara, 2019). Conservative troll accounts talked mostly about refugees, terrorism, Islam, as well as Trump, Clinton, and Obama, whereas liberal trolls talked about the police and gun violence in addition to Trump and Clinton (Badawy et al., 2019). In the two months before the election, the trolls had mostly conservative pro-Trump agenda (Badawy et al., 2018). In the ten weeks before the election, these troll accounts posted around 175,993 tweets of which approximately 8.4% were election-related. (Mueller, 2019). Although people across the political spectrum engaged with the Russian troll accounts, it was mostly conservatives who helped to amplify their content (Badawy et al., 2018; Badawy et al., 2019). Out of the accounts who interacted with the troll accounts (referred to as spreaders) more were liberal (2:1) but conservative accounts generated more content in terms of tweets (including retweets) with the ratio of 3:2, meaning they shared the content produced by troll accounts more widely than liberal users (Badawy et al., 2019). In fact, as previously mentioned, many conservative high-profile US political figures and people associated with the Trump campaign followed the accounts and retweeted and responded to their content, among them Sean Hannity, Donald Trump Jr, and candidate Trump himself (Mueller, 2019). Badawy et al. (2019) estimate that 5% of the liberal spreaders were bots in comparison to the 11% of conservative users who were bots. Conservative bots also generated seven times as many tweets as liberal bots (Badawy et al., 2019).

In addition to the liberal and conservative bots identified Badawy et al. (2019), Bessi and Ferrara (2016) estimate that nearly 15 per cent the twitter accounts active in the U.S. Presidential election discussion were bots and that they contributed 19 per cent of the total volume of the election-related tweets. The bots were more active in the Midwest and South of the United States, whereas humans were more active in the most populated states like California, Texas, and Florida (Bessi & Ferrara, 2016). Bessi and Ferrara (2016) also found that bots supporting Trump generated almost no negative tweets, and a significant amount of them (two-thirds) were positive tweets in support of candidate Trump whereas the bots in support of candidate Clinton produced slightly less positive tweets of Hillary Clinton than her human supporters. Of the negative tweets produced by both Trump and Hillary supporters (human and bot) majority of them were deriding Hillary Clinton. (Bessi & Ferrara, 2016). However, it's hard to tell for certain how many of the bots active on Twitter during the campaign were IRA bots, since anyone with sufficient resources can purchase bots and, over the years, they have become increasingly easy to deploy (Bessi & Ferrara, 2016).

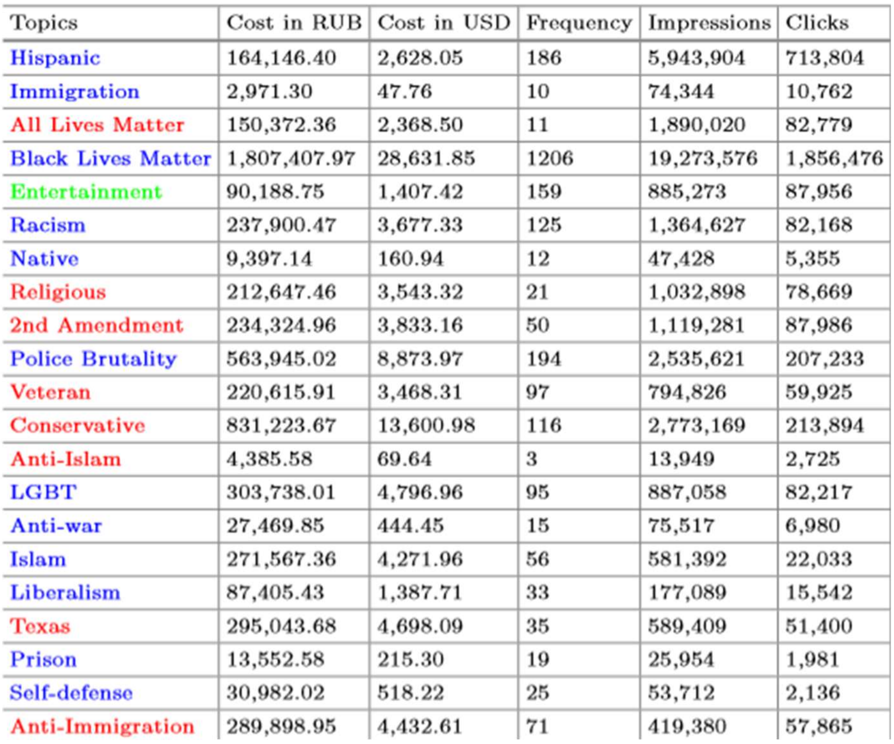
As mentioned before, the IRA-run troll and bot accounts shared false information or "fake news" on their platforms that, according to Gaughan (2017), has become a "defining feature of the 2016 Election" (Gaughan, 2017). Fake news are fictitious and often partisan stories that are presented as factual (Pennycook et al., 2018) or stories that grossly distort genuine news stories (Bovet & Makse, 2019). Most of the fake stories shared during the election season favoured Donald Trump (Allcott & Gentzkow, 2017) with a ratio of 4 to 1 (Gaughan, 2017). A study by Bovet and Makse (2019) that focused on news stories concerning presidential candidates found that 10% of the tweets containing links to news outlets shared in the five months preceding the 2016 Presidential Election included links to fake news stories, with extremely biased news accounting for 15% of tweets. When accounting for the number of distinct users, the share drops to 12% per cent in total, with centre-leaning news taking 29% and left-leaning news taking 43% of the share. However, the users posting links to false and extremely biased articles were, on average, more active than other users, with twice the number of tweets. The top spreaders of such stories were now-deleted accounts and accounts with deceiving profiles that followed the Twitter activity of Trump supporters. (Bovet & Makse, 2019). Candidate Trump also shared a false news story about Hillary Clinton during one of his speeches that had been created by Sputnik, a Russian propaganda site (Persily, 2017). Bots also played a significant role in the viral spread of false information by sharing a fictitious news article in the few seconds after such article was published on Twitter, and targeting users with popular accounts, increasing its chances to go viral and exposing more people to it (Shao et al., 2018). Humans are just as likely to retweet content by bots as by other humans (Shao et al., 2018; Bessi and Ferrara, 2016), making them vulnerable to this type of manipulation (Shao et al., 2018). Even a single exposure to a fake news story has been shown to increase the believed accuracy of the story, with repeated exposures increasing the effect even more, impacting the judgement of those who see such stories. (Pennycook et al., 2018). Allcott and Gentzkow (2017) estimate that an average US adult was exposed to at least one fake news story before the election (Allcott & Gentzkow, 2017). Fake news stories were not only created and spread by the Russian government but also third parties for ideological and monetary reasons (Allcott & Gentzkow, 2017).

In addition to running social media pages, IRA purchased advertisements from social media sites like Instagram and Facebook to reach larger audiences. (Mueller, 2019). The first known IRA advertisement bought in support of Trump was in April 2016. (Mueller, 2019). Facebook General Council testifying on November 1, 2017, in front of the Senate Intelligence Committee suggested that it would hard to identify every ad in their platform that was in violation of campaign finance laws, but they had managed to identify 3,500 advertisements that were paid for by Rubles and were bought between June 2015 and August 2017 that met the criteria (Dutt et al., 2018). These advertisements cost the Russian government around 100,000 USD (Mueller, 2019; Dutt et al., 2018). The IRA was able to reach a large number of users at such a low cost by taking advantage of the fact that Facebook micro-targets to users by using their personalised data, therefore spreading same content to people with similar political beliefs. (Polyakova & Boyer, 2018). The advertisements were either in promotion of their social media accounts or the IRA organised rallies, or they were political advertisements that either supported or opposed a presidential candidate. (Mueller, 2019). With a few exceptions, most advertisements concerning Hillary Clinton were negative. The earliest advertisement in opposition to candidate Clinton was purchased in March 2016. (Mueller, 2019). In contrast, most IRA bought advertisements that concerned candidate Trump were supportive in nature (Mueller, 2019). It is uncertain if the primary purpose of these ads was to aid Donald Trump in achieving victory or sow social discord in the population as the duration and the promotion of the advertisements might suggest. (Dutt et al., 2018).

Dutt et al. (2018) performed an analysis of the effectiveness of these advertisements that were released to the public on May 10, 2018. They only considered the ads that had been viewed by at least one person, which totalled 93K USD worth of advertisements. They found that most ads had attained sufficient outreach and popularity and that a considerable fraction of them was targeted towards younger users (Dutt et al., 2018).

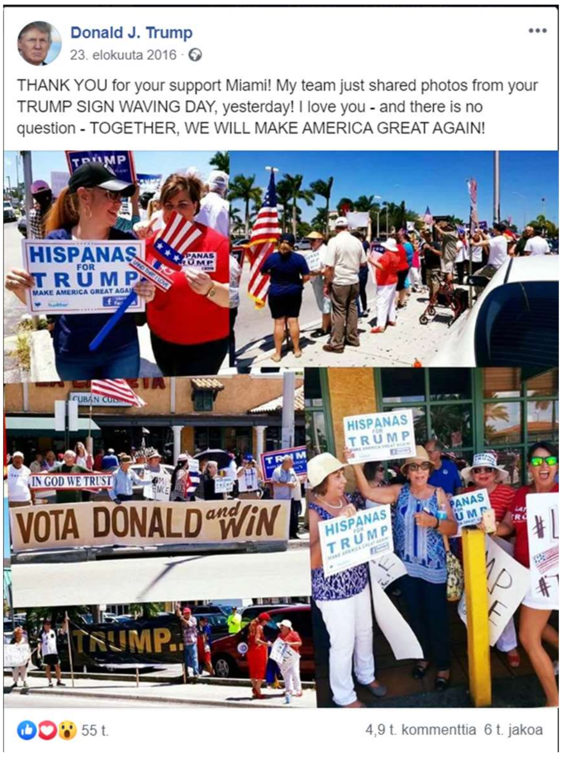
Dutt et al. (2018) also identified numerous campaigns targeted to either side of the political spectrum (Dutt et al., 2018). The different campaigns and their associated parties identified by Dutt et al. (2018) are shown in Table 2 in decreasing order of effectiveness. The campaigns targeted to either side of the political spectrum were often concerned with contradictory ideas like the Black Lives Matter and All Lives Matter movements, which indicates that the Russian government desired to sow further social discord between the two political parties (Dutt et al., 2018) that are already more hyperpolarised than they have been in the last hundred years, with 43% of Republicans and 38% of Democrats having a "very unfavourable" view of the other party (Gaughan, 2017) thus following the Russian practice of taking advantage of existing social divides in their efforts to destabilise adversary countries. Although there was no significant difference in the distribution of impressions and clicks between the two parties, the campaigns targeted to Democrats were more effective in terms of cost and effectiveness, but the IRA invested more in the campaigns targeted towards Republicans (Dutt et al. , 2018).

Table 2: Statistics of the IRA Facebook campaigns in decreased order of effectiveness. Reprinted from *"Senator, We Sell Ads": Analysis of the 2016 Russian Facebook Ads Campaign* by Dutt, Deb and Ferrara, 2018.



Topics	Cost in RUB	Cost in USD	Frequency	Impressions	Clicks
Hispanic	164,146.40	2,628.05	186	5,943,904	713,804
Immigration	2,971.30	47.76	10	74,344	10,762
All Lives Matter	150,372.36	2,368.50	11	1,890,020	82,779
Black Lives Matter	1,807,407.97	28,631.85	1206	19,273,576	1,856,476
Entertainment	90,188.75	1,407.42	159	885,273	87,956
Racism	237,900.47	3,677.33	125	1,364,627	82,168
Native	9,397.14	160.94	12	47,428	5,355
Religious	212,647.46	3,543.32	21	1,032,898	78,669
2nd Amendment	234,324.96	3,833.16	50	1,119,281	87,986
Police Brutality	563,945.02	8,873.97	194	2,535,621	207,233
Veteran	220,615.91	3,468.31	97	794,826	59,925
Conservative	831,223.67	13,600.98	116	2,773,169	213,894
Anti-Islam	4,385.58	69.64	3	13,949	2,725
LGBT	303,738.01	4,796.96	95	887,058	82,217
Anti-war	27,469.85	444.45	15	75,517	6,980
Islam	271,567.36	4,271.96	56	581,392	22,033
Liberalism	87,405.43	1,387.71	33	177,089	15,542
Texas	295,043.68	4,698.09	35	589,409	51,400
Prison	13,552.58	215.30	19	25,954	1,981
Self-defense	30,982.02	518.22	25	53,712	2,136
Anti-Immigration	289,898.95	4,432.61	71	419,380	57,865

While posing as their online personas, the IRA used its social media platforms to organise and promote rallies inside the United States. (Mueller, 2019). The Mueller investigation identified dozens of rallies organised by the IRA, earliest of which was held in November 2015. (Mueller, 2019). From June 2016 to the end of the election, almost all of the rallies focused on supporting candidate Trump or opposing candidate Clinton (Mueller, 2019). These rallies included three in New York and series of rallies in Florida and Pennsylvania. The Florida rallies drew the attention of the Trump campaign, which posted about a Miami rally in Trump's Facebook account, as can be seen in Figure 4 (Mueller, 2019).



Donald J. Trump
23. elokuuta 2016 ·

THANK YOU for your support Miami! My team just shared photos from your TRUMP SIGN WAVING DAY, yesterday! I love you - and there is no question - TOGETHER, WE WILL MAKE AMERICA GREAT AGAIN!

55 t. 4,9 t. kommenttia 6 t. jakoa

Figure 4: President Trump posting on Facebook about the IRA-organised Miami rally

To promote the rallies, the IRA contacted the media to inform them of the events and their followers on social media with invitations to attend the rallies. From the people who expressed interest in attending, they sought a person to act as the events coordinator with the excuse that they themselves could not participate in the event because they had a previous engagement, or they were somewhere else in the United States. (Mueller, 2019). After the event, pictures and videos of the rally were posted on the IRA run social media accounts. (Mueller, 2019). The attendance at the rallies varied from zero to a few hundred participants (Mueller, 2019).

The IRA employees who run the social media accounts also recruited people from across the political spectrum to promote and amplify IRA-generated content and perform political acts such as wearing a costume and a Trump mask (Mueller, 2019).

Many of the individuals involved in the social media campaign, such as Prigozhin and his companies and IRA employees, have been charged with conspiracy to defraud and some counts of identity theft. The Mueller investigations did not find evidence that any US individual knowingly or intentionally helped the IRA in its interference efforts. (Mueller, 2019).

4.1.4 Russian Hacking Operations

As part of the Russian government's efforts to interfere in the US 2016 Presidential elections, the Democratic National Committee (DNC) was hacked by the

Main Intelligence Directorate of the General Staff of the Russian Army (GRU) in June 2016 (Mueller, 2019). GRU started releasing the hacked materials the same month, using the online personas DCLeaks and Guccifer 2.0 that were created for the purpose, with additional releases taking place through the website WikiLeaks till November of the same year (Mueller, 2019). The releases of the documents were timed to interfere with the election and undermine the campaign of Hillary Clinton (Mueller, 2019).

The GRU began its hacking operation in March 2016 with hacking into the email accounts of individuals associated with the Clinton Campaign, including, organisations, volunteers, employees, and the campaign chairman John Podesta. (Mueller, 2019). Hacking into the computer networks of the Democratic Congressional Committee (DCCC) and the Democratic National Congress was started in April 2016 (Mueller, 2019). These hacking operations lead to the stealing of hundreds of thousands of documents and over 70 GB in data that included internal strategy documents, fundraising data, opposition research and emails (Mueller, 2019). The documents stolen were released first using their online personas and later through WikiLeaks (Mueller, 2019).

The military units responsible for the hacking operations were Military Units 26165 and 74455. Unit 26165 is a cyber unit dedicated to targeting different political, military, and non-governmental and governmental organisations that reside outside of Russia, whereas Unit 774455 is a related multi-departmental unit that engages in cyber operations. (Mueller, 2019).

Unit 26165 was primarily responsible for hacking into the DCCC and DNC and the Clinton Campaign. They sent out 90 spearphishing emails to the Clinton Campaign. These and other spearphishing emails gained them access to the email accounts of the Clinton Campaign, including to the account of John Podesta (Mueller, 2019) and into the computer network of the DCCC, which led to the GRU compromising approximately 29 different computers in the network. From there the GRU gained access to the DNC network, compromising 30 computers via a virtual private network connection between the two networks. (Mueller, 2019). After gaining access, the Unit also implanted two malware programs into the networks that allowed them to record keystrokes, take screenshots, and gather other data and extract it. (Mueller, 2019). After candidate Trump expressed his hope that "[Russia is] able to find the 30,000 emails that are missing", the Unit targeted Hillary Clinton's personal office on the same day with spearphishing attacks (Mueller, 2019).

Unit 774455 helped to Unit 26165 in the hacking operations to the DCCC and DNC, but they also promoted anti-Clinton content on social media and hacked into computers belonging to state boards of elections, county governments, secretaries of state and US companies that supplied technology used in US elections (e.g. voting software and electoral polling stations) as well as people who worked for those entities throughout the November 2016 election (Mueller, 2019). They gained access to the computers by exploiting known vulnerabilities and using such methods as SQL injection (injection of malicious code to a website) and spearphishing emails that contained a Trojan. The Unit gained access to voter data related to thousands of US voters and, according to the FBI, gain access to at least one Florida county government. (Mueller, 2019).

As mentioned before, the release of those stolen documents was first executed through the use of two fictitious online personas, DCLeaks, and Guccifer 2.0 (Mueller, 2019). The GRU started planning the leaks as early as April 2016 (Mueller, 2019). The releases on DCLeaks site consisted of thousands of documents that included personal identifying and financial information, internal correspondence and information related to fundraising. The promotion of the stolen materials was primarily handled through a GRU-created Facebook page under the same persona, but they also had a twitter and an email account for communication purposes. (Mueller, 2019). The GRU sent out early-access passwords to material that hadn't yet become public to some US reporters (Mueller, 2019). The DCLeaks page remained operational until March 2017 (Mueller, 2019). After the June 2016 DNC announcements of the leaks, Unit 74455 created the Guccifer 2.0 persona that claimed responsibility for the attack on a Romanian hacker in a WordPress blog post and started releasing the public stolen documents, ultimately releasing thousands of documents between June 5 and October 18, 2016. (Mueller, 2019). The released documents included opposition research, internal police documents, analyses of congressional races and fundraising documents (Mueller, 2019). Some of the documents were also sent to some interested reporters and politicians (Mueller, 2019). Guccifer 2.0 persona was also in contact with a former Trump campaign member, offering them help and asking what they thought of the Democrats' presidential campaign (Mueller, 2019).

In order to broaden the scope of their interference, the GRU started transferring the stolen documents to WikiLeaks, whose founder Julian Assange had previously expressed opposition to candidate Clinton and who had already published 30,000 Clinton emails in March 2016. (Mueller, 2019). WikiLeaks first started releasing the stolen documents, numbering 20,000, in July 2016 around the same time that President Trump had expressed his wish that Russia finds candidate Clinton's stolen emails although his aides have later expressed that he was speaking sarcastically and only three days before the Democratic National Convention. (Mueller, 2019). WikiLeaks also started releasing the 50,000 documents stolen from campaign manager Podesta on October 7, 2016, less than an hour after a potentially damaging video of candidate Trump was published in the news media. (Mueller, 2019). The documents included Hillary Clinton's private speeches, internal communication between high-ranking members of the campaign and correspondence related to the Clinton Foundation (Mueller, 2019). Both WikiLeaks and GRU attempted to hide their communications on Twitter and to obscure the real source of the hacked emails, claiming they had been released by a deceased DNC staff member and not Russia even after it was announced that Russia was behind the hacking operation. (Mueller, 2019).

These hacking operations led to charges being raised against the GRU officers responsible for the hacking for breaking the federal computer-intrusion statute. Evidence of WikiLeak's releases of hacked materials was not sufficient for charges to be raised (Mueller, 2019).

4.1.5 Contacts with the Trump Campaign

Although the Mueller investigation could not prove active collaboration between the Trump campaign and the Russian government, it did identify numerous links between them (Mueller, 2019). Individuals associated with the Trump campaign, including Donald Trump Jr. and the candidate Trump, promoted IRA-generated content from IRA-run accounts by linking, retweeting, and responding to the content. In total there were dozens of posts. (Mueller, 2019). The IRA also contacted the Trump campaign to request sings and other material for use at the rallies, which we granted. However, there was no evidence that the contacted campaign officials knew they were giving materials to foreign agents (Mueller, 2019). In addition, Russian intelligence officials also made personal contact with various Trump campaign officials (Mueller, 2019).

The Mueller investigations started investigating whether the Trump campaign had coordinated with the Russians on their interference efforts in July 2016 for the social media campaign, and the hacking operations coincided with numerous contacts between individuals associated with the Russian government and the members of the Trump campaign. (Mueller, 2019). These contacts consisted of business-related communications, offers of assistance, invitations for President Trump to meet President Putin, and for his campaign officials to meet with representatives of the Russian government (Mueller, 2019).

The earliest contacts happened in 2015 when candidate Trump was considering building a Trump Tower in Moscow. This project was pursued by Trump until at least June 2016 well into his presidential campaign and included Michael Cohen, now former Trump organisation executive, being in contact about the project with a Russian Government press secretary, Dmitry Peskov. (Mueller, 2019).

In the spring of 2016, a Trump campaign foreign policy adviser George Papadopoulos met with professor Josehp Mifsud who indicated to him that the Russian Government had "dirt" on candidate Hillary Clinton in the form of emails. A week later, Papadopoulos told an official of a foreign government that the Russian government had offered to assist the Trump campaign by the anonymous release of damaging information to the Clinton campaign. In the coming months, Papadopoulos worked with Russian officials to arrange a meeting between them and the campaign that ultimately did not take place. (Mueller, 2019).

In the summer of 2016, the Russian outreach continued. On 9th of June, only five days before the DNC announced that Russian hackers had gained access to information in its database, a meeting between Russian lawyer, who claimed to have dirt on Hillary Clinton that would be beneficial to the Trump Campaign, and three individuals associated with the Trump campaign, among them Trump Jr. and Trump's son-in-law Jared Kushner, took place in the

Trump Tower in New York. However, no such information was presented. (Mueller, 2019).

On July, the month when WikiLeaks released stolen emails by the GRU and the tip from a foreign government official about the actions of Papadopoulos that launched the investigation into potential coordination between the Russian government and the Trump campaign came out, a campaign foreign policy advisor Carter Page, who advocated for pro-Russia foreign policy, travelled to Russia and met with two Russian intelligence officers upon his return to the United States. Page was later fired from the campaign in September 2016. (Mueller, 2019). Throughout the election, the Trump campaign showed interest in those documents released by WikiLeaks and welcomed the potential damage they could do to Hillary Clinton. Donald Trump Jr. has direct contact with WikiLeaks during the campaign period. President Trump also directed his staff to seek out the stolen Hillary Clinton emails and expressed his hope that Russia would find them on a campaign speech, although it was later claimed the President was speaking sarcastically. (Mueller, 2019).

In August 2016, campaign chairman Paul Manafort met with his business associate Konstantin Kilimnik, who has ties to Russian intelligence. Manafort had shared polling data with Kilimnik before the meeting and continued to do so afterwards. They discussed a peace plan for Ukraine that they thought would require Trump's support if he were to win the election and the status of the Trump campaign and how they would win votes in the Midwestern states. (Mueller, 2019).

Post-election, the Russian Government tried to make inroads with the new administration. The Russian embassy called the President-Elect Trump hours after the election to congratulate him and arrange a call with President Putin. Other officials continued to make contact with individuals associated with the Trump administration to try to work on policy proposals that were favourable to Russia. After sanctions were placed on Russia over the election interference by President Obama, contact with the Trump administration made the Russian government agree not to retaliate. (Mueller, 2019).

While the investigation identified numerous links between the Russian Government and the Trump campaign, there was not sufficient evidence to support criminal charges of conspiracy and espionage. The June 9 meeting and the WikiLeaks releases also did not have enough evidence to lead to charges of violation of campaign-finance laws. However, charges were raised against Michael Flynn, George Papadopolous, Michael Cohen, and Paul Manaford were charged and found guilty of lying to the investigators, therefore impairing the investigation. (Mueller, 2019).

4.2 Table of Findings

The findings of the thesis concerning research question three ("How can information operation tactics be used to influence the elections of a foreign nation?") are summarised in Table 3.

Table 3: Examples of IW/IO activities used to influence the politics of a foreign nation

Activities	**Examples**	**Sources**
Disinformation	- Writing and sharing fake news articles and spreading false information in social media about an opponent candidate - Purchasing biased political advertisements	Giles 2016, Mueller 2019, Richie 2018, Bovet & Makse 2019
Trolls and bots	- Propagate and spread disinformation - Organise activities within the target country - Communicate with the citizens and officials of the target country - Create an illusion of grassroot support with automated bots	Giles 2016, Mueller 2019, Shao et al. 2018
"Active measures."	- Taking advantage of the concept of free speech and so-	Giles 2016, Mueller 2019, Polyakova & Boyer 2018, Dutt et al., 2018

	cial media and mass media to widen political divides - Turning democratic institutions against themselves - Exploiting existing social divides	
CNE/cyberattacks/ spearphishing	- Hacking into government institutions and campaign offices to seek harmful materials - Hacking into electronic voting systems	NATO 2009, Mueller 2019, Polyakova & Boyer 2018

5 Conclusion

Information warfare has information at its core; it is both the weapon and the target. It is various activities that are used to defend friendly information systems and information while attacking enemy information and information systems. It is different from information operations in the way that it can be only done during wartime, and it is mostly concerned with operation conduction. Information operations are a strategic campaign that combines different activities to defend and attack information and information systems from peace to war and back to peace. It aims to affect the decision-making capabilities of the target. Activities include PsyOps, OpSec, electronic warfare, deception, computer network operations, disinformation, and physical destruction.

Russian information warfare is broader from the Western definition. In the Russian construct, Information Warfare is not only a tactical warfare activity; it is an ongoing activity that covers a wide range of activities to use information as a tool, or as a target, or as a domain of operations. Russian information warfare is divided into two main categories; information-technical and information-psychological. Information-psychological warfare is continuous, and it aims to psychologically affect the enemy armed forces and both enemy and friendly populations. Information-technical is the type of information warfare that is waged during the active conflict to affect information systems, although its activities like cyberattacks can be used in information-psychological operations. Russian disinformation campaigns are large multi-national operations which aim is to distort reality and take advantage of existing social divides in adversary societies.

Foreign electoral interference is when a country intervenes in another's elections either via covert or overt means, with covert operations being more common. Interference campaigns use various methods from the threat of force to promises of resources to undermining the opponent with a disinformation campaign. Usually, electoral interference campaigns are tailored to fit the supported candidate. In the last decade, the US and Russia intervened in every nine national elections. In order to be coded electoral interference, the intervention has to be biased towards one candidate and carry with it a significant cost in terms of money and/or risk. Electoral intervention can systematically affect the elections in favour of the candidate on whose behalf the intervention was made.

This thesis researched what information operation tactics that can be used in foreign electoral interference by committing a case study of the Russia interference in the 2016 presidential election. It was shown that the Russian government intervened in the election by an extensive social media disinformation campaign that involved the use of trolls, bots, disinformation, "active measures" and purchasing of political advertisements as well as computer network attacks on systems containing sensitive information and the leaking of that information.

Levin (2016) found that electoral interference can affect election results, but it's difficult to say precisely how much of an impact the Russian interference effort had on the 2016 election results, and there are varying views on the matter. Wilder and Vorobeychik (2018) have calculated the type of social influence that fake news represents can be a salient threat to election integrity, although not so much in narrow races, and Pennycook et al. (2018) have found that fake news can have an effect on an individual's judgement, so it's possible that the Russian interference efforts had some impact on the outcome of the election. Even if this is not the case, the Russian efforts did manage to at least undermine Americans' trust in the integrity of their electoral system (Gaughan, 2017).

The USA Presidential election is not the only election Russia has intervened in by using the same tactics. Russia has also intervened or tried to intervene in elections in France, Ukraine, and Germany, and in each case, the tools, (disinformation, cyberattack, and subversion campaigns) and objectives were similar. (Polyakova & Boyer, 2018). Indeed, The USA 2016 Presidential election was not notable because interference happened, but because a great power intervened in the election of another great power (Berghel, 2017).

An assessment of NATO's definitions included in the domain of information asserted that there exists a lack of consensus regarding definitions because there are conflicting definitions that are used in different contexts to describe different objectives and actions. (Giles, 2016). This aligns with the observations that were made when searching for sources for this thesis. There seemed to be a confusion regarding the terminology that should be used. Some researchers used the term Information Warfare, some hybrid warfare, political warfare, and so on, all seeming to be talking about the same thing. According to Giles (2016) Russia, however, has formed all these concepts into a unified whole under the name of information warfare (Giles, 2016). The Russian Government, therefore, seems to have an advantage over other countries, with their cohesive terminology and strategy. The Russian disinformation campaigns are cyber-enhanced campaigns that are holistic and exploit culture, history, language disaffection, and more (Giles, 2016). The Western approach to defence is focused on the technical response, so it's not equipped to deal with the threat Russian's holistic approach holds (Giles, 2016).

Russia is not the only one interested and capable of using new technologies and information operation methods to undermine other nations, various state and non-state actors are as well, including terrorist organisations (Polyakova & Boyer, 2018; Theohary & Rollins, 2011). In fact, there have been a number of incidents in recent years where information warfare tactics have been used as an extension of politics and current countermeasures are struggling to defend against such attacks (Van Niekerk, 2018). The United States also has a history of intervening in elections and using the protection of democracy as a pretext (Levin, 2019b) so it would perhaps not be unreasonable to assume they could also use information operation tactics to intervene in elections, although they are somewhat constrained by legislation (JP3-13, 1998). New, more effective countermeasures should be developed against information operation campaigns (Richey, 2018; Polyakova & Boyer, 2018).

I would suggest that more research is dedicated to the subject, not just on the matter of the US election and committed by Russia, but as a general topic. To protect the integrity of democratic elections, research should also be dedicated to finding out how much effect such campaigns have the voters and election results and what measures can be used to counter such effects. Some researchers such as Polyakova & Boyer (2018) and Richey (2018) have suggested actions that could be taken to defend against influence efforts, but more research is perhaps needed to properly defend against such efforts, as the 2016 Presidential election has shown that the USA was not sufficiently prepared for such an attack against their electoral system. I suggest the following research questions:

- How are information warfare/operations tactics used in electoral interference?
- Do information campaigns affect voter behaviour? And if so, to what extent?
- To what extent can information operations and disinformation affect election results?
- What more can be done to counter interference campaigns, especially regarding disinformation?

It was somewhat challenging to find sources from high-quality publications for this study. There seems to be a lack of scientific research regarding information warfare/operations and electoral interference. In the latter case, most usable sources that could be found were mostly military sources and books, and in the case of the former, most research seeming to have been done by a single researcher. In contrast, it was relatively easier, although not by much, to find research concerning the US 2016 Election, which was likely due to it being such a prominent topic in the public consciousness these past few years and I'm confident that there will be more in the coming years since relatively little time has passed since the election, but not so much research was found on the general topic of information operation tactics used in electoral interference.

Due to somewhat lacking source material, the sources are not from as high-quality publications as they could be, but I did manage to find some from high-quality publications as well. The Publication Journal ratings for each category of sources can be seen in Table 4. However, both those sources that have been evaluated and those that haven't been, in my opinion, sufficiently followed academic research standards. Most works also had a good amount of citations, although not as much as there could be, perhaps because of the recent publication dates. The sources used in defining information warfare/operations are mostly from military organisations since they are military terms, and therefore military organisations were seen as the best source for definitions on the subject. Where most concern lies in the reliability of the sources is in the case study. Many of the sources used news reports and government reports as their own sources, and the primary source on the matter was a special investigation report by a US government institution, which leads to some concerns of biased reporting and false accounts of events given for political reasons. However, since information operations are confidential military and government matters, relying on public government reports was necessary despite the risk. Parts of the Mueller report were also classified, and there was not sufficient evidence on all matters, or it had been destroyed by persons under investigation, therefore not giving a full picture of the IRA campaign.

Table 4: Publication Journal ratings of the source materials

Sources	N/A	Grade 1	Grade 2	Grade 3	All
Journals	1	9	3	6	19
Books	3	1	1	1	6
News articles	2				2
Military/Gov	6				6
Conferences	2	1	1		4
Total	14	11	4	7	37

SOURCES

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of economic perspectives,* 31(2), 211-36.

Armistead, L. (Ed.). (2004). Information operations: Warfare and the hard reality of soft power. *Potomac Books*, Inc. Washington D.C.

Badawy, A., Ferrara, E., & Lerman, K. (2018, August). Analyzing the digital traces of political manipulation: the 2016 Russian interference Twitter campaign. In *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 258-265). IEEE.

Badawy, A., Addawood, A., Lerman, K., & Ferrara, E. (2019). Characterizing the 2016 Russian IRA influence campaign. *Social Network Analysis and Mining*, *9*(1), 31.

Berghel, H. (2017). Oh, what a tangled web: Russian hacking, fake news, and the 2016 US presidential election. *computer*, *50*(9), 87-91.

Bessi, A., & Ferrara, E. (2016). Social bots distort the 2016 US Presidential election online discussion. *First Monday*, 21(11-7).

Bovet, A., & Makse, H. A. (2019). Influence of fake news in Twitter during the 2016 US presidential election. *Nature communications*, 10(1), 7.

Dutt, R., Deb, A., & Ferrara, E. (2018). "Senator, We Sell Ads": Analysis of the 2016 Russian Facebook Ads Campaign. In *International Conference on Intelligent Information Technologies* (pp. 151-168). Springer, Singapore.

Elections. (n.d.) In *Lexico.* Retrieved from: https://www.lexico.com/en/definition/election

Fabre, C. (2018). The case for foreign electoral subversion. *Ethics & International Affairs*, 32(3), 283-292.

Gaughan, A. J. (2017). Illiberal Democracy: The Toxic Mix of Fake News, Hyperpolarization, and Partisan Election Administration. *Duke Journal of Constitutional Law & Public Policy,* 12, 57-139.

Giles, K. (2016). Handbook of Russian information warfare. *NATO Defence College Research Division*. DeBooks Italia Srl. Rome.

Gueorguieva, V., & Simon, R. J. (2009). Voting and Elections the World Over. Lanham, Md: *Lexington Books.*

Hamilton, R. E. (2019). Russia's Attempts to Undermine Democracy in the West: Effects and Causes. *Orbis*.

JP 3-13 (1998*). Joint Publication 3-13: Information operations. Joint Chiefs of Staff. Armed Forces of United States*. Washington D.C. Retrieved 17.07.2019 from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Kessler, G., Rizzo, S. & Kelly M. (2019, Oct 14). President Trump has made 13,435 false or misleading claims over 993 days. *The Washington Post.* Retrieved 22.11.2019 from: https://www.washingtonpost.com/politics/2019/10/14/president-trump-has-made-false-or-misleading-claims-over-days/

Klingemann, H.-D. (2009). The Comparative Study of Electoral Systems. Oxford: *Oxford University Press.*

Levin, D. H. (2016). When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results. *International Studies Quarterly,* Volume 60, Issue 2, Pages 189–202

Levin, D. H. (2018). Voting for Trouble? Partisan Electoral Interventions and Domestic Terrorism. *Terrorism and Political Violence*, 1-17.

Levin, D. H. (2019a). Partisan electoral interventions by the great powers: Introducing the PEIG Dataset. *Conflict Management and Peace Science,* 36(1), 88-106.

Levin, D. H. (2019b). A Vote for Freedom? The Effects of Partisan Electoral Interventions on Regime Type. *Journal of Conflict Resolution*, 63(4), 839-868.

Libicki, M. C. (1995*)*. What is information warfare? *National Defense University, Washington DC Institute For National Strategic Studies.* Retrieved 31.03.2019 from https://apps.dtic.mil/dtic/tr/fulltext/u2/a367662.pdf.

Lijphart, A. (2012). Patterns of Democracy (Vol. 2nd ed). New Haven [Conn.]: *Yale University Press.*

Mueller, R. (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. US Department of Justice*, Washington D.C. Retrieved 17.07.2019 from https://www.documentcloud.org/documents/5955118-The-Mueller-Report.html

NATO. (2009). Allied joint doctrine for information operations. Retrieved 31.03.2019 from https://info.publicintelligence.net/NATO-IO.pdf.

Pennycook, G., Cannon, T. D., & Rand, D. G. (2018). Prior exposure increases perceived accuracy of fake news. *Journal of experimental psychology: general.*

Persily, N. (2017). The 2016 US Election: Can democracy survive the internet?. *Journal of democracy*, 28(2), 63-76.

Polyakova, A., & Boyer, S. P. (2018). The future of political warfare: Russia, the West, and the coming age of global digital competition. *EUROPE.* Brookings.

Richey, M. (2018). Contemporary Russian revisionism: understanding the Kremlin's hybrid warfare and the strategic and tactical deployment of disinformation. *Asia Europe Journal*, 16(1), 101-113.

Schedler, A. (2002). Elections without democracy: The menu of manipulation. *Journal of democracy*, 13(2), 36-50.

Schmitter, P. C., & Karl, T. L. (1991). What democracy is... and is not. *Journal of democracy*, 2(3), 75-88.

Shao, C., Ciampaglia, G. L., Varol, O., Yang, K. C., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature communications*, 9(1), 4787.

Smith, D. (2019, Sep 7). 'Enemy of the people': Trump's war on the media is a page from Nixon's playbook. *The Guardian.* Retrieved 22.11.2019 from: https://www.theguardian.com/us-news/2019/sep/07/donald-trump-war-on-the-media-oppo-research

Theohary, C. A. & Rollins, J. (2011). Terrorist use of the internet: Information operations in cyberspace. *DIANE Publishing*. Washington D.C.

Van Niekerk, B. (2018). Information warfare as a continuation of politics: An analysis of cyber incidents. In *2018 Conference on Information Communications Technology and Society (ICTAS)* (pp. 1-6). IEEE.

Ventre, D. (2016). Information warfare (Revised and updated second edition.). London, England; Hoboken, New Jersey: *iSTE.*

Wilder, B., & Vorobeychik, Y. (2018). Controlling elections through social influence. In *Proceedings of the 17th international conference on autonomous agents* *and multiagent systems* (pp. 265-273). International Foundation for Autonomous Agents and Multiagent Systems.

Ziegler, C. E. (2018). International dimensions of electoral processes: Russia, the USA, and the 2016 elections. *International Politics*, 55(5), 557-574

ATTACHMENT 1 FIRST ATTACHMENT