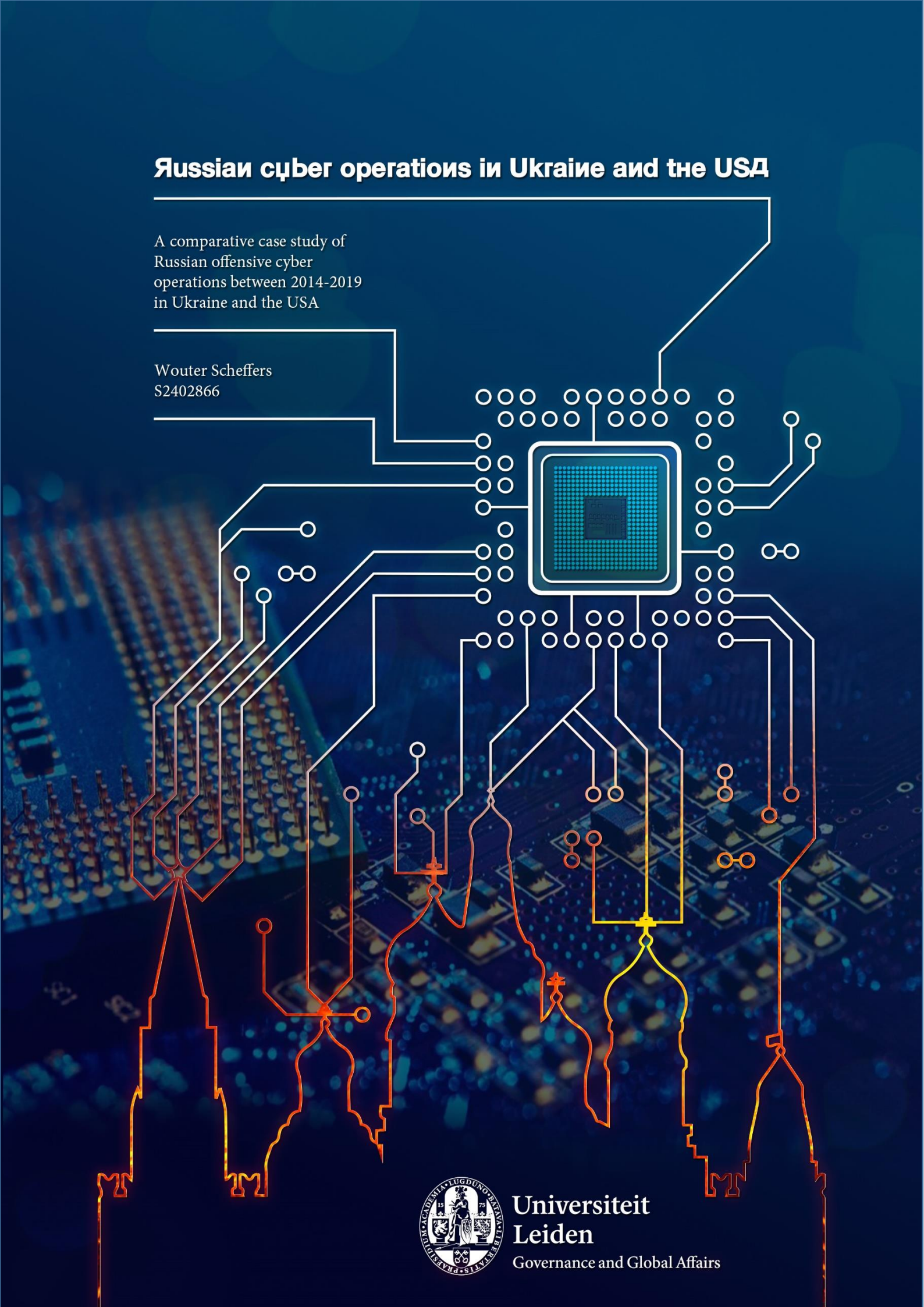
# Russian cyber operations in Ukraine and the USA

A comparative case study of Russian offensive cyber operations between 2014-2019 in Ukraine and the USA

Wouter Scheffers
S2402866



Universiteit Leiden
Governance and Global Affairs

# Abstract

This thesis compares Russian cyber operations against Ukraine and the United States of America between 2014 and 2019. It aims to research which factors influence the different outcomes in the studied operations. The studied operations involve cyberattacks on power grids on the one hand and digital information operations interfering in elections on the other. The results show that Russian power grid cyberattacks in Ukraine are more disruptive than in the USA, while their information operations were more effective in the USA. The argument put forward in this research is that Russia is less hesitant to disrupt critical infrastructure in Ukraine due to is involvement in the Ukrainian conflict. Moreover, there is limited potential of escalation of applying such disruptions in Ukraine. Finally, Ukraine provides Russia with opportunities to test its cyber operations without risking large scale retribution from powerful states.

Information operations targeting the presidential elections have been more effective in the USA than similar operations in Ukraine. In this research it is argued that Ukraine is both more familiar and more resilient to Russian (dis)information operations. Furthermore, the conflict scenario between the two countries causes Ukrainians to be suspicious of pro-Russian narratives. Western media on the other hand amplified the Russian disinformation in the USA. In both countries Russia succeeded in deepening the social polarisation between opposing groups.

# Acknowledgements

Throughout my part time master's program, I have been fortunate with the support I received. It would not have been the same without it. At times it has been challenging to combine work with studying, while also minding other people near me. The latter may have slipped my attention at times. I am grateful to my employer, the Netherlands Ministry of Defence, for giving me the time and funding to follow this programme. I am grateful to my supportive and excellent supervisors James Shires and Tatiana Tropina. It has been an educating experience with both of you all the way. I am indebted to my amazing girlfriend Naomi who's love and patience throughout our lives has been immeasurable, not least during these last few months. Finally, I would like to thank my parents, family and friends. You were genuinely interested in my progress and general wellbeing and have often given me advice. All of you have helped shape this thesis.

# Contents

# 1. Introduction

Tensions between the West and Russia have increased over the course of the past fifteen years. The United States of America (USA) and the North Atlantic Treaty Organisation (NATO) arguably remain among the primary adversaries of Russia in many affairs. The digital world and the power struggle over it symbolise these rising tensions. The number of interstate cyber enabled espionage, sabotage, subversion as well as overall computer network attacks have increased exponentially in the period between 2014 to now. This includes operations attributed to Russia. (Faesen, Torossian, Mayhew, & Zensus, 2019) Not just the number of attacks, but also the intensity and corresponding threats have increased. Evidently this creates a serious security concern for governments worldwide. (Faesen et al., 2019)

The USA and Russia accuse one another of conducting offensive cyber operations, digital espionage and interference in domestic affairs. Russia's Intelligence and Security Services (RISS) are viewed as the preeminent and most capable Russian actors conducting offensive cyber operations.(Connell & Vogler, 2017) Both the American and Ukrainian governments as well as cybersecurity companies have attributed a significant number cyberattacks to Russian Intelligence services. (Greenberg, 2019; Symantec, 2017; US CERT, 2018) These operations are a serious threat to states, but also pose a significant threat to private companies. The infamous NotPetya malware is one of the most prominent examples, causing around $10 billion in damages worldwide and paralysing multinational companies' networks. (Greenberg, 2019, pp. 197–199) Such historic events have made the field of cybersecurity increasingly relevant.

Russian cyber operations have influenced regional politics in Eurasia too. Several countries which were once republics within the Soviet Union have distanced themselves from Russia, some of them now favouring close ties with the West. The Baltic States, Ukraine and Georgia are well-known examples. These strategically important countries are referred to as the *near abroad* by Russia.[1] The deteriorated relationship between Russia and some of its former Soviet Republics has resulted in several conflicts with varying levels of hostility. These conflicts often included the use of offensive cyber operations. (Popescu, Secrieru, Soldatov, & Borogan, 2018)

[1] The near abroad are the fourteen republics that, together with Russia, formed the Union of Soviet Socialist Republics (USSR). The Baltic States, Ukraine and Georgia are among those 14.

In 2014, the annexation of Crimea by Russia and the ensuing civil war in Eastern-Ukraine marked a low point in East-West relations. This conflict has seen the use of various offensive cyber operations. Ukraine also remains among the primary target of Russian digital information operations in 2019. (EU vs Disinformation, 2019) It seems cyber operations have become an inseparable part of interstate diplomacy, competition and political warfare.

Russia has applied similar cyber operations against Ukraine and the USA, with different outcomes. This research examines which factors influenced these different outcomes, aiming to help understand Russian cyber operations from an academic perspective.

This first chapter serves to explain the academic scope, methodology and research questions. Chapter two examines Russia's conception of information operations. Chapters three and four contain case studies of recent Russian cyber operations, providing empirical data to answer the research questions. Chapter three examines Russian cyberattacks targeting power grids in Ukraine and the USA. Chapter four examines cases of digital information operations targeting elections in Ukraine and the US. Finally, in the concluding fifth chapter, the results of the comparative case study as well as limitations of the research and recommendations for future study are discussed.

## 1.1 Literature review & research questions

### 1.1.1 Terminology

The field of cybersecurity has a multitude of terms associated with it. This thesis has chosen to use the following terminology:

All cases in this research are regarded as offensive operations executed by Russia. Herbert Lin defines cyber operations as: "*actions taken against an adversary's computer systems or networks that harm the adversary's interests*". (Lin, 2012) In this thesis Lin's umbrella term (offensive) cyber operations is applied to all studied operations. A subdivision is created to distinguish operations which predominantly target networks, in particular industrial control systems, from operations targeting mostly the non-physical information sphere. It distinguishes **cyberattacks**; digital attacks on physical networks such as control systems, from **digital information operations;** information operations targeting predominantly the non-physical information sphere.

### 1.1.2 Area of research

This thesis is placed in between two subfields of academic research, political science and conflict studies on the one hand and cybersecurity on the other. Its aim is to research the factors influencing the effects that Russian cyber operations have in Ukraine and in the United States. To understand Russian cyber operations, it is necessary to understand the security strategy of the Russian state, its threat perception, and its take on information security and -warfare. This thesis is based primarily on English language sources that analyse these Russian concepts.

### 1.1.3 Russian national security concerns and objectives

According to several European security services, Russia remains among the biggest threats to western national security. (Karlsen, 2019) Not entirely surprising, Russia regards the United States and NATO as the biggest threats to its national security. (Karlsen, 2019)

Developments in the near abroad including Ukraine are an important part of Russia's threat perception. The end of the Soviet Union also signalled the end of its status as a superpower. Several countries in the near abroad have since leaned increasingly westward. Russia attributes these defeats at least partially to western information warfare. (Blank, 2013; Bouchet, 2016) Since President Putin took the oath of office in 2000, Russia has steadily tried to regain its status as a global power. The annexation of Crimea and the war in Donbass are regarded by Russia as a reaction to the ongoing encroachment of NATO and the increasing western influence in Ukraine. These operations are indicative of a more ambitious Russian foreign policy in the last decade. (Dobbins et al., 2019) Russia has applied a broad range of cyber operations in this conflict.(Greenberg, 2019, p. 313)

The other focus of this research is the Russian perspective towards cyber operations in conflict or competition scenarios with the West and in particular the United States. There is no declared state of war between Russia and the West. However, as Russia's highest ranking general Valery Gerasimov has stated: "*In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template".*(Gerasimov, 2013) Although this citation has been ill-analysed and misinterpreted by many, British scholar Galeotti pointed it out to argue that Russia regards itself threatened by an expansionist western and NATO agenda. (Galeotti, 2016a)

### 1.1.4 Non-linear strategy

Galeotti argued that to counter these threats against numerically stronger adversaries, Russia relies on a non-linear strategy. (Galeotti, 2019) This strategy employs a wide range of both military, but mostly non-military means against countries and adversaries that are not necessarily at war with Russia. This applies to the near abroad as well as the west. Non-linear *warfare* has no clear boundaries and aims to subvert an adversary's political and social structures. (Schnaufer, 2017) Clausewitz's most famous statement *"war is continuation of politics by other means"* is thus still relevant. (Clausewitz, 1832) Information warfare is an important part of Russia's non-linear strategy, and part of Russian information warfare are cyber capabilities. (Allen & Moore, 2018) Cyber capabilities have grown in importance because they are suitable for covert operations, are less risky than for example covert human intelligence (*humint)* operations and the countries that Russia perceives to be the largest threats are vulnerable to cyberattacks. (Karlsen, 2019)

Hybrid warfare is sometimes used interchangeably with non-linear warfare. However, according to Schnaufer, it fails to aptly describe Russian strategy, particularly in Ukraine. Hybrid warfare includes the involvement of non-state actors, insurgents, criminals, and terrorists in a conflict scenario. The civil war in Ukraine however is fought primarily between the Ukrainian armed forces and largely militarised separatists supported by Russia. Moreover, hybrid warfare definitions often*: "do not include the information, economic, social, and political aspects of warfare that states can apply on a much larger scale compared to non-state actors and for a much different intent".* (Schnaufer, 2017)

Non-linear warfare combines types of warfare such as conventional, irregular, political and information warfare, coordinated by a state. (Kofman & Rojanksy, 2015; Schnaufer, 2017) This includes cyber operations and cyber enabled *active measures* (see 1.1.6). Hybrid warfare is western coined term often used to describe Russia's non-linear approach in Ukraine. (Renz, 2016) In the Ukraine conflict, conventional and non-linear warfare co-existed, and both were supported by cyber operations. The Russian annexation of Crimea is characterised by the absence of direct force and a heavy reliance on psychological influence operations. As such non-linear warfare is a better suited umbrella term for the Russian operations in Ukraine following the Crimea and Donbass conflicts.(Galeotti, 2016a; Schnaufer, 2017)

### 1.1.5 Strategic value of cyber operations

In an article written by Max Smeets, offensive cyber operations are divided between counterforce and countervalue operations. Counterforce operations target military targets or other operationally relevant targets.(Smeets, 2018) Cyberattacks which aim for such targets can be considered counterforce operations. Countervalue operations target a state's centres of power, for example critical infrastructure.(Smeets, 2018) The lines between these types of operations can become somewhat blurry. An example is found in the 2008 Russo-Georgian war, when Russia used cyberattacks against several civilian targets alongside a conventional military offensive in Georgia. On the other hand, the 2015 cyberattack on the Ukrainian power grid, part of the case studies in this research, is given as an example of a countervalue operation. However, at the time Russia was involved in armed conflict with Ukraine too and used several other military means against its government. Furthermore, Smeets argues that cyber operations can be applied in similar fashion as special operations, adding they are often used "pre-escalatory"; before a conflict erupts. (Smeets, 2018) However, it is clear that this was not the case in Ukraine, where conflict had already begun.

The theory is useful though, as it concludes: "*The potential use of offensive cyber capabilities provides an extra option to state leaders across a range of situation"*. (Smeets, 2018) It does *not* explain why Russian cyber operations lead to different outcomes in Ukraine compared to the USA. An example of countervalue cyber operations are *active measures*. The application of cyber operations as active measures provides another useful point of view.

### 1.1.6 Active measures

Cyber capabilities are in some ways a continuation of Soviet active measures in contemporary Russia. (Bentzen, 2018; Rid, 2020b) Active measures are a form of political warfare that aims to weaken an adversary from the inside, using tools such as forgery, disinformation, covert operations, blackmail, terrorism, and assassinations. Often they include disinformation, but built up around elements of truth. (Abrams, 2016) Cyberattacks can be considered active measures, when they are not applied in a narrow, counterforce type of operation. Digital information operations are particularly suitable as active measures and can also be countervalue operations.

In the 1980's the United States erected a dedicated interagency group solely to counter Soviet active measures. This Active Measures Working group battled Soviet disinformation with success, leaving president Gorbachev with the decision to discontinue these measures. (Schoen & Lamb, 2012) Being vigilant to Russian disinformation became less pressing for the USA after the dissolution

of the Soviet Union. This thesis will delve deeper into the use of *active measures* by the Russian Federation *after* these historic events, and how they are integrated into contemporary cyber operations.

Two things are important to add to this from a US perspective. In the US government official cyber strategy, a distinction is made between cyberattacks on networks, and disinformation and active measures. (The White House, 2018) There currently is no specific US agency responsible for countering active measures, as opposed to several agencies responsible to countering cyberattacks on networks in the USA. (Raymond, 2020) The relevance of this will be further explored later.

### 1.1.7 The role of the Intelligence agencies

Russia's Intelligence and Security Services (RISS) are first and foremost the responsible agencies for Russian cyber operations. (Heickerö, 2010) These agencies have differing responsibilities. The domestic services such as the FSB are likely primarily responsible for informational security: protecting strategic information of great value to Russia. (Heickerö, 2010) Foreign intelligence service SVR and military intelligence service GRU are active in matters of digital (military) espionage as well as covert sabotage and subversion in foreign countries.

There is competition between the different services as well as overlapping areas of responsibility, which means that there are numerous exceptions to this rule of thumb. RISS are governed by different parent organisations and some are under direct control of the president of the Russian Federation. This is reflected in differing organisational cultures and *modus operandi* among RISS. The GRU, for example, is known to be rather aggressive using all means necessary, whereas the SVR is known for a more subtle, long term approach. (Galeotti, 2016b)

Russian cyber operations are primarily executed or coordinated by RISS. Thus, it can be argued that cyber operations are likely to support their traditional activities too, which include espionage, subversion, and sabotage.

These paragraphs lay the foundation of the first hypotheses: Among Russia's foremost national security threats are the West and the expansion of NATO into its near abroad. The United States and NATO (the West) are numerically and conventionally stronger adversaries. To counter these threats, Russia relies mostly on RISS to execute non-linear operations, including traditional intelligence activities such as espionage and active measures. RISS use cyber operations as non-military means and intelligence capabilities to weaken adversaries and gain a strategic advantage in interstate competition and conflict.

The review explains why Russia uses cyber operations in conflicts but fails to explain why similar operations lead to different outcomes in the studied countries. This implies there are other, unknown factors that influence Russian cyber operations.

The goal of this research is to bridge this gap by looking for these factors. To this end, the following main research question in formulated:

**Which factors influence the different effects of Russian cyber operations in Ukraine compared to similar operations in the USA?**

One of these factors could be different Russian strategic approaches towards cyber operations in the near abroad (Ukraine) versus the West (United States). The first chapter examines this theoretical approach. The hypotheses are derived from the identified gap as well as the concepts covered in this literature review.

This leads to the following, first sub research question:

**1. Is Russia's theoretical understanding of offensive cyber operations in Ukraine different from such operations in the USA?**

Based on the reviewed concepts, the following hypotheses have been created to fill this gap:

*H 1.1: Russian Intelligence and Security Services use cyber operations as tools of non-linear warfare against Ukraine, while avoiding escalation and potential armed conflict with the West.*

And:

*H 1.2: Russian Intelligence and Security Services use cyber operations as active measures, aiming to subvert and sabotage the USA, and as political espionage, supporting Russia's national security objectives.*

As stated previously, the United States government thinks differently about countering digital information operations and active measures compared to countering cyberattacks. The effects of these different Russian cyber operations vary as well. In Ukraine, these two concept are mentioned separately too, although Ukraine's national security strategy has as somewhat more holistic approach. (Office of the President of Ukraine, 2016; Streltsov, 2017) The different characteristics of such operations could be a factor influencing the effects of Russian cyber operations as well. Considering all this, chapter two and three will research these Russian cyber operations as two separate types: cyberattacks on networks and digital information operations. The following concepts in academic literature are relevant to this approach.

### 1.1.8 Home-field advantage

History and geography play an important role in the power of states in the digital realm. The world wide web known now as the internet started in the 1960's as a research project within the U.S Department of Defence, known as ARPANET.[2] In the following decades, American universities and companies strengthened the leading position of the US in the world wide web to this day. Buchanan refers to this position as a 'homefield advantage'. (Buchanan, 2020, pp. 16–20)

In the near abroad, Russia can benefit to some extent from being the successor of the Soviet Union as well. In this capacity, Russia has technological, infrastructural, and cultural knowledge of those countries that once were part of the Soviet Union. Much of the telephone and other network infrastructure used in a country like Ukraine originates from the Soviet era. (Soldatov & Borogan, 2017) Ukraine and Russia too share large parts of their history and culture. Moreover, many Ukrainian citizens speak or understand Russian. Finally, there is a significant ethnic Russian population in Ukraine. (State Statistics Committee of Ukraine, 2001) Especially in Ukraine's separatist regions, pro-Russian sentiments have grown stronger during the civil war, although only a minority of the population supported separatism before it was declared. (Giuliano, 2018)

This home-field advantage is not present for Russia when conducting cyber operations in the United States. In fact, according to Buchanan, the United States actually have a home-field advantage over Russia.(Buchanan, 2020, pp. 16–20) Consequently, this could be a factor influencing the difference in effects Russian cyber operations have in Ukraine as opposed to the United States.

### 1.1.9 Social polarisation & cyber operations

The internet is increasingly important as a news medium. In the United States, almost two-thirds of the population gathers their news from social media. People are more susceptible to polarisation in an online environment than in the physical world. (D. Gallacher & W. Heerdink, 2019) Furthermore, digitally disseminated content travels much faster and can reach people that do not have access printed media or other forms of traditional journalism. As such, the internet and social media could provide very suitable tools for any actor aiming to influence a target audience. Furthermore it could be used to exploit existing tensions in order to subvert societies. (Golovchenko, Hartmann, & Adler-Nissen, 2018)

[2] Advanced Research Projects Agency Network

In countries where traditional media are either censored or even steered by governments, this has another benefit. Governments generally have less control over internet news media and as such digitally disseminated news can fill a gap for citizens looking for alternative narratives. (Szostek, 2018) Russia has used internet and social media to spread their narrative on several occasions. Considering their experience and the comparative salience Russia has towards the west in terms of information warfare, it would make sense to exploit this non-linear warfare strategy against the USA.

As explained previously, this research maintains the distinction between cyberattacks and digital information operations. Moreover, the literature describes Russian strategy to be non-linear in order to counter conventionally superior adversaries. The academic gap that remains is, *which factors* influence the different effects that similar Russian cyberattacks have in Ukraine compared to the USA. This leads to the second sub research questions:

**2. Which factors influence the different effects of Russian cyberattacks on the power grid in Ukraine compared to similar operations in the USA?**

Considering Russian conception of non-linear warfare and the home-field advantage it has in Ukraine, the following hypotheses can be derived specifically for the cyberattacks.

*H 2.1 Russia's cyberattacks in Ukraine are dependent on the factors; technical 'home-field advantage', societal knowledge and a conflict scenario, which are absent in the USA.*

*H 2.2 Russian cyberattacks in the USA are deliberately designed to avoid extensive damage, considering the superior power of the USA in conventional and cyber warfare.*

*H 2.3 Russia tests cyberattacks in Ukraine which makes them operational for potential use against countries such as the USA.*

The specific choice for power grids is based on the available cases to analyse, while maintaining sufficient similarity. This is further explained in the chapter on research design.

Finally, in chapter three the process is repeated for Russian digital information operations. The previously mentioned home-field advantage in Ukraine relied on Russian language proficiency, cultural knowledge, and an ethnic Russian minority. These characteristics could be otherwise relevant for Russian digital information operations. Golovchenko et al (2018b), for example, found that opinions regarding responsibility of the downing of MH-17 between pro-Russian and pro-Ukrainian users on Ukrainian social media was very polarised. Both sides applied information operations to influence public opinion. Interestingly,

ordinary citizens had a significantly stronger influence on the debate than any state or commercial users on social media had. (Golovchenko et al., 2018)

Sentiments towards Russia among Ukrainian citizens, especially given the ongoing conflict scenario, could be a factor influencing the effects of Russian digital information operations. Another factor which could be relevant in both countries is the (lack of) familiarity with Russian disinformation and active measures. Referring to the discontinuation of Soviet active measures after 1987, the USA had since perhaps grown unfamiliar with similar Russian operations. Ukraine on the other hand is the most targeted country of Russian disinformation campaigns. (EU vs Disinformation, 2019) Furthermore it has been under the influence of Russia and its predecessors for centuries. Considering these arguments, chapter three's hypotheses have been formulated.

The academic gap identified is accordingly: which factors influence the different effects of similar *digital information operations*. This leads to the third sub research question:

**3. Which factors influence the different effects of Russian digital information operations targeting elections in Ukraine compared to similar operations in the USA?**

Again, the specific target of elections is based on cases available for study. The following hypotheses have been formulated:

**Hypotheses**

*H 3.1: Russian digital information operations in Ukraine are designed to damage the confidence of the population in the state and those who lead it as well as to exploit and amplify social polarisation.*

*H 3.2: Russian digital information operations in Ukraine are dependent on the factors: Ukrainian sentiments concerning Russia, familiarity with disinformation and a conflict scenario.*

*H 3.3: Russian digital information operations in the USA are dependent on the factors: familiarity with Russian information operations, a climate of social polarisation and the dissemination of 'Russian' content by domestic media.*

## 1.2 Research Design

The sub research questions, and the accompanying hypotheses have been introduced in the initial literature review. The goal of this paragraph is to explain the design choices which have led to the hypotheses.

This research aims for hypotheses which are both directional and correlative. Correlative in this context means that there is a relation between the independent and the dependent variable; the different outcomes of similar Russian information operations in two countries. Directional means that a prediction is made by a researcher regarding the nature of the relationship between two variables of a research, for example a positive or negative change, relationship, or difference. (Salkind, 2012) Since this is a qualitative study, quantitative change is not part of the focus. For this research two different target categories are compared, two cases concerning critical infrastructure and again two cases concerning presidential elections.

### 1.2.1 Epistemology

The field of cybersecurity is both relatively new and multi-disciplinary. This research aims to use theories from the field of politics and international relations (PIR) applied to a cybersecurity issue.

The thesis is based on a positivist approach on international relations. Positivism is the opposite school of thought to interpretivism. It is based on the premise that PIR is a field comparable to natural sciences in which positive laws can be created.(Lamont & Boduszynski, 2020) This means scientifical research *"should be conducted in a systemic replicable and evidence based manner that leads to conclusion about causality"* (Gerring, 2011) Positivist research aims to maximise causal inference between an independent variable and a dependent variable. The main research question strives to find this causal inference.

### 1.2.2 Methodology & case selection

The research will be conducted as a qualitative literature study, using a comparative (observational) case research design. Qualitative research: "seeks illumination, understanding, and *extrapolation to similar situations".* (Hoepfl, 1997) In this research it is conducted using a relatively small but highly similar number of real-world cases that can be analysed through literature study. The disadvantage of such a design is that it limits the level of control the researcher has on determining the variables. However, the advantage of such a design is that it generally has higher external validity, meaning the results are better suited to be generalised for other, similar cases. (Lamont & Boduszynski, 2020)

Since this thesis has a positivist, causal design, the main research question has several underlying hypotheses which will be tested.

### 1.2.3 Sources, data dependability & validity

The used sources are derived mostly from academic books, journals, and papers as well as official government publications and reputable journalism. The technical analyses include quite a few sources derived from private cybersecurity companies. Since it is written in partial fulfilment of an academic degree, it cannot and does not include classified material. Considering the focus on cyber operations coordinated by RISS, official Russian sources concerning this are often classified and thus unavailable, However, the studied Russian cyber operations have been exposed and analysed by cybersecurity companies, western government agencies and journalists, which mitigates this limitation to a large extent. Certain empirical data is collected from declassified intelligence reports which include censored evidence, meaning parts of it are unverifiable.

Considering that the subject of the research is often clouded in secrecy, it is almost inevitable to use some of these declassified reports despite these limitations. The dependability of the data is increased by using other independent sources which confirm statements made in these reports. (Golafshani, 2003) Another design choice which influences dependability is the sample size. To this end the research includes four cases of Russian cyber operations, two in Ukraine and two in the USA. Additionally, all four cases in fact consist out of multiple subcases, for example different power stations and grids which fell victim to cyberattacks in both Ukraine and the US. Finally, reliability is "*a consequence of the validity in a study".* (Golafshani, 2003)

Adcock and Collier argue that in political science, construct validity is the subsuming factor to assess the validity of a qualitative research. In short, this means whether or not "*a test measures the intended construct".* (Adcock & Collier, 2001) The foundation of this research's construct validity is the literature review, which is based on established and peer-reviewed scientific literature. The construct validity is increased by using positivist causal hypotheses, which are derived from the literature review. Finally, triangulation increases the validity of a research. (Golafshani, 2003) This research again aims to do so by using the different selected cases and subcases searching for: "*convergence among multiple and different sources of information",* which increases the validity and consequently the reliability of the research. (Golafshani, 2003)

### 1.2.4 Russia as subject of study

In the period leading up finalising this research, new allegations high-profile Russian cyber operations kept making headlines. In July 2020, it involved Russian attempts to obtain COVID-19 related research information. In December 2020, it allegedly involved Russian intelligence agency SVR[3] which had compromised *hundreds* of companies using SolarWinds software, including the nuclear research facilities, the US State Department, the Pentagon, and cybersecurity company FireEye. (David, E. Sanger, Perlroth, & Schmitt, 2020) Notably, FireEye has inquired into several Russian state hacker collectives.(Newman, 2020) It is an indication of just how pressing the threat of Russian cyber operations still is. According to the website Privacy Affairs, Russia is responsible for 27% of all state attributed cyber operations. (Robinson, 2020) Carnegie Mellon University found Russia among the top attacking countries as well, with 0.52 launched cyberattacks registered for *every* computer in Russia. (Mezzour, Carley, & Carley, 2016) Although countries like China and Iran are conducting offensive cyber operations too, Russia remains among the first to integrate cyber operations into both armed conflict as well as interstate competition other than war. Russia also stands out in sophistication of its cyber operations. (Buchanan & Sulmeyer, 2016) As such, it provides a unique as well as current subject of study.

### 1.2.5 Case selection criteria

The selection of cases is critical to the outcomes of any comparative case study. It also has an inherent weakness. A particular case of a Russian cyber operation interfering in a foreign state does not automatically draw general conclusions about every other cyber operation that Russian intelligence conducts. However, generalisations can be made when the cases are representative and have similar independent variables. (Lamont & Boduszynski, 2020)

The subject of the research is Russian offensive cyber operations, this is also referred to as the unit of analysis. Next, a two-by-two comparative case research design is created. This *most similar systems* (MSS) design aims to compare similar cases in Ukraine and in the USA, while keeping other variables as similar as possible too, improving the causal inference. (Lamont & Boduszynski, 2020)

The dependent variable is the difference in outcomes of similar Russian cyber operations. There are two, distinct independent variables: the first being the geographical area in which the cyber operations took place, either in Ukraine or the United States of America (USA). The second independent variable is the type

[3] See appendix 1 for elaboration on APT 29

of cyber operation, cyberattacks on critical infrastructure on the one hand, and digital information operations on the other. Further explanation of these variables will be given further on. Keeping all this in mind, four cases have been selected. Schematically the research design looks as follows:

**Case selection model**

| **Independent variables** | **Ukraine** | **USA** |
|---|---|---|
| Critical infrastructure | C1: BlackEnergy3/CrashOverride | C2: Dragonfly 2.0 |
| Digital information operations | C3: 2014/2019 presidential elections | C4: 2016 presidential elections |

Additional to this model, the following criteria have been selected for the cases:

- The cases are attributed to Russia with a certain degree of confidence.
- The cases are regarded as representative of Russian cyber operations within the academic discourse and within their distinct category: infrastructure or information sphere.
- The cases are selected based on a large degree of similarity, aiming to rule out as many other factors as possible which can influence the outcome.
- The cases are limited in time; the period between 2014-2019, aiming to limit the influence of developing Russian strategy and tools while maintaining similarity.

### 1.2.6 Selected cases

**Critical Infrastructure**

2015-2016 Cyberattacks on Ukrainian power grid.

2016-2017 DragonFly 2.0 cyberattacks on US power grid.

These cases have been selected based on a confident attribution to Russia or strong suspicions of links towards Russia. The cyber operations both targeted the same kind of critical infrastructure, power grids, with similar attack characteristics. As such these cases are suitable for this case study.

**Digital information operations**

2014/19 Ukrainian presidential elections

2016 US presidential elections

Again, these cases show similar attack characteristics and target the same phenomenon. These cases have been selected to keep as many as possible variables similar, striving for optimal causal inference. Furthermore, there is plenty empirical data on these cases.

# 2. Russia's conception of offensive cyber operations

## 2.1 Introduction

To understand Russia's use of offensive cyber operations, this chapter will delve into the history and strategic thought behind these operations. Is there such a thing as *cyber*security in Russia? Are cyber operations the exclusive domain of the RISS? The second part of this chapter covers Russia's national security doctrine and the role of cyber operations in it.

## 2.2 Information operations versus cyber operations

The word cyber is used in Russian strategic theory exclusively to describe western strategies and capabilities. Western countries such as the United States have the tendency to regard cyber as the fifth domain of warfare. (Hayden, 2011) The other domains are land, sea, air, and space. Three of these domains usually have their specialised branch of the armed forces: navy, army, and air force. Some countries have a separate space force and cyber command as well.

Russia has a different, more comprehensive approach towards cyber operations. The premise of this approach is that cyber operations are in fact part of information operations (IO), as opposed to the technical and network oriented approach that western countries have. (Connell & Vogler, 2017; Giles, 2011) It has existed alongside other traditional forms of exercising power in both physical and psychological domains for decades. (Giles, 2016b). Russia applies information operations both in conventional wars as well as below the threshold of armed conflict. Consequently, IO are not exclusively the domain of the Russian armed forces, but of all government bodies. (Connell & Vogler, 2017)

Russia views information operations as: "*means the state uses to achieve its goals in international, regional and domestic politics and also to gain a geopolitical advantage. . . ".* (Darczewska, 2014)

The official Russian military doctrine on information security defines information warfare (IW) as follows:

"*…The ability to, among other things, undermine political, economic, and social systems; carry out mass psychological campaigns against the population of a state in order to destabilize society and the government; and force a State to make decisions in the interests of their opponents"* (T. Thomas, 2018)

These definitions imply that IO and IW are viewed as strategic and operational tools employed by the state through its security institutions, such as the military *and* the intelligence community. Both definitions mention the psychological

aspect of cyber operations, indicating the importance of this particular element. Furthermore, cyber operations can be deployed in interstate competition, in all domains of warfare and in varying intensity levels of conflict. [4] [5]

Information Warfare is not clearly defined in western sources. In the USA, the difference between IO and IW has been defined as the absence of war or armed conflict. When armed conflict is involved, information operations become part of what is called information warfare. However, there is no clear difference between IO and IW in Russian sources. (Theohary, 2020) More importantly, there is no real difference between cyberattacks on physical networks or infrastructure on the one hand, and operations targeting the information sphere on the other.

The RISS are on the forefront of the execution of Russia's IO. (Heickerö, 2010) Consequently, this research focusses on Russia's intelligence services and in particular their offensive cyber operations in Ukraine and the west. The Soviet roots of the Russian Intelligence agencies have influenced how they operate nowadays. (Abrams, 2016; T. L. Thomas, 2010) Therefore, the next paragraph will delve into the history of the IO in the Soviet Union.

## 2.3 Historical context of Russia's information operations

Russia's conception of information operations and information security can be traced back to its Soviet past and even further. The father of the Soviet Union, Vladimir Ulyanov (Lenin) defeated his opponents against unfavourable odds, by mobilising the masses to revolt against the Tsar and join the Bolshevik cause. The Bolsheviks made extensive use of propaganda and information operations in doing so. After they had seized power, Lenin and his Soviet comrades had to strengthen their hold to power by eliminating internal opponents and regime dissidents whilst safeguarding the support of the people (the proletariat). Propaganda played an important role in this. The Soviets used the entire information sphere including printed media such as newspapers and pamphlets and radio broadcasts to spread their propaganda. (Siggett & Capstone, 2017). To consolidate its position of power domestically, the Soviet Union largely tried to

[4] The military generally defines three levels of warfare, starting with strategic, then operational and finally the tactical level.

[5] Information Operations (IO) are more narrowly defined in western military doctrines. For instance, the American definition of IO is as follows: "*The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own"*(Joint Chiefs of Staff USA, 2012)

control nearly all information sources available to its citizens. This concept of 'information security' turned the Soviet Union into a bastion of secrecy, which helped to safeguard the survival of the Soviet regime (Soldatov & Borogan, 2017)

An important role in safeguarding secrets and keeping threats at bay was, and still is, a responsibility of the intelligence and security services. During the Soviet era, the primary security service was the KGB.[6] Lenin and his successor Stalin were very aware of the power of information, propaganda, and mass media: they had used it extensively to stay in power. The Soviet leaders subsequently gave the security services, primarily the KGB, an increasing responsibility in controlling the information sphere. Consequently, newspapers, theatres, films, literature and poetry were censored by an array of different committees and officers. (Soldatov & Borogan, 2017)

During the Cold War, the Soviet Union (USSR) was facing many challenges: protecting the sovereignty and unity of its vast territory, maintaining the planned economy, fighting an (ideological) war with its adversaries, and so on. Additionally, the Second World War had taken its toll on the Soviet Union. It had to rebuild and restore large parts of its cities, infrastructure, and industry. All these efforts required significant funds, forcing the USSR to set priorities for it its security strategy. (Davis, 2002) (Abrams, 2016)

When the Cold War against the West and predominantly the United States started to intensify, both sides got involved in an arms race which again required unprecedented military-scientifical budgets. At the pinnacle, CIA analysis set the military budget of the USSR at 17.8% of GDP in 1988, yet it was still losing this arms race. (Davis, 2002) Whereas the USSR could not compete with the USA in military spending and technological advancement, it was on par or ahead of the USA when it came to using (counter-)intelligence, espionage and tools of (dis)information against its adversaries. (Abrams, 2016).

[6] **K**omitet **G**osudarstvennoy **B**ezopasnosti; or Committee for State Security.

## 2.4 Active measures

Active measures can be subdivided into three categories, white, grey, and black. White active measures are those executed by government officials using diplomacy, foreign policy, and state media. Black active measures are covert, illicit activities conducted by intelligence agencies such as the KGB and the military's Main Intelligence Directorate (GRU) without using diplomatic covers. The grey active measures are those activities that hover in between. (Abrams, 2016)

In the Cold War, both sides used active measures against each other. However, after the rise of the Berlin Wall (1961) western countries gradually stopped doing so, which caused the loss of their know-how. The age of the internet and social media changed the pace and nature of active measures. In 1995 only about 0.5% of world population had access to the internet. In 2008 this number had gone up to nearly 22%. (Internet World Stats, 2020) The ability to spread disinformation faster and to a larger audience meant that active measures became more active, less sophisticated, and less controllable.

Finally, disinformation and active measures do not blend well with democracy. This means that strong democratic countries are less capable in deploying active measures. However, democratic foundations also provide the best defence against it. Conversely, deploying active measures against an adversary simultaneously erodes and undermines a country's own democratic foundations. (Rid, 2020b, p. 14)

## 2.5 End of the Cold War

The dissolution of the Soviet Union was a dramatic turning point in Russian history. Influential Russian military strategists attribute this defeat to a comprehensive information warfare campaign led by the United States. (Giles, 2016a) The colour revolutions in former Soviet republics such as Georgia, Ukraine and Kyrgyzstan dealt another blow to Russian foreign interests. Pro-Russian autocratic leaders were replaced by governments which often sought to improve relations with western countries, some even voiced a desire to join NATO. (Selhorst, 2016)

Russia attributed these revolutions to foreign intervention and information warfare against what it regards as its *near abroad.* In the 21st century the Arab Spring revolutions led to the ousting of several long serving autocrats in the Middle East. High ranking Russian officials viewed this as a largely digital campaign orchestrated by the United States. Russia again felt threatened by this western, information-driven 'expansion'. (Allen & Moore, 2018)

Russia's new powerbrokers, the S*iloviki*,[7] agreed that their country had lost too much power, influence, and prestige on the international stage, partly due to this information war which the West was waging on them and their former allies. Among those *Siloviki* was future President Vladimir Putin. Putin served as a KGB officer between 1975 and 1991. Later, he returned to its primary successor, the Federal Security Service, or FSB, as its director. As a KGB officer who had served in East-Germany (DDR), Putin is familiar with the concept of active measures and IW. (Abrams, 2016) Russia under Putin aspires to regain its position as a regional and eventually global power and will use IW to reach its objectives.

## 2.6 Russia's national security strategy

The official and latest publicly available version of Russia's national security strategy was formalised in December 2015. The basic premise as laid out in article 6 is as follows:

*" The protection of the individual, society, and the state against internal and external threats, in the process of which . . . the sovereignty, independence, state and territorial integrity . . . of the Russian Federation are ensured . . . National security includes the country's defence and all types of security . . . primarily state, public, informational, environmental, economic, transportation, and energy security . . . "* (IEEE, 2016)[8]

In article 7, another objective is mentioned: *". . . increasing the Russian Federation's economic, political, military, and spiritual potentials and for enhancing its role in shaping a polycentric world"*. (IEEE, 2016) This illustrates Russian ambition to challenge western dominance, to become a centre of power and to strive for a polycentric world.

Several articles in the 2015 strategy point towards external threats posed by the USA and NATO in particular. Both are explicitly mentioned as prime external threats for Russia in article 15:

- The "*Build-up of the military potential of NATO"*
- NATO's "*violation of the norms of international law",*
- "*The further expansion of the alliance",* and
- *"The location of its military infrastructure closer to Russian border creating a threat to national security".* (IEEE, 2016)

[7] Literally: "People of force"; politicians and other powerful men in Russia that often had a military or intelligence background.
[8] Besides matters of sovereignty and defence, the national security strategy also encompasses matters of individual security, economic growth, energy security and improving the international prestige of Russia.

Then the strategy explicitly mentions the negative influence the USA and the EU have had on Ukraine and the regional security situation following the Ukraine crisis in article 17:

"*The support of the United States and the European Union for the anti-constitutional coup d'état in Ukraine led to a deep split in Ukrainian society and the emergence of an armed conflict. The strengthening of far right nationalist ideology, the deliberate shaping in the Ukrainian population of an image of Russia as an enemy . . . and the deep socioeconomic crisis are turning Ukraine into a chronic seat of instability . . . in the immediate vicinity of Russia's borders*". (IEEE, 2016)

This citation is indicative of Russian concern with the geopolitical situation in Ukraine. This is reflected in the military doctrine which stresses the importance of Ukraine and the near abroad in Russia's national security.

Important to this research is Russia's view on informational security within its national security strategy. Informational security is explicitly mentioned multiple times which indicates its importance. Citations from Russia's security strategy illustrate Russia's perception of being threatened by the West and USA. One article mentions information technologies as geopolitical tools used by other countries against Russia:

21: *"The intensifying confrontation in the global information arena caused by some countries' aspiration to utilize informational and communication technologies to achieve their geopolitical objectives, including by manipulating public awareness and falsifying history, is exerting an increasing influence on the nature of the international situation"* (IEEE, 2016)

These statements are indicative of the Russian perception that it is embroiled in an (information) war with the West. Furthermore, this paragraph has shown that Russia considers the USA, NATO, and the latter's expansion drive as the foremost threats to its national security.

## 2.7 Non-linear & grey zone warfare versus cyber operations

Hybrid warfare is a term used by western institutions and governments to describe offensive operations of Russia, including those in Ukraine. It combines types of warfare such as conventional, irregular, political or information warfare. (Kofman & Rojanksy, 2015) A better suited term for such Russian operations is non-linear warfare. This includes cyber (enabled) operations and active measures, as were mentioned before. Although neither new nor exclusively Russian, the hybrid warfare label sticks to Russian offensive (cyber) operations despite scholars' attempts to discard it.

Russian military strategists view information warfare and consequently cyber operations as an asymmetrical (non-linear) strategy. A relevant quote on asymmetrical measures states: "*Important strategic facilities to damage include . . . major industrial enterprises, important communications facilities and installations posing a potential environmental hazard. Inflicting such damage in nonmilitary spheres is an asymmetric measure"* (T. Thomas, 2014) Such strategic facilities include the targets of Russian cyber operations covered in this research.

In Ukraine, there is an ongoing civil war between the Ukrainian armed forces and armed separatists in the eastern provinces of Donetsk and Luhansk, together known as Donbass. These separatist are supported by Russia. Furthermore, the Crimean Peninsula, with its ethnic Russian majority and strategic position in the Black Sea, was annexed by Russia following the Euromaidan revolution of 2014. As mentioned before, this revolution is regarded by Russia as an illegal coup d'état that increased insecurity and animosity between the two countries.

In both regions, Russian armed forces and RISS have 'engaged' the Ukrainian and Russian population. In this conflict, Russia has made extensive use of offensive cyber operations, which will later be covered in detail. It included an intelligence war waged by RISS "*spreading despair and disinformation, encouraging defections, and breaking or corrupting lines of command and communications".* (Galeotti, 2015) The operations thus affected both the information sphere as well as physical targets.

Examples of such operations are severing (digital) communications between Crimea and Ukraine, psychological operations through social media and the use of anonymous soldiers.[9] The Russia-Ukraine conflict is often seen as exemplary of Russian non-linear warfare. Russian operations have been successful in Crimea but much less so in Donbass. These operations are thus neither easily replicated elsewhere, nor a blueprint for Russian non-linear warfare. (Kofman & Rojanksy, 2015)

Grey zone warfare is another western coined term, describing the zone in between peaceful relations and conventional war. It is considered a form of political warfare filling the gap between diplomacy and open war and used *"Where traditional statecraft . . . is ineffective and large-scale conventional military options are not suitable or are deemed inappropriate for a variety of reasons . . . It is a population-centric engagement that seeks to influence, to persuade, even to co-opt"*. (Votel, Cleveland, Connett, & Irwin, 2016)

[9] These 'little green men' wore no Russian insignia on their uniforms and claimed to be Crimean citizens protecting their homeland, while in fact they were Russian military.

Russia also uses such capacities to fight the information war with the West, in an effort to challenge western worldwide information dominance. (Pomerantsev & Weiss, 2014) Given the absence of a civil or conventional war between the USA and Russia, this might be characterised as a form of grey zone warfare. In similar fashion to non-linear war, it uses nearly all means available and necessary other than conventional war to achieve its objectives. Cyber operations are very suitable tools of political and non-linear warfare. (Karlsen, 2019) When properly applied, they:

- Are rarely interpreted as an act of war.
- Provide asymmetric advantage against technologically superior adversaries.
- Provide fast and accessible access to an adversary's population.
- Provide strategic ambiguity and plausible deniability.
- Provide excellent tools of (political) espionage. (Karlsen, 2019)

These potential benefits combined with historically developed information security views help explain why Russia uses cyber operations both in Ukraine and the USA, although with different objectives.

## 2.8 Sub conclusion

The first sub research question was:

*1. Is Russia's theoretical understanding of offensive cyber operations in Ukraine different from such operations in the USA?*

Based on the studied sources, Russia views cyber capabilities as tools of information warfare that can be deployed on varying intensity levels of conflict. The fact that cyber operations allow Russia to maintain plausible deniability and strategic ambiguity is beneficial too. Russia can and does simply deny being involved in certain operations, perhaps losing the plausibility from time to time. The following hypotheses were defined:

*H 1.1: Russian Intelligence and Security Services use cyber operations as tools of non-linear warfare against Ukraine, avoiding escalation and potential armed conflict with the west.*

Non-linear warfare is not an *official* Russian strategic concept, and as such it is unfit to understand Russian foreign policy integrally. It should merely serve as an explanation to western audiences of, often existing and established, strategies employed by non-western countries including Russia in various types of conflicts.

Nevertheless, Russia has and will apply non-linear strategies in their involvement in Ukraine. Ukraine is considered the most important country of Russia's near abroad. After several perceived defeats in former Soviet states and other areas regarded within Russian influence sphere, it seems that Russia drew the line in Crimea. This quick and successful intervention, supported by cyber operations, may have tempted Russian leadership to further cripple Ukraine through support of the Donbass separatists. (Galeotti, 2015) This intervention turned into an actual civil war, and one which proved significantly harder to win. Russian information and influence operations are part of their war effort. Tensions between Russia and the West have risen significantly after the Ukraine crisis, but it has not led to armed conflict. The first part of H 1.1. is thus partially falsified. However, it is true Russia succeeded to avoid armed confrontation with the west with its approach. (Jonsson & Seely, 2015) Although it is impossible to know for certain based on available sources, it is likely that this avoidance strategy was intentional, meaning the second part of H 1.1. is not falsified.

*H 1.2: Russian Intelligence and Security Services use cyber operations as active measures, aiming to subvert and sabotage the USA, and as political espionage, supporting Russia's national security objectives.*

Russia considers itself to be in conflict with the West, although there is no conventional armed conflict between the two blocs. This is the most significant difference between these two cases. Russia's cyber operations are part of the larger concept of information warfare. In line with the Russian definition on IW, these operations aim to impose Russian will on its opponents. NATO and the USA are among the primary threats to Russian national security. An ongoing (ideological) fight over power continues between the USA, NATO, and Russia. Russia's ambition is to challenge American information dominance and to establish a polycentric world order with a larger role for itself. Information warfare is seen as a useful tool of political warfare and espionage that help complete these objectives, while preventing war like confrontations and escalation. H 1.2 is thus not falsified.

However, it is worth mentioning that Russia must balance its actions and aggressiveness in order to prevent provoking western countries both in Ukraine as well as in the USA. It is likely that Russia tailors its cyber operations to an extent, enabling them to be more aggressive and blunt with its cyber operations in Ukraine. In Russian strategic thought however, employing information operations in Ukraine is essentially not different from doing so against the USA. The context and objectives of Russian cyber information warfare *are* different in Ukraine. The existence of such a tailored approach to cyber operations will be further explored in the case studies.

# 3. Case studies: critical infrastructure

## 3.1 Introduction

The following chapters form the empirical core of this research. Several cases of Russian cyber operations in Ukraine and the USA are studied. Every case will be examined using four central questions, followed by a sub conclusion. These central questions are:

1. Technical description: How was the operation executed?
2. Attribution: Was it Russia? Who in particular?
3. Effects: What type of effects did the operations have? For example, technical or political effects. Were the effects intended? Were there any unintended effects?
4. Is there a discrepancy in the effects of the operation in Ukraine and the operation in the United States?
5. Sub conclusion: what factors influenced the different effects, if found?

## 3.2 Ukraine: BlackEnergy3 & CRASHOVERRIDE

In December 2015, a region in Ukraine suffered a blackout for several hours, leaving hundreds of thousands of citizens without electrical power. The effects at the several different power distribution stations would be even more severe and had lasting effects for nearly a year on the regional Ukrainian grid. (Buchanan, 2020, p. 196) This attack became knowns as the BlackEnergy3, named after a piece of malware used in it. Before the Ukrainian grid had fully recovered, a second and more sophisticated cyberattack led to a black out in the Ukrainian capital Kiev, almost exactly a year later. (Buchanan, 2020, pp. 196–200) This attack was nicknamed CRASHOVERRIDE. Both these attacks targeted the Ukrainian power grid successfully, albeit with some significant differences as well.

### 3.2.1. Technical description: BlackEnergy3

In 2015 the attackers used several methods to cause the black out in Western-Ukraine. Firstly, a spear phishing campaign targeting email addresses of the *Oblenergo*[10] employees enabled the attackers to install a piece of malware knows as BlackEnergy3 onto the network. This malware gave the attackers access to the corporate network of the company. The regional power company had wisely separated its industrial control systems (ICS) network from the rest of the

[10] Power distribution stations

corporate network with a firewall. (Buchanan, 2020, p. 195) The attackers used the foothold within the corporate network for reconnaissance, which eventually lead to acquiring administrator credentials for the separated part of the network. In turn this provided them with remote access to the ICS. (US CISA, 2018)

Access to the industrial network allowed the attackers to remotely control so-called breakers, which are automatically controlled electrical switches. These breakers are able to interrupt the current flow, designed to prevent damage to a substation. When the attackers opened up one after the other breaker, they were able to interrupt the flow of power into the grid, ultimately causing the blackout.(Lee, Assante, & Conway, 2016) However, the attack did more than interrupting the current flow at the stations. Other parts of the attack were aimed to amplify the effects caused by opening the breakers.

This was done using a data wiper known as KillDisk, disabling workstations and wiping master boot records[11]. This left the station's staff locked out of their workstations. Furthermore, the attackers modified code that controls a piece of hardware known as a serial to ethernet converter[12], further impeding engineers trying to take back control over the power stations. This caused engineers rushing to the actual substation breakers to restore power locally. In one substation, the attackers modified an uninterruptable power supply (UPS) which left this particular station literally in the dark without its backup power. Finally, the attackers launched a telephone denial of service (TDOS) attack onto one of the power company's customers support centre, which denied access to worried customers and leaving the company unaware of the actual consequences of the blackout. (Buchanan, 2020, p. 194; Lee et al., 2016) The combined efforts of the attack left an estimated 225.000 customers without electrical power for up to six hours.

### 3.2.2. Technical description: CRASHOVERRIDE

In 2016, almost exactly a year later, a second blackout occurred at a transmission station named Ukrenergo near the Ukrainian capital of Kiev. At first sight, this blackout may have seemed less disruptive than the 2015 occurrence since it did not last as long, nor did it affect as many customers. However, the attack was regarded as both more sophisticated in its approach and more alarming to leading cybersecurity experts due to its aim and potentially devastating effects. (Cherepanov & Lipovsky, 2017; Slowik, 2019)

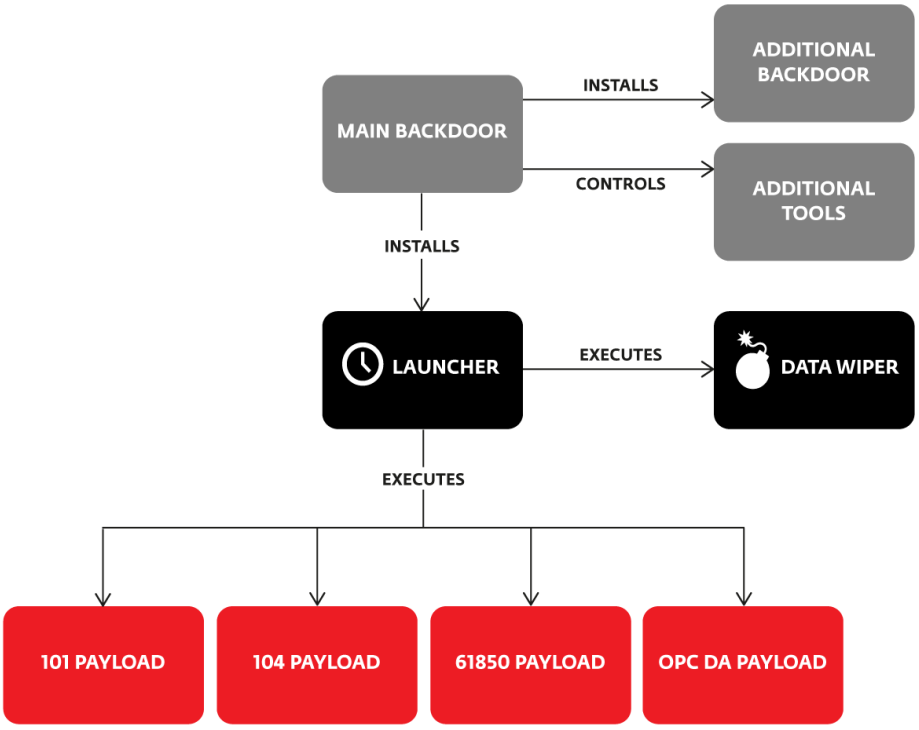
[11] Master boot record is the parts of a (computer's) hard drive which among other thing enables the startup of an operating system. A successful wipe of the MBR causes a failure to boot the computer.
[12] A serial to ethernet converter is typically hardware that enables remote control of a serial industrial device.

The malware used in the 2016 attack was capable of disrupting industrial control systems such as power grids, without hackers 'physically' taking control over parts of the ICS. In order to do so, the attackers had meticulously studied the infrastructure of the Ukrenergo station, building up their knowledge through several previously used espionage tools such as Havex and BlackEnergy2. The initial attack vector was a so-called back door, but no public information is available that further specifies this.

This initial foothold enabled the attackers to control switches and relays at the transmission station, similar to the 2015 attack. (Slowik, 2019) Like BlackEnergy3 (BE3), CRASHOVERRIDE included data wipers too. However, these wipers would automatically search for configuration settings of the ICS and overwrite them, while wiping employees' workstations as well. (Buchanan, 2020, p. 199) For unknown reasons, the attackers chose to deploy the attack solely on the Ukrenergo station.(Lee et al., 2016)

What set this malware apart from BE3 was that it could be used against other critical infrastructure using industry standard communication protocols. This significant difference between BE3 and CRASHOVERRIDE was used to execute four payloads that altered legitimate communication protocols. These protocols communicate between the remote network and the physical parts of the grid such as switches and relays. Worth noting is that the attackers did so without using employees' credentials. (Cherepanov & Lipovsky, 2017) This allowed them to remain more or less undetected, executing malicious code during night shifts for example. The data wiper enabled the attackers to simultaneously disable all monitoring of control systems. Being able to control electrical relays while leaving the engineers unaware of the attack is what made this malware potentially much more destructive. (Cherepanov & Lipovsky, 2017) In any power grid, relays prevent severe damage to a grid when irregularities in the power supply occur. It is very likely that the attackers observed the Ukrainian engineers' response to the 2015 attack, who moved quickly to manual control over the substations in order to restore power. If the engineers would act similarly during this second attack, the disabled relays would have caused severe damage to the entire region's grid. (Slowik, 2019)

In fact, the Ukrenergo staff acted exactly as expected, but no further harm was done to the grid. This may have been due to an error in the code written by the attackers. If this error had not been made and/or the attackers would have chosen to deploy CRASHOVERRIDE to more power distribution stations, it is highly probable the attack would have caused significantly more damage. (Lee et al., 2016; Slowik, 2019) Another suggested explanation for the lack of severe damage, is that the CO malware served as a proof of concept, and some of its functionalities were not executed in the Kiev attack. Such a test could also be used as to signal deterrence to other countries. (Sebenius, 2017)




[13]

### 3.2.3. Attribution

Researchers of private cybersecurity companies have independently attributed the 2015 and 2016 attack to a group named as ELECTRUM, which in turn has been linked to, or seen as part of SANDWORM: a Russian military intelligence (GRU) hacker unit. (Hultquist, 2016; Slowik, 2019) This is based both on public information, as well as additional classified evidence unavailable to this research. Cybersecurity companies FireEye and Dragos argue that the use of distinct versions of the BlackEnergy malware are evidence of Russian involvement, pointing towards earlier use of this malware by SANDWORM to back their claim. (Hultquist, 2016; Slowik, 2019)

Additionally, cybersecurity company ESET found Russian language in both lines of code in the BE malware as well as a Russian language guide in malware that was also used in the CRASHOVERRIDE attack. (Cherepanov, 2016) Although the latter could also be a false flag operation from another actor trying to escape attribution. Hiding behind a different IP address, leaving breadcrumbs

[13] *Figure 1: Schematic overview of CRASHOVERRIDE. Source: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/*

of a certain language, or using a specific type of malware; these are all methods used in cyberattacks to mislead investigators, drawing attention away from the actual culprit. Countries other than Russia use this tactic too. (Goodman, 2010)

In October 2020, the United States Department of Justice in a public statement announced legal charges against six Russian officers affiliated with GRU Unit 74455. This formal indictment included criminal offences such as computer hacking and wire fraud. It explicitly mentioned the BlackEnergy, KillDisk and Industroyer malware as responsible for separate power blackouts in Ukraine. The statement corroborated the research findings of cybersecurity companies with regard to attribution of the Ukraine blackouts, while identifying SANDWORM and Unit 74455 as one and the same.(US Department of Justice, 2020) During the 2015 attack, the TDOS calls were reported to come from Moscow, another indicator of Russian involvement. (Buchanan, 2020, p. 194)

Finally, the attacks and spear phishing campaigns were traced back to a number of command and control servers which were used in other attacks, targeting Ukrainian rail and financial infrastructure as well as the mining industry. (Wilhoit, 2016) This indicates that whoever was behind these attacks, was willing and able to target Ukraine on a large scale. Since it is difficult to attribute these attacks definitively using the limited available technical details, it can be informative to look at other possible explanations of attribution. Using motives and potential gains involved in executing the described operations we now enter the area of informed speculation:

Leaving the fact that two government intelligence agencies and two renowned cybersecurity companies independently attributed these attacks to SANDWORM and Russia's GRU aside, why would an actor capable of these operations conduct them? Given the sophistication of the attacks, not many types of organisations can be held responsible. Criminal incentives seem improbable since these attacks offered no obvious opportunities to create profit. Professional hacker collectives, such as Anonymous, might be able to execute such attacks, but usually claim their attacks. No such claims were made. Consequently, a nation state seems the most probable culprit of such an attack.

The fact that Ukraine and Russia were embroiled in an ongoing conflict over Crimea and the Donbass region cannot be overlooked in this respect. Within this armed conflict, Ukraine and Russia were fighting over energy supply too, both sides were nationalising energy companies in either Crimea or Ukraine that belonged to an adversary. (Buchanan, 2020, p. 203) Russia for instance blamed Ukraine for a particular blackout in the Crimean capital Simferopol as recent as March 2014. (Herszenhorn, 2014) Adding things up, it can be argued with quite some level of confidence that Russia and Russian intelligence in particular were indeed involved.

### 3.2.4. Effects of the operations: BE3

On the surface, the BE3 blackout had the most serious effects on critical infrastructure. As mentioned before, up to 225.000 people lost power anywhere between one to six hours. The attack also left several serial-to-ethernet converters unrepairable, as well as quite a few workstations. Combined, this left the regional power company dealing with the damages for nearly a year. (Buchanan, 2020, p. 196) According to at least two experts, the attackers could have caused much more damage to the Ukrainian grid. (BBC News, 2016; Smith, 2016) A definitive explanation lacks, but a plausible one is that the attackers restrained themselves. Besides the technical effects there were multiple political effects worth mentioning.

Ukraine was quick to blame Russia for the first attack, an understandable move in the light of their ongoing conflict. BE3 showed the willingness and ability of Russia to hack critical infrastructure targets in order to sabotage and subvert Ukraine, especially since this was part of larger cybercampaign that included political and financial targets. (Wilhoit, 2016) However, the story was also given extensive worldwide media coverage as the first cyberattack to cause an actual blackout. Researchers and journalists pointed out that the Ukrainian company was relatively well digitally secured, particularly given the fact that critical infrastructure often is not. (Lee et al., 2016; Zetter, 2016)

Both in the United States and United Kingdom experts warned that this could happen in their home countries too. (BBC News, 2016) Another interesting fact was that the American power grid uses the same serial-to-ethernet converter as those targeted in Ukraine. (Zetter, 2016) This amplified speculations that Russia was now likely able to carry out blackouts in the USA too, although it is not entirely clear whether these converters are very similar in the rest of the world too.

Lastly, the TDOS attack which left customers unable to reach the power company, made little impact on the restart of operations. An explanation could be that it served as the psychological part of the attack, aiming to undermine the image of the national energy company. Considering the reported restraint, the attackers showed, and the interstate conflict background, the attack can be interpreted in many different ways. It could have served as a warning to Ukraine, a retaliation for power cuts in Crimea, a proof of concept for developing cyberattacks to come, or all of the above. The other question that remains is whether all of these effects were intended. This is impossible to determine definitively, and perhaps this is what suits Russia best too. Cyber capabilities can cause harm without evoking escalation. (Lin, 2012) Russia could test its offensive cyber capabilities *and* cause damage to an adversary. Furthermore, they could maintain plausible deniability, avoid provoking western countries,

while still displaying Russian capabilities. Although escalation with Ukraine was likely not a Russian concern, preventing escalation with more powerful adversaries may very well have been: an example of grey zone warfare in practice.

### 3.2.5. Effects of the operations: CRASHOVERRIDE

Similar to BE3, the CRASHOVERRIDE (CO) malware caused a blackout in the northern part of Kiev, if only for about an hour. Although the number of customers affected was smaller, the total power output lost (200MW) in the second blackout exceeded the output loss of all substations in the 2015 attack combined (135MW). (Lee et al., 2016) As mentioned in the technical description, the potential damage in the CO attack could have been far greater. If the CO malware would have been used against more stations, it could have triggered a longer blackout with exceedingly worse consequences. This could have caused backup systems to overload with even more failures as a result.

The different outcomes in technical and systems effects of CO became clear in the aftermath of the attack. The CO attack had very limited lasting effects on the station in Kiev. Furthermore, the attack had lost its potency within an hour. If some parts of the code had worked as researchers at Dragos suspected, causing the relays to malfunction, the damage could have been much more severe. (Slowik, 2019) Arguably the most significant difference was that CO code was more modular than BE3 and therefore applicable to a wide range of industrial control systems. This distinction remains theoretical since it did not make any difference in the actual outcome.

The political effects of the CO attack are perhaps even more complicated. Whether or not the attackers withheld themselves is still an issue of debate but remains a plausible explanation. Was the restraint in their operation a coding failure, or was it intentional? The same could be argued with respect to the chosen singular target, using much wider applicable malware. Another commonly heard explanation is that the Kiev grid may have served as a proof of concept of the CO malware. (Lee, 2017)

An interesting discrepancy appears between this apparent restraint on one hand and the wide ranging cyberattacks aimed at Ukraine over the course of many years on the other. This could indicate that Russia uses Ukraine as a live ‘test facility’ for its arsenal of cyber weapons. Moreover, both explanations for the limited damage in Ukraine can be understood as attacks serving as a warning towards the west and the USA in particular.

## 3.3 USA: Dragonfly 2.0 cyberattacks on critical infrastructure

Between late 2015 and 2017, critical infrastructure targets including power grids located in the United States were attacked by a group identified as Dragonfly 2.0. Among the more than twenty affected targets were nuclear power plants, although these turned out be more resilient to the attacks. Several conventional energy utilities were however penetrated, down to the level of the industrial control systems; a similar feat as the events described in Ukraine. Contrary to the Ukraine cases, none of these attacks caused blackouts. (Symantec, 2017)

### 3.3.1. Technical description Dragonfly 2.0

Dragonfly 2.0 started with reconnaissance of mostly third-party networks with ties to the energy sector, known as staging targets. The attackers collected bits of sensitive information such as technical specifications of the targeted industrial systems. In one example they examined a publicly available picture on a webpage which provided them with the ICS model being used at a particular plant. (US CERT, 2018) The reconnaissance phase provided the necessary knowledge for the attack phase.

The first attack consisted out of a series of (spear) phishing campaigns targeting specific third parties in the energy sector in an attempt to steal legitimate user credentials. Examples given by US CERT include legitimate CV's of technical personnel stolen and then sent by the attackers to incite victims to open malicious attachments. (US CERT, 2018) The toolkit (phishery) used for stealing the credentials was publicly available on the internet at the time. Simultaneously, the attackers used a watering hole attack to collect network credentials from energy sector employees as well as trusted third parties. Such an attack compromises websites which are known (or suspected) to be used by a targeted victim, in order to gather network credentials. (Symantec, 2017)

Armed with legitimate credentials and knowledge of the network's structure, the attackers build a back door into the networks of the third parties giving them remote access and allowing them to create local administrator accounts. The attackers could now install both software and malware on third party servers which, by then, were compromised sufficiently to serve as command-and-control servers in the attack on the intended final targets. These servers now contained compromised services,[14] that provided access to the networks of the energy companies. (US CERT, 2018)

[14] The compromised services included a Virtual Private Network (VPN), a remote desktop protocol (RDP) and the Outlook Web Access mail client. (US CERT, 2018)

Continuing with a second reconnaissance phase on the final target's internal network, the attackers gained access to the domain controllers[15] of several targeted networks. This allowed them to view ICS data output and configuration profiles to access the ICS network. They could now access the ICS and SCADA[16] systems of several electrical utilities. Similar to the intrusions in Ukraine the attackers could now interrupt the current flow, through control over equipment such as breakers. After compromising the ICS the attackers tried to cover their tracks by deleting log files and registration of remote access connections they had used in the attacks, although authorities nevertheless succeeded in recovering these files afterwards. (US CERT, 2018) A crucial difference between Dragonfly and the Ukraine case was that the attack stopped short of 'flipping the switch': now power loss or blackouts have been reported in the aftermath of this attack. (Greenberg, 2017)

### 3.3.2. Attribution

The United States government CERT and the domestic intelligence agency FBI[17] released a joint technical report in 2018 where they publicly attributed the Dragonfly 2.0 case to the Russian government. No specific evidence was given to back this claim up, although the report provided great detail in the methods used by the attackers. (US CERT, 2018) It is likely that these agencies had more concrete evidence, ungrounded allegations would make a court case impossible. A plausible explanation for non-disclosure could be to prevent compromising their (technical) sources, safeguarding future collection on Russian APTs. This is something many intelligence agencies tend to do. (Buchanan, 2020, pp. 70–76) Statements made by NSA[18] officials allegedly accuse Russian agencies as well. (Nakashima, 2017)

Earlier attacks on energy infrastructure by a group known as Dragonfly occurred around 2014. Both the *modus operandi* and recognized indicators of compromise were linked to Russian APTs 28 and 29, according to the US intelligence community. When working together these APTs are nicknamed Grizzly Steppe. (DHS & FBI, 2016) Although Dragonfly (likely GRU & SVR) and Dragonfly 2.0 (likely FSB) are generally seen as two distinct groups, they used similar methods and two exact same pieces of malware, suggesting a certain link between the two groups, and therefore with Russia. (Greenberg, 2017)

[15] Domain controllers are mainly used for security, including the authentication of users accessing domain resources. (Red Hat, 2020)
[16] Supervisory Control and Data Acquisition; a type of ICS usually including a graphic user interphase to monitor and control industrial installations.
[17] Federal Bureau of Investigation
[18] National Security Agency; America's foremost signals intelligence agency.

The Russian intelligence community is known to compete amongst each other over matters like funds and areas of responsibility. (Galeotti, 2016b)

Follow up intrusions in other countries attributed to Dragonfly 2.0 strengthen the American claims. Germany's domestic security service declared in 2018 that highly likely Russian security service FSB, through Dragonfly 2.0 (Berserk Bear) had attacked energy companies in Germany, only succeeding to breach their corporate network. (REUTERS, 2018) In 2020, a classified report of the German foreign intelligence agency sent to industry cybersecurity officials attributed ongoing critical infrastructure intrusions in Germany to Dragonfly 2.0, again also identified as Berserk Bear. (Lyngaas, 2020a)

Besides governmental institutions, some private cybersecurity companies have tracked Russian APT's including Berserk Bear over time, resulting in another link between the Russian government associated groups and attacks on critical infrastructure. (Crowdstrike, 2020; CrowdStrike, 2013) The initial report from Symantec noted that the attackers used several tools which were available on platforms such as GitHub, and the intrusions did not involve the use of zero days. This could have been an attempt to prevent attribution. The report did find strings of code written in Russian, although this provides very little certainty. (Symantec, 2017)

The attributions to the group dubbed as Dragonfly 2.0 regarding the attacks on US energy sector provide little publicly available technical or forensic evidence, making it again hard to be absolutely certain of Russian state involvement. However, as with the BlackEnergy case, again there are several reputable and independent sources that attribute these intrusions to Russian APTs with high confidence. The number of sources linking Dragonfly 2.0 to Russian government agencies, such as the FSB, is significant. One could argue as well that the pattern of these attacks seems to be coherent with one another, although with differing success.

### 3.3.3. Effects of the operations

A number of government investigations were conducted in between and after the various reported incidents that were attributed to Dragonfly 2.0. The United States Computer Emergency Response Team (US CERT) identified several vulnerabilities in the software and security architecture of the affected companies as well as the involved third parties. The attackers succeeded in penetrating all the way down to the ICS level, so the potential consequences could have been similar to what happened in Ukraine in 2015 and 2016; provided the attackers would have proceeded with the attack. The fact that they chose not to proceed with the attack is crucial in this respect.

A part of the vulnerabilities found in the energy sector stem from legacy systems, which were never designed with (digital) security in mind. Most of the legacy (operating) systems used in critical infrastructure are no longer supported and patched for vulnerabilities. But simple preventive measures, which are becoming standard cybersecurity principles, and are featured in common email clients or cloud storage services, were lacking in these companies' networks. Examples given by private parties were; two factor authentication of user credentials, enforcing minimum password requirement policies, encrypting network stored data and updating anti-virus suites regularly. (Symantec, 2017) US CERT gave an even more extensive advice on best practices protecting against campaigns such as Dragonfly executed. Proper segmentation, better monitoring of remote access sessions, monitoring of email accounts registered, to name a few.

A second effect of this operations was that it once again reminded the US and other western countries just how vulnerable their critical infrastructure is and how much there is to improve on securing it. The story was relatively well covered by the media, which served to amplify this notion.

The given advice should therefore be implemented beyond the energy sector as well, to better secure other critical infrastructure. The wider disruption of critical infrastructure in Ukraine has shown that this is an issue that transcends the energy sector. Industrial control systems managing other critical infrastructure are at risk in the United States too. Especially since experts have noted that the network security in Ukraine was on par with or better than in the USA, and similar hardware is found in both countries. Attackers can exploit similar vulnerabilities identified in the Dragonfly 2.0 case to this end. When several critical infrastructure systems are affected simultaneously and fail, it can create a cascading effect with far reaching consequences. (Desouza, Ahmad, Naseer, & Sharma, 2020)

This warning created a political effect related to the discussion on cyberwar and its thresholds. The US, itself no stranger to cyber enabled espionage and sabotage, was targeted with some level of success by one of its oldest adversaries. The fact that Russia did not 'flip the switch', causing a blackout in the United States, may well have been caused by a fear of cascading cyber operations. However, this *cybersecurity dilemma* is a separate field of study which lies outside the focus of this research.

Perhaps Russia was signalling to the United States what they are capable of in cyberspace as means of deterring. Both states have been embroiled for decades in an ongoing espionage and sabotage cat and mouse game. The US has had reconnaissance probes installed on Russian energy sector control systems since 2012. (David E. Sanger & Perlroth, 2019) Given the proven sophistication of the US Cyber Command and the NSA, it is not unlikely that the US is or was able

to disrupt critical infrastructure in Russia too. The operations in the US could have served as an intentional warning from Russia showcasing that they too are 'a mere snap away' from inflicting actual damage.

An interesting point against this goal of signalling through cyber espionage and sabotage is put forward by Buchanan. Cyber operations are unfit for the task of signalling, because the exposure of a state's cyber capability often makes that very capability ineffective. (Buchanan, 2020, pp. 307–312) Let us explore this for a moment.

If Russia wanted to warn the United States that it could disrupt its energy sector, the US would have to notice the warning for it to work. When noticed, the intrusion serving as a warning would certainly be thoroughly investigated, as was the case for the Dragonfly 2.0 intrusions. The modus operandi of the Russian intrusion would be compromised, and the exploited vulnerabilities would be patched, making it harder to repeat and damaging the credibility of the deterrence. In a worst-case scenario, it could also negatively affect other Russian cyber capabilities using similar techniques and/or vulnerabilities.

Besides, Russia's cyber sabotage operations in Ukraine already sent a message of warning to the West, whether this was intentional or not. Given the risks involved of repeating this course of action in the US, this may seem irrational. Although perhaps they wanted the warning to be very credible indeed. Signalling therefore seems a less likely explanation.

Ultimately, it could have been an espionage and/or training operation which was fortunately discovered by cybersecurity professionals. Some of the tools used were publicly available, which eliminates the risk of compromising one's capabilities and tailor-made tools. Other techniques had been applied in previous operations as well. Similar activities attributed to Dragonfly were reported in Turkey and Switzerland as well, indicating this could all be part of a wide ranging reconnaissance operation. (Symantec, 2017)

## 3.4 Discrepancies

The most straightforward difference in the Russian operation in Ukraine and the United States is the fact that in the US, no blackouts had occurred. According to several cybersecurity companies and reputable journalists, the dominant explanation is that Russian hackers showed restraint against the US energy sector. Another difference between both BlackEnergy and DRAGONFLY on the one hand and CO on the other was the wider applicability and operator independent functioning of the latter. The CO malware was more sophisticated and likely a further developed version of BlackEnergy, though based on its predecessor's proven effectiveness. A year had passed since ELECTRUM had

shut down the stations in western Ukraine, and it seems Russia learnt from it. This is also reflected in the CO payload which was likely developed based on observed reactions from Ukrainian staff after the first attacks in 2015. Assuming that these operations were conducted by two different intelligence agencies, this slightly complicates the comparison between the BE3 and CO attacks with the Dragonfly case.

## 3.5 Sub conclusion

Our second sub research question was:

**2. Which factors influence the different effects of Russian cyberattacks on the power grid in Ukraine compared to similar operations in the USA?**

The accompanying hypotheses were:

*H 2.1 Russia's cyberattacks in Ukraine are dependent on the factors; technical 'home-field advantage', societal knowledge and a conflict scenario, which are absent in the USA.*

A technical 'home-field advantage' was present in the fact that much of the infrastructure used in Ukraine originates from the Soviet era, which is advantageous for Russian hackers who know these systems well. The conflict scenario was too very likely a factor in these attacks. First, the Russian attacks spanned much wider than just the power grid and included attacks on the railway, television, mining and government sectors, indicative of a larger conflict between the two. Second, Ukraine and Russia were fighting over energy supply in particular too, with power cuts being used as a coercive tool by both sides. Evidence against this hypothesis is that Russia succeeded to compromise the US grid without any home-field advantage, although they did not actually cut the power as discussed. Neither is there any evidence suggesting that societal knowledge played a part in these operations. The factors home-field advantage and societal knowledge are therefore considered falsified. The conflict scenario factor is not considered falsified.

*H 2.2 Russian cyberattacks in the USA are deliberately designed to avoid extensive damage, considering the superior power of the USA in conventional and cyber warfare.*

The operations in Ukraine did inflict damage on the power grid and caused blackouts, whereas in the United States they did not. Considering Russia had compromised the US grid similarly down to the ICS level this was likely not a matter of ability, supporting H 2.2. Whether Russia was willing to disrupt the US power grid at the time remains a matter of debate, but this chapter has argued that they were in fact not willing to cross that line. Further support for hypothesis

3.2 can be found in the fact that Russia used the same malware against other states such as Turkey and Switzerland. No blackouts were reported as a result of these attacks either, while both attacks in Ukraine did inflict damage. It can also be argued that this restraint is evidence of Russian consideration for the US military and cyber superiority, although Russia will probably never admit it.

Arguing against this hypothesis is that BE3 and CO were likely the responsibility of the GRU, while Dragonfly is likely FSB. The GRU is known to be aggressive and its operations have escalated before, notably in the NotPetya incident. FSB cyberattacks do not share the same infamy. The next chapter will also show that the GRU does not hesitate to target the USA with information operations either. Another countering argument could be the coding error in the CO attack. If it was not an unintended error, it means Russia deliberately avoided extensive damage in Ukraine too. But then again, attacks on other Ukrainian infrastructure were still disruptive. Therefore, hypothesis 3.2 is not considered to be falsified.

*H 2.3 Russia tests cyberattacks in Ukraine which can then be regarded as operational for potential use against countries such as the USA.*

Both the Ukraine and US operation can be attributed to Russian intelligence with high confidence. Exactly why Russia did it is impossible to know except in the unlikely scenario where for example Kremlin officials will state this explicitly. Evidence that supports this hypothesis includes: in all three cases covered in this chapter some level of restraint on behalf of Russia remains a plausible explanation for the relatively limited damage inflicted. The malware was adjusted after initial execution and observation of Ukraine's response, to then be executed again, which may indicate a trial phase. Moreover, the CO malware was applicable to a larger set of critical infrastructure but not applied as such. The chronological order of the attacks permits the theory that the Ukraine attacks could have served as a study for Dragonfly 2.0, although these were two separate agencies. The fact that Berserk Bear used the same attacks against Turkey and Switzerland makes matters more complicated. It is possible that Ukraine served as a test site for these countries too. Even if this was not the case, H 2.3 is not falsified by this or any of the other findings.

Thus, we can conclude that Russian cyberattacks on the power grid in Ukraine are intentionally causing damage, whereas in the USA they are not. The conflict scenario between Russia and Ukraine and the risks involved with such disruptions in the USA are contributing factors in this matter. Finally, it seems plausible that Russia uses the opportunity it has to test cyber weapons functionalities in Ukraine.

# 4. Case studies: digital information operations

## 4.1 Ukraine: 2014 & 2019 presidential election interferences

Both and 2014 and in 2019, attempts to meddle with the Ukrainian elections were reported. Both elections took place in tumultuous circumstances. In 2014 the elections were held shortly after the Ukrainian revolution, also known as the Euromaidan revolution. The revolution escalated into civil war and to make matters worse, Russia annexed the Crimean Peninsula just days later. Both conflicts are currently unresolved.

### 4.1.1. Technical description: 2014 elections

As stated before, the 2014 elections followed the Euromaidan revolution, after which incumbent president Yanukovych fled to Russia. The elections are organised by the Central Election Commission (CEC), using paper ballots and digital monitoring systems. On the 21st of May 2014, the CEC was attacked by hackers targeting parts of voting monitoring system, resulting in flawed vote monitoring for almost twenty hours. (Baezner & Robin, 2018) The attackers, who nicknamed themselves CyberBerkut, boasted they had destroyed the tallying system and leaked emails to back their claims. The Ukrainian government responded quickly by restoring all data and services a day later. (Rid, 2020a)

On election day, minutes before the polls would close, the attackers placed a forged result on the CEC server, falsely stating that far right candidate Dmitry Yarosh had won the election. The CEC had set up mirrors of its website, causing the false results not being visible on the public website of the CEC. However, CyberBerkut had leaked the forged results to Russian media, who immediately picked up the story. (Rid, 2020a) Non-CEC websites related to the 2014 elections were successfully targeted as well. The morning after election day, the CEC website was struck by a Distributed Denial of Service Attack (DDoS)[19], further delaying the actual results of the election. (Clayton, 2014)

Furthermore, Ukrainian CERT reported they had identified espionage malware on the CEC network, but had successfully mitigated the threat. (Koval, 2015) This attack was again claimed by the group identified as CyberBerkut.[20] (Baezner & Robin, 2018) According to the Ukrainian CERT head of

[19] DDoS attacks are blunt instruments which aim to launch large amounts of data (requests) to a server, causing it slow down or crash.
[20] Berkut was the name for the Ukrainian riot police, which was deployed to suppress the Euromaidan protests during president Yanukovych tenure. The unit was dissolved after the revolution due to its violent reputation.

investigation, the attack was both sophisticated and well planned, initial reconnaissance had taken place since at least March 2014. Allegedly, the attackers had gained administrator level access to the CEC network. (Koval, 2015)

Three months later, the parliamentary elections would take place in Ukraine. Again, attackers targeted CEC website with a DDoS attack. The attack slowed the CEC website down but did not cause a crash. Both the May and October attacks were unable to change any voter data held by the CEC, the CEC used paper ballots and manual counting to determine the outcome. Furthermore, the attackers did not gain access to the votes registration part of the network. (Marks, 2014)

Besides the attempts to interrupt the services of the CEC, several other efforts seemingly aimed to deface the Ukrainian government and its officials were reported over the course of 2014. These efforts included:

- Sabotaging fibre optic cables in the Crimean Peninsula, cutting official communications with the mainland short. This happened during the Russian annexation of Crimea.
- Disabling access to- and altering data on-, Ukrainian government websites.
- Smear campaigns against individual politicians.
- Telephone Denial of Service attacks against Ukrainian members of parliament. (Weedon, 2015)

### 4.1.2. Attribution

As mentioned, the group CyberBerkut publicly claimed responsibility of the attacks on the CEC website. The initial assessment of cybersecurity researchers and academia was that CyberBerkut was likely a pro-Russian hacktivist group based in Ukraine. In its public statements, the group had mimicked the symbols and language of infamous hacktivist collective Anonymous. Ukrainian CERT assessed that due to the sophistication of the attack and the presence of espionage malware linked to Russia, these hacktivist had to be state sponsored. (Koval, 2015)

CyberBerkut is a reference to the Ukrainian riot police (Berkut) which was involved in the violent suppression of the Euromaidan protests of February 2014. Likely the group tried to signal they were Ukrainian through naming themselves as such. (Jensen, Valeriano, & Maness, 2019) More thorough investigation later led to a different assessment: CyberBerkut was likely a Russian state sponsored group tied to the Russian government. (Jensen et al., 2019)

Rid takes this assessment even further, claiming CyberBerkut was a front operation of Russia's military intelligence agency GRU. (Rid, 2020a) This claim is backed up by forensics which reveal the usage of the same shortened URL's associated with APT28, or GRU Unit 26165. Citizen lab also found strong commonalities in the domains set up by APT28 and CyberBerkut for different operations, suggesting a link between the two. (Hulcoop, Scott-Railton, Tanchak, Brooks, & Deibert, 2017) The United Kingdom's National Cybersecurity Centre stated with 'high confidence' that the GRU was behind the moniker CyberBerkut.(UK NCSC, 2018) Finally, a study by Stanford university revealed several references to GRU cyber operations outside of Ukraine in social media content disseminated by CyberBerkut. (Diresta & Grossman, 2019)

The group claimed responsibility or was seen as the culprit of other attacks too, both in Ukraine and in the rest of the world. Among the Events tied to CyberBerkut are:

- An attack on a large Ukrainian bank, which had suspended its services in the separatist regions of Donetsk and Luhansk. (The Moscow Times, 2014)
- The targeting of several NATO websites. (Jensen et al., 2019)
- The placement Holocaust related defacement material on Polish websites including the stock exchange. (Jensen et al., 2019)
- Attacks in 2015 on German government websites. (Trend Micro, 2015)
- Hack and leak operations aimed to discredit journalist David Satter, a known critic of the Russian government. Worth noting is that it applied a phishing technique that matched the John Podesta phishing operation exactly. (Hulcoop et al., 2017)
- Hack and (tainted)[21] leak operations against George Soros' Open Society Foundation (OSF). (Hulcoop et al., 2017)

A well trained and funded hacktivist group could have been able to target the CEC servers as observed in this case. However, other attacks attributed to CyberBerkut fit poorly into the narrative of being a Ukrainian nationalist hacktivist group, such as the attack against Poland. Considering that several operations were leaked proactively to Russian media; strong similarities were found in the methodology applied by APT28 and CyberBerkut and multiple sources tying CyberBerkut to the Russian government and the GRU in particular;

[21] The Citizen Lab has named operations in which stolen data or communication is altered before it is leaked 'tainted' leaks. OSF has been formally declared an undesirable organisation by the Russian government.

it is no leap of faith to state that the interference was a Russian false flag operation.[22]

### 4.1.3. Technical description: 2019 presidential elections

The 2019 presidential elections in Ukraine were again targeted by disinformation and digital fraud. According to a statement from a high-ranking Ukrainian cyber police official, the attacks consisted of phishing emails and malicious software updates seeking to harvest credentials from government officials. As such it started months before the elections would take place in March and April. The same source reported that the attackers tried to buy sensitive information on the dark web related to election officials, using cryptocurrency. (Reuters, 2019) The US Director of National Intelligence, in its annual threat assessment, added that Russia was proactively trying to influence these elections through exploitation of cyber vulnerabilities and other information operations: *"Hoping to remove Petro Poroshenko from top office in Ukraine and aiming to bring to power a less anti-Russian parliament"* (Director of National Intelligence, 2019) However, other than in 2014 no intrusions onto the CEC networks were reported.

Besides the efforts aiming to gain access to election officials' personal files and government computer networks, other active measures including disinformation were employed in Ukraine. Social media companies such as Facebook and Twitter had increased their monitoring and detection capabilities following disinformation operations in the US elections. Disinformation spread by suspicious IP addresses and coming from foreign countries would likely be detected and flagged. Facebook alone reportedly took down more than 100 accounts and almost 2000 pages, used to impersonate candidates and spread disinformation. Presidential candidates mobilised their constituencies to help identify imposter accounts, overflowing them with messages of support for the candidate. The perpetrators tried to circumvent security measures by using proxies in Ukraine who were offered payment for the use of their social media accounts. (Schwirtz & Frenkel, 2019)

Partly due to this new strategy of hiring citizens instead of using forged accounts, plenty of disinformation was successfully spread. An interesting example involved a Telegram account posing as an employee of the Ukrainian national security service (SBU). This 'mole' claimed he leaked inside information from the service. It included stories claiming the SBU was secretly plotting to keep incumbent president Poroshenko in power in spite of his unpopularity. To this end, it posted several unverifiable statements. On such message included vague

[22] False Flag operation: when an attacker tries to shield their true identity or origin by putting the blame on a forged or real third party.

pictures of ‘instructions’ handed out to SBU to use violence against protests aimed at Poroshenko. These messages were then amplified by other social media accounts involved in the spread of disinformation. (DFR Lab, 2019)

A Kiev based non-governmental fact checking organisation pointed to Russian television talk shows and news channels as the most successful spreaders of disinformation. These media also reach an estimated 1.4 million Ukrainian citizens, predominantly in the separatist regions of Donetsk and Luhansk. In a survey of three of these channels they registered several baseless and/or partially biased claims in 18 broadcasts dedicated to the Ukrainian elections. (StopFake, 2019) These are depicted in the table below:

| Message | Number of programs in which the message was mentioned |
|---|---|
| Ukraine is under the external control of the West | 18/18 |
| Ukrainian authorities rig presidential elections | 10/18 |
| There is a civil war in Ukraine | 10/18 |
| Nazism flourishes in Ukraine | 8/18 |
| Ukrainian authorities are preparing provocations for the period of the elections | 8/18 |
| A repressive regime has been established in Ukraine | 6/18 |
| Some Ukrainians are trying to impose their ideology on others | 6/18 |
| The nation of Russophobes is being brought up in Ukraine | 6/18 |
| The results of the elections showed that Ukraine is split | 5/18 |
| Ukrainian authorities are ready to kill opponents | 5/18 |

[23]

### 4.1.4. Attribution

The head of Ukrainian cyber police was quoted saying it was ‘likely’ that Russia was behind the phishing attacks targeting Ukrainian election officials, though no evidence was given to support this. (Reuters, 2019) The US Director of National Intelligence gave a similar assessment, but as is often the case with intelligence agencies, no further specifications were given here either. The head of Ukraine’s foreign intelligence service stated that the Russian government had allocated $350 million just for operations regarding the 2019 elections. These operations had the goal to prevent Poroshenko from being re-elected. (UNIAN, 2019) That same president Poroshenko went public to state that the Russian government was behind two different DDoS attacks targeting the CEC website in February 2019. (Lyngaas, 2019)

[23] Figure 6: Overview of claims made by three Russian news outlets (Channel One and Russia 1) with regard to the presidential elections in Ukraine. (StopFake, 2019)

Concerning the disinformation efforts, again Ukrainian SBU pointed towards the Saint Petersburg based Internet Research Agency, which will be covered in the next paragraph. (UNIAN, 2019) Furthermore, they assessed that it was Russian intelligence who had approached Ukrainian citizens to lend their social media accounts in exchange for money. (Schwirtz & Frenkel, 2019) Observers working for the Canadian government revealed that there were significant spikes in the creation of bot-controlled Russian language Twitter accounts during the 2014 Ukrainian election, during the first days after the MH-17 aircraft crash and during the 2019 Ukrainian elections. (Rapid Response Mechanism Canada, 2019) Facebook reported that it had removed accounts that "originated in Russia" which "*created fictitious personas, impersonated deceased Ukrainian journalists, and engaged in fake engagement tactics. They also operated fake accounts to increase the popularity of their content, deceive people about their location, and to drive people to off-platform websites"* The advertisement space bought by these account were paid for in Russian Rubles. (Facebook, 2019)

None of the above provide any definite proof nor absolute certainty. This means it is hard to identify Russian government agencies responsible for any of it. Some of the sources might have benefited politically, making attribution in this particular case slightly more speculative. However, the efforts made were well aligned with Russian interests in Ukraine. This is especially true for the efforts hindering the re-election of Poroshenko, who took a firm stand against Russia during his presidency. Then there is plenty of circumstantial evidence pointing towards Russia and Russian intelligence. Finally, the observed methods and targets are also similar to what would be observed in the United States election interference in 2016 as well as the 2014 Ukrainian elections. Both these instances provide much more reliable and concrete evidence of Russian involvement. Altogether, it is hard to maintain that Russia, still engaged in a bitter conflict with Ukraine, had nothing to do with this election interference whatsoever.

### 4.1.5. Effects of the operations

Both the 2014 and the 2019 presidential elections elected presidents which were not the candidates that Russia supported with their information operations. In the 2014 election, candidate Poroshenko, who had supported the Euromaidan revolution, won 54% of the votes. CyberBerkut's claim that far right candidate Yarosh had won the election was therefore far from credible: he gained 0,7% of the votes. Another effect of the operation was that Ukraine immediately accused Russia. This claim was then gradually supported by other states, journalists, and non-governmental organisations. Therefore, the operation was likely to strengthen anti-Russian sentiments in Ukraine and other European countries.

Studies have found that the Russian information campaign prior to the 2014 elections did influence Ukrainian voters. It concluded that the pro-Russian population's attitude towards Russia benefitted from the campaign. However, on the pro-Western population it had no such effect, which means it primarily led to further polarisation of the Ukrainian society. (Peisakhin & Rozenas, 2018) Another contributing fact in this respect is that people living in the Donbass and Crimea regions are generally isolated from information that is not controlled by Russia, whereas people in Western Ukraine have little to no access to Russian information. (Baezner & Robin, 2018)

The intended effects were likely to damage the trust in the Ukrainian government and the elections in general rather than having a significant influence on the outcome of the elections. This is part of ongoing Russian efforts to destabilise Ukraine and delegitimise its government. This campaign was successful for certain target audiences, notably people in pro-Russian regions. (Jensen et al., 2019)

In 2019, Russian efforts tried to prevent the re-election of Poroshenko, according to the US intelligence community. Poroshenko's challenger Zelensky eventually won the election with more than 70% of the votes. There is no evidence that Russian information operations influenced the results in any significant way. The landslide victory of former professional comedian Zelensky was likely due to a very successful media campaign, which articulated the fact that he was anything but a corrupt career politician. (Dosenko, Gerachkovska, Shevchenko, & Bessarab, 2019)

Although Russia had not been able to influence the outcome in 2014, it tried to interfere again in 2019. Perhaps they had regained confidence after the partial success of the 2016 US elections. However, it is more likely the interference was again part of the combined Russian efforts to subvert Ukraine by any means available and further fuel social polarisation.

## 4.2 USA: 2016 presidential election interference

In the run up to the 2016 United States presidential elections, a number of confidential emails were leaked on the website DC leaks. These emails exposed a bias in the democratic party favouring presidential candidate Hillary Clinton over Bernie Sanders. The stolen emails were then leaked by a hacker group at the time known as Guccifer 2.0. Investigations later indicated that Russia was likely responsible for this hack and leak operation, adding that Russian President Putin ordered the operation.(DHS, 2016) By discrediting the primary democratic candidate, Russia aimed to influence the elections. (Mueller, 2019; Office of the D.N.I., 2017)

### 4.2.1. Technical description & subsequent leaks

In March 2016, Russian military units started a spear phishing campaign against dozens of employees working for the Clinton candidacy, the Democratic National Convention (DNC) and Democratic Congressional Campaign Committee (DCCC). Official and private email accounts of staff members working for the presidential candidate were compromised. One of the victims was Clinton's campaign leader John Podesta. The hackers extracted campaign related communication and user credentials from their victims, which granted them access to the DCCC network. Once on the DCCC network, they collected administrator credentials, compromising more than 20 different computers. In both instances they used a credential harvesting tool known as *Mimikatz*.[24] (Mueller, 2019)

The credentials enabled them to traverse from the DCCC to the DNC network using a VPN connection between the two. Between April and June, they continued to compromise the DNC network. Using malware knowns as X-Tunnel, the attackers could transfer large amounts of data back to their 'own' control servers, which were leased from a commercial party in Arizona. Another malware known as X-agent, enabled the attackers to log keystrokes and take screenshots, capturing both sensitive business and personal information from DNC and DCCC employees during business hours. These combined efforts allowed the intruders to collect thousands of documents and emails from the Democratic party, which were secured on their leased servers. (Mueller, 2019; Rid, 2020a)

[24] Mimikatz was a tool that was created by a French programmer. The Russians allegedly tried to physically steal the source code, but failed. It was then published online and has been used in infamous hacking operations such as NotPetya and BadRabbit targeting Ukraine.

The next step was to leak large amounts of information without compromising the source. For this step, the attackers had registered the domain DCleaks.com anonymously through a commercial service which they paid for in bitcoins. These bitcoins were mined by the computing resources of the attackers. The documents and emails were neatly sorted, and the timing of their release was tightly controlled. The first leaks occurred around early June 2016, which were then promoted via social media accounts registered by the hackers under the alias DCLeaks. In addition, email accounts were opened to communicate with journalists. Some were given early access by DCLeaks to documents that were password protected. Meanwhile, the DNC had hired a private cybersecurity company to investigate the intrusions. Within two weeks of the first leaks, the DNC disclosed they had been compromised by Russian state-sponsored hackers identified as 'Fancy Bear'. (Mueller, 2019)

The response to the DNC disclosure did not take long; a blog was created on WordPress under the moniker Guccifer 2.0. The author, a self-proclaimed Romanian hacker, claimed to be responsible for the leaks and began to publish new stolen documents from the DNC. Additionally, it provided exclusive access to parts of the DCLeaks website to individual journalists and even provided information to a republican candidate for congress regarding his democratic opponent. This indicated that the author of the Guccifer 2.0 blog at least had access to the DCleaks documents, as he claimed. (Rid, 2020a)

The stolen documents were shared with an independent third party as well: Julian Assange's WikiLeaks. Staff working for DCLeaks contacted WikiLeaks in order to synchronise the joint release of new stolen documents. Near simultaneously, WikiLeaks staff contacted Guccifer 2.0 offering to help disseminate future leaked materials. According to WikiLeaks staff this would increase the impact of the Guccifer revelations. The hackers behind Guccifer 2.0 accepted, sharing communication from campaign leader John Podesta with WikiLeaks through encrypted online archives. Wikileaks subsequently released tens of thousands of emails and document via their channels three days before the National Convention would take place. (Mueller, 2019) The involvement of WikiLeaks did in fact increase the impact of the leaked documents. The DCLeaks initially did not receive a lot of attention, but this changed when WikiLeaks got involved and some of the files were altered by the hackers to give them a fictive classification. (Rid, 2020a)

The efforts of the attackers did not focus solely on the Democratic Party and its presidential candidate. Several election administration related organisations and individuals were targeted, as well as companies providing soft- and hardware used in electronic polling stations. In one instance they successfully installed malware on the network of such a private company.

According to an investigation led by the FBI, this allowed the attackers to delete casted votes in the state of Illinois. However, there was no evidence that the attacker deleted any votes. (D. Sanger & Edmondson, 2019)

### 4.2.2. Social media troll campaign

The interference in the elections actually started nearly two years before the first intrusions into the DNC network were noticed. As early as 2014, a Russian private institution known as the Internet Research Agency (IRA) started a social media campaign in the United States. The IRA employed social media profiles of fictitious US citizens, also known as trolls. These trolls are created to actively comment on all sorts of political issues in both the English and Russian language on platforms such as Twitter and Facebook. (Jamieson, 2020) The IRA aimed to be a secretive organization. Working industriously in 12 hour shifts to produce large amounts of forged content, it became known as a troll farm or factory. (Rid, 2020a)

The IRA troll farm is an example of contemporary active measures, which aims to influence (interstate) political affairs. It is estimated that IRA could reach millions of American citizens on divisive political matters. In order to do so they sent out millions of tweets, tens of thousands of Facebook messages and created more than 1100 YouTube videos filled with disinformation and other content aiming to influence the debate. Additionally, legitimate political advertisement space was bought to disseminate their message and fake organisational accounts were set up, mimicking actual political organisations. (Howard, Ganesh, Liotsiou, Kelly, & François, 2018)

These efforts had several goals; to discredit the Democratic candidate Clinton, to boost the campaign of candidate Trump and to increase domestic tensions and polarisation in the US. (Mueller, 2019) The amount of disinformation spread was significant. An open source analysis showed that disinformation spread in the final months of the election campaign outperformed the Facebook engagement of 19 large media outlets combined.(Silverman, 2016) The table below indicates this engagement.

**Table 2: The Total Audience Engagement with Facebook Posts, by Year**

| Year | Shares | Likes | Emoji Reactions | Comments |
|---|---|---|---|---|
| 2015 | 1,388,390 | 2,104,487 | 478 | 131,082 |
| 2016 | 12,861,314 | 15,077,235 | 1,698,646 | 1,322,342 |
| 2017 | 16,714,594 | 21,644,714 | 3,695,278 | 2,001,882 |
| *Total* | *30,964,298* | *38,826,436* | *5,394,402* | *3,455,306* |

[25]

The trolls repeated narratives of republicans such as candidate Trump, who referred to candidate Clinton as "crooked Hillary" and suggesting Clinton should be imprisoned. However, the trolls took the derogatory narrative much further, using terms such as "Killary" and "Hitlery". Furthermore, the trolls focused on the suggestive consequences of the election of candidate Clinton, such as increased taxes, near limitless immigration, gun banning legislation, increased terrorist threats and economic depression. Simultaneously, the trolls would spread the narrative which endorsed the policies and views of candidate Trump. These efforts again focused on matters such as the perceived loss of the American identity, the threat of mass immigration towards American culture and the deteriorated economic perspective of white working-class Americans. These were among the main issues that candidate Trump focused on during his campaign. (Jamieson, 2020)

IRA trolls targeted left wing audiences too, with topics such as the Black Lives Matter movement and Hashtags #PoliceBrutality. This activity was nearly on par with the conservative narrative until some months before the elections, when conservative narratives peaked. Through this double edged sword they again tried to deepen the divide between liberal and conservative American audiences. (Howard et al., 2018)

### 4.2.3. Attribution

One of the first reports that attributed the DNC campaign to Russia was drafted by the three intelligence agencies in the US: CIA, FBI, and NSA. In their joint report they concluded with high confidence (CIA and FBI) that Russian President Putin himself had ordered the interference campaign. Furthermore, the assessment was that Russia preferred presidential candidate Trump over Clinton, directing their efforts to help candidate Trump win the election. (Office of the D.N.I., 2017)

[25] Figure 5: Shows the Facebook engagement that the IRA caused with their troll campaign. (Howard et al., 2018)

The unclassified report provided little (technical) evidence, referring to the classified version. None of the members of congress who had seen the classified report, neither Republican nor Democrat, questioned its conclusions that Russia was responsible. This is important, since president Trump initially rejected the conclusions even though he was informed on the contents of the classified report. (Jamieson, 2020) Later, President Trump did admit Russia was involved. Even President Putin did not deny that Russians had interfered in the elections two years after the events occurred. However he did deny the government had anything to do with it and pointed to '146 million Russian people'. (President of Russia, 2018)

After president Trump had won the elections, accusations were made that his campaign had worked together with the Russian government in order to secure their victory. Eventually, the Department of Justice initiated its own independent investigation into the campaign and its aftermath, led by special counsel Robert Mueller. His 2019 report has again attributed the entire campaign to Russian intelligence, stating Russia had aimed to influence the election *"in sweeping and systemic fashion"*. (Mueller, 2019) The report provides some unclassified evidence against Russia's units held responsible for the DNC leaks and the 2016 election interference.

According to the 2019 report assembled by special counsel Robert Mueller, Russia's military intelligence agency GRU was the primary responsible agency. In particular, Main Special Service Unit 26165 (APT28) in cooperation with Unit 74455 (SANDWORM) were identified as the culprits. Unit 26165 was behind the spear phishing campaigns that led to the initial foothold within the DNC network. It also registered the domain name DCLeaks.com. Unit 74455 was responsible for the persona Guccifer 2.0 and most of the communication with WikiLeaks staff. According to the Mueller report, both units coordinated their actions with one another.(Mueller, 2019)

However, the initial investigation led by Crowdstrike stated forensics had indicated that two separate agencies had worked on the DNC hack. These agencies did not seem to cooperate, even to compete with one another. On certain occasions they compromised each other's operations while trying to gain a foothold on the DNC servers. According to Crowdstrike, these agencies were APT28 (Unit 26165) and APT29 (Rid, 2020a; U.S. House of Representatives, 2017) The Mueller report however does not mention APT29.

The District Court of Columbia indicted twelve Russian GRU senior officers of Units 26165 and 74455 for 'large scale interference' in the 2016 elections stating their full names, rank, and position. This is indicative of the level of knowledge and confidence the US had in their attribution. (U.S. District Court of Columbia, 2018)

Among the technical traces that the GRU left are:

- The use of a Moscow based server by Unit 74455 server to create the Guccifer 2.0 Wordpress blog. (Mueller, 2019)
- The bitcoin payments of hired servers in Arizona. Mueller's investigation points out that these coins were mined by the GRU to increase anonymity. The servers exfiltrated the DNC data from servers in Arizona and Illinois back to the GRU. (Rid, 2020a)
- Twitter accounts set up by the GRU were used to communicate with DCLeaks and Wikileaks, including WikiLeaks founder Assange. (Mueller, 2019)
- Spear phishing URLs targeting the DNC staff were all traced back to Bitly accounts which had targeted thousands of other known GRU targets. These included Eastern-European militaries, critical journalists and the spokesperson for the prime minister of Ukraine. (SecureWorks, 2016)
- The use of Russian metadata found in the documents disseminated by Guccifer 2.0. (Franceschi-Bicchierai, 2016)
- The lack of Romanian language skills of the persona Guccifer 2.0 (Franceschi-Bicchierai, 2016)
- The presence of GRU attributed malware (indicators of compromise) used in other attacks including Ukraine. (U.S. House of Representatives, 2017)
- The presence of Russian state hackers digital 'fingerprints' based on tactics and procedures in previously investigated attacks by Russia. (U.S. House of Representatives, 2017)
- The use of known APT28 registered spoofed name servers in the operation.[26] (Bundesamt für Verfassungsschutz, 2016)
- The use of a Russian language only VPN service by Guccifer 2.0. (ThreatConnect, 2016a)

The IRA troll farm was financed by Yevgeny Prigozhin, a Russian businessman who is loyal to president Putin. (Rid, 2020a) The troll operations were traced back to the agency's headquarters in St. Petersburg, based on both classified evidence in the Mueller report as well as data provided by social media companies analysed by academia. (Howard et al., 2018; Mueller, 2019) Some IRA accounts were set up using Russian (St. Petersburg) IP-addresses and phone carriers. (Howard et al., 2018) Another clue was found in the metadata of the documents shared with WikiLeaks. One of the hackers used the Cyrillic

[26] A spoofed name server resembles a legitimate name server, but is actually administered by another party. An example is nato-org.com. In this case, Russian intelligence paid in bitcoins for more than 300 spoofed name servers. (ThreatConnect, 2016b)

nickname of a former Soviet director of the secret police as his username[27], another hacker gave away his Russian language settings through the metadata. (Rid, 2020a)

Furthermore, the agency sent two covert operatives to the US in order to collect information for the IRA, they later were identified and indicted. (Mueller, 2019) Finally, internal communication within the IRA that was secured by the US confirmed the aim to criticise Clinton and support Trump. (Office of the D.N.I., 2017) Prigozhin, his companies and a few employees have too been indicted for this interference by a US court. Although the IRA's campaign served the interests of the Russian government and was financed by an ally of President Putin, there is no evidence indicating it coordinated its actions with Russian intelligence agencies. (Rid, 2020a)

### 4.2.4. Effects of the operations

Few people had predicted that Donald Trump would become the 45th president of the United States, with the famous exception of the Simpsons cartoon series. Both Trump and Sanders were widely regarded as outsiders for the presidency. (Jamieson, 2020) If the Russian information operation was indeed a factor in this unlikely outcome, it is a very significant effect.

Many scholars have written about the effectiveness of the 2016 election interference campaign. Whether the campaign had a decisive effect on the election of President Trump is virtually impossible to say, but it cannot be ruled out entirely. Many scholars agree that the combined information operations and active measures of Russian intelligence and the IRA did have an effect on voters in the US. In this case, it had an unquantifiable though favourable effect on Donald Trump's campaign. It can also be argued safely that those same efforts, including the leaked documents from campaign leader Podesta, damaged Hillary Clinton and the Democratic Party's reputation. In that sense, the operations were successful in its intended effects. (Howard et al., 2018; Jamieson, 2020; McCombie, Uhlmann, & Morrison, 2020)

Interestingly however, traditional and contemporary independent media contributed greatly to the successfulness of the Russian operations. They did so by publishing leaked documents stolen by the GRU and published by well-read websites such as WikiLeaks, while obscuring the Russian source. They did so by their reporting on fake news trolls, giving these stories much wider coverage (Rid, 2020a) Lastly they did so by allowing already exposed trolls spread

[27]The username was "Феликс Эдмундович" or Feliks Edmundovich, the nickname of "Iron" Feliks Dzerzhinsky, the father of active measures and a Soviet (dis)information specialist. (Rid, 2020a)

divisive and violent messages all over social media. Consequently, both the actual and the perceived influence that Russia had on the election outcome were amplified. (Jamieson, 2020)

The 2016 election interference operation had other, perhaps less intended (political) effects. It further damaged the already strained relationship between Russia and the West. It also helped increase the distrust of the US (and western) citizens in main stream journalism, shifting people away from established media to more partisan and 'fake news' outlets. (Jamieson, 2020) This shift gave rise to some infamous conspiracy theories such as Pizzagate.[28] Furthermore, it exploited and amplified the damaged trust of voters in the other party, be it the Republican or Democratic. This process of domestic polarisation was already ongoing, but certainly not hindered by the Russian operation. (Jamieson, 2020)

Finally, the world and the US again were made aware of the power of social media and the companies who dominate these platforms, as the Cambridge Analytica scandal had already shown before.[29] Open and democratic societies and the United States in particular are vulnerable to influence operations through social media, especially given the deeply rooted polarisation within the US. (Cosentino, 2020) Russia effectively weaponised the use of American social media and technology companies against the United States. Politicians and NGO's have called for more government oversight and control over social media to battle fake news, but thus far these calls have had limited effect. All together it means that the US and other western states are still susceptible to such forms of information warfare. Western societies are still under attack by other states, including Russia, who aim to undermine their democracies. (Cosentino, 2020; Howard et al., 2018)

[28] In the leaked documents stolen from campaign leader Podesta, sentences such as ordering pizza and hotdogs were explained in a conspiracy theory as a codewords used in pedophile circle run by candidate Clinton's inner circle. According to research, nearly one in three American believed this was "probably" or "definitely" true. (Jamieson, 2020)

[29] Cambridge Analytica was a company who harvested data from Facebook users to build profiles of its customers. These profiles were then sold for political purposes, including the campaign of President Trump

## 4.3 Discrepancies

Both operations deployed attacks against election infrastructure, although in Ukraine, Russia was slightly more successful with the partial CEC website data fraud. The troll campaign was largely similar too, and not very effective. The defacement of politicians was somewhat effective too in both elections, arguably slightly more in the US in particular with regard to candidate Clinton. Domestic media and Wikileaks quickly picked up on the leaked materials of the DNC. Such credible and well covered *kompromat* was not observed in the Ukrainian elections. Finally, the operations in Ukraine were part of a larger offensive cyber operation against Ukrainian infrastructure, in the USA such large-scale operations were not reported, although they may have occurred.

## 4.4 Sub conclusion

The third sub research question was:

**3. Which factors influence the different effects of Russian digital information operations targeting elections in Ukraine compared to similar operations in the USA?**

The accompanying hypotheses were:

*H 3.1: Russian information operations in Ukraine are designed to damage the confidence of the population in the state and those who lead it as well as to exploit and amplify social polarisation.*

The Russian information operations aim to undermine the Ukrainian government and to increase social tensions, instead of actually swaying the vote to Russia's advantage. Ukrainian politicians have gained a reputation of corruption for good reason, and information campaigns successfully emphasised this. President Poroshenko most likely would have lost the 2019 election regardless of Russian interference. Even so, well-developed Russian smear campaigns against Ukrainian politicians are likely to further erode the already little confidence citizens have in the government and its institutions. (Golovchenko et al., 2018) Studies have shown that spreading divisive content through social media and online news outlet fuels social polarisation and consequently the ongoing civil war in Ukraine. Russia intentionally uses theses political warfare methods to prevent Ukraine from becoming a unified and pro-Western state. (Allen & Moore, 2018) Hypothesis 3.1 is thus considered not falsified.

*H 3.2: Russian digital information operations in Ukraine are dependent on the factors: Ukrainian sentiments concerning Russia, familiarity with disinformation and a conflict scenario*

Russia regards Ukraine part of the Russian near abroad and a region of great strategic and cultural importance for centuries. Those in power perceived the anti-Russian developments in Ukraine, which culminated in the Euromaidan revolution of 2014 and the following civil war, as a plot orchestrated by the West. (Delcour & Wolczuk, 2015) Conversely, the general attitude of Ukrainians towards Russia, other than the population of separatist regions, has steadily deteriorated since that revolution. (Pifer, 2017)

Ukraine has been a part of the Soviet Union and (at least partially) of Imperial Russia for centuries. As such it is familiar with Russian propaganda tricks and the methods of its intelligence agencies. Considering the recent aggravated hostility between the countries, it is apparent that the general Ukrainian attitude towards pro-Russian information is at the very least suspicious. Still, Russian information operations in pro-Russian regions have had a positive effect on the perception of Russia there. This leads to increasing social polarisation in Ukraine, which *is* advantageous for Russia. Although this does not counter the hypothesis, it does mean that Russian election interference meets other objectives in similar fashion as was concluded in H 3.1.

Then there is the ongoing conflict scenario in Donbass and, to a lesser extent, Crimea. In Donbass pro-Russian separatist fight against the Ukrainian armed forces supported by Russia. Russia employs a wide range of tools, including digital information operations, which support the separatists who continue the fight. Election results in Ukraine are barely affected by Russian interference. Instead, these operations aim to influence the public opinion regarding the conflict, again discrediting the Ukrainian government and armed forces. The information operations should be understood as part on an integral effort by Russia to advance its interests in the Ukraine conflict. Hypothesis 3.2 is considered not falsified.

*H 3.3: Russian digital information operations in the USA are dependent on the factors: familiarity with Russian information operations, a climate of social polarisation and the dissemination of 'Russian' content by domestic media.*

Although Soviet active measures have targeted the USA since the Cold War, the USA had grown unfamiliar with the nature of the combined Russian active measures that preceded the 2016 elections. The hack and leak operation against the DNC successfully spread *kompromat* materials about the DNC, but the effects this had on the Democratic Party and its candidate were significantly amplified by western media. The much smaller exposure that Russian website DCLeaks had compared to WikiLeaks is an example of this. The fact that the GRU had contacted Wikileaks proactively contributed greatly to their smear campaign against Clinton. Furthermore, the IRA troll factory, though not known for its sophistication nor subtleness, contributed to the further deteriorating

socio-political climate in the USA. In the end, the Russian information operations likely had a favourable effect on the election of President Trump because the US had been unfamiliar with such an integral and cunning campaign. Moreover, the deteriorated socio-political climate was exploited successfully by the Russian operation. Hypothesis 3.3 is considered not falsified.

Finally, it can thus be concluded that:

- The differences in familiarity with information operations as observed in these elections;
- The presence of an ongoing conflict scenario (and the lack of this in the USA) and;
- The dissemination of Russian content by American media and subsequent increased exposure of it;

were the most important contributing factors to the relatively successful operation in the USA and the consequent discrepancies between these two different Russian operations.

# 5. Conclusion

The main research question was:

**Which factors influence the different effects of Russian cyber operations in Ukraine compared to similar operations in the USA?**

In line with Russia's national security strategy, cyberattacks disrupting critical infrastructure and digital information operations interfering in elections are in fact both examples of cyber enabled information warfare used in separate conflicts. These operations provide Russia with deniability and ambiguity in their campaigns. Furthermore, these operations are a continuation of Russian non-linear strategies in armed conflict scenarios as well as in its fight against American (information) dominance. Information warfare provides Russia with tailored tools of information warfare serving varying interests and objectives in Ukraine and the USA.

This research has found that Russian power grid cyberattacks in Ukraine are more disruptive than in the USA, while information operations were more effective in the USA. Russia is less hesitant to disrupt critical infrastructure in Ukraine due to is involvement in the Ukrainian conflict and the limited potential of escalation of applying such disruptions in Ukraine. Additionally, Ukraine provides Russia with opportunities to test its cyber operations without risking large scale retribution from powerful states. In the USA, the risks involved with disrupting critical infrastructure are considerably higher. These factors help explain why Russia tries to challenge the USA with a more subtle, political war. Interestingly, Russia has been quite effective in the latter.

Conversely, the information operations targeting the presidential elections in Ukraine failed to influence these elections, although this was not the ultimate goal. Russia *was* able to deepen the divide between the pro-Russian and pro-Western population in Ukraine. They also succeeded in damaging Ukraine's confidence in some of its elected leaders, though not to the same extent as in the United States. This research argues the fact that Ukraine is more familiar with-, and more resilient to-, Russian disinformation is a factor which influenced this. Overall, anti-Russian sentiment has risen since the 2014 revolution in spite of Russian information operations. The ongoing conflict in Donbass and the annexation of Crimea are an important factor in this.

In the USA information operations are primarily used as *active measures*. These measures aim to counter the perceived Russian national security threats coming primarily from the West, by weakening America from the inside. They also serve as excellent tools of political espionage. The DNC hack and leak effort applies to both purposes. Through espionage they were able to attack American

politicians effectively with an information war effort. These efforts were supported considerably by domestic and western media. This factor applies significantly less to the situation in Ukraine. The lack of an armed conflict with Russia, as is the case in Ukraine, was another factor of influence found in this research contributing to the different outcomes.

Russia had success in the USA on a political-strategic level. Digital information operations in the 2016 US elections were unexpectedly influential. If Russia just want to erode trust in democracy and the Federal government in the US, they likely succeeded. But they achieved more than that. This research has argued that Russia had a favourable effect on the election of President Trump, which is an astonishing feat on its own.

As said, in both countries Russia succeeded to exploit and worsen social polarisation. In doing so they damaged these societies' confidence in government, politics, established media and even facts. The discussed operations have also been instrumental to the worst multi-lateral relations between the West and Russia since the end of the Cold War. Moreover, Ukraine is still an independent country and relations with its large Slavic neighbour have also steadily deteriorated. The question which comes to mind is whether the costs of information warfare outweigh the benefits for Russia.

Open and democratic societies are equally or perhaps even more vulnerable to disinformation than to disruptions of critical infrastructure. Improving our cybersecurity defences should therefore include efforts to defend against future attempts to subvert and weaken our societies by autocratic states including, but not limited to, Russia. One of the best defences can be found in protecting and maintaining the foundations of democracy in the widest possible sense. Much is at stake here: civil war is still raging in Donbass causing losses to both sides, while democracy is under attack in the USA and in Europe from the outside and the inside. We need to be on guard.

## 5.1 Limitations

The effects of cyber operations depend on many different factors, some of which have been compared and studied in this research. The similarities between the different cases are not absolute, small differences may still influence the effects of cyber operations. Furthermore, there most likely are factors influencing the effects of cyber operations in a country that have not been included. Economical and geographical differences between Ukraine and the USA, might influence the effects of Russian cyber operations in these countries. Another factor that has not been dealt with in this research is the cyber resilience against attack of the compared countries. This could very well be an important factor in the effects that Russian operations had or did not have.

This research has found that certain factors and circumstances such as the presence of armed conflict matter both to the intentional effects and the actual effects of Russian cyber operations. Real world variables evidently cannot be controlled for scientifical purposes. Inferring conclusions on such empirics is therefore difficult, especially since Russian Intelligence agencies have shown they do not always operate in a rational, unified, or predictable way. Another limitation is the secrecy involved with intelligence operations, meaning many detailed sources on offensive cyber operations are off limits for public research. The same is true for detailed information on the discovery and mitigation of such threats.

## 5.2 Further research

Further research could help increase the validity of the conclusions. This could be done in several ways. One option could be to study Russian similar cyber operations conducted in other countries than Ukraine and the USA. These could include countries in Western Europe and the near abroad as there are plenty of available cases. Several European countries including Germany, the United Kingdom and France have reported election interference by Russia. Such an approach could provide insights into whether intended effects and actual effects of such operations are similar to what was found in this research.

Another approach could be to widen the scope, for example by examining attacks on critical infrastructure in western countries by Russian Intelligence agencies, or even all Russian cyberattacks on critical infrastructure on record. Again, this could help sharpen or adjust the conclusions found in this research that such operations are in fact information operations too.

Further research could also include focussing on other countries conducting offensive cyber operations against digital infrastructure in the West, such as China, Iran, and North-Korea. There are likely to be both differences and similarities in their different approaches and effects. Finally, in particular for the USA, its own offensive cyber operations and digital espionage efforts cause reactions from (digital) adversaries. The NotPetya worm is perhaps the best example. It showed the world that exploits developed by state hackers can be also be used against the country they serve. As such this may influence operations that countries like Russia and Iran in turn conduct against the USA. This approach could shed light on potential action-reaction correlation factors in offensive cyber operations.

# Bibliography


Abrams, S. (2016). Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections: The Quarterly Journal*, *15*(1), 5–31. https://doi.org/10.11610/connections.15.1.01

Adcock, R., & Collier, D. (2001). Measurement validity: A shared standard for qualitative and quantitative research. *American Political Science Review*, *95*(3), 529–546. https://doi.org/10.1017/S0003055401003100

Allen, T., & Moore, A. (2018). Victory without Casualties: Russia's Information Operations. *Parameters*, *48*(1), 59–71. Retrieved from http://search.proquest.com/openview/6e817c9bebbbd44daa6a27e599371b1c/1?pq-origsite=gscholar&cbl=32439

Baezner, M., & Robin, P. (2018). *Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict*. Zurich. Retrieved from www.css.ethz.ch

BBC News. (2016). Ukraine cyber-attacks "could happen to UK." Retrieved October 11, 2020, from https://www.bbc.com/news/technology-35686493

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

Blank, S. (2013). Russian information warfare as domestic counterinsurgency. *American Foreign Policy Interests*, *35*(1), 31–44. https://doi.org/10.1080/10803920.2013.757946

Bouchet, N. (2016). Russia's "militarization" of colour revolutions. *CSS Policy Perspectives*, *4*(2), 1–4. https://doi.org/10.3929/ethz-a-010682969

Buchanan, B. (2020). *The Hacker and the State* (1st ed.). Cambridge, MA: Harvard University Press. https://doi.org/10.4159/9780674246010

Buchanan, B., & Sulmeyer, M. (2016). *Russia and cyber operations: challenges and opportunities for the next U.S. administration*. Retrieved from https://carnegieendowment.org/files/12-16-16_Russia_and_Cyber_Operations.pdf

Bundesamt für Verfassungsschutz. (2016). *BfV Cyber-Brief Nr. 01/2016*. Koln. Retrieved from https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-cyberabwehr/broschuere-2016-03-bfv-cyber-brief-2016-01

Cherepanov, A. (2016). *The rise of TeleBots: Analyzing disruptive KillDisk attacks . ESET*. Retrieved from https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/

Cherepanov, A., & Lipovsky, R. (2017). Industroyer: Biggest threat to industrial control systems since Stuxnet. *WeLiveSecurity, ESET*, *12*. Retrieved from https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

Clausewitz, C. V. (1832). *On War Translated; and edited by Michael Howard and Peter Paret, Princeton, N.J. Princeton University Press* (Translatio).

Clayton, M. (2014). Ukraine election narrowly avoided "wanton destruction" from hackers . Retrieved November 6, 2020, from

https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

Communications Security Establishment. (2020). CSE Statement on Threat Activity Targeting COVID-19 Vaccine Development. Retrieved November 29, 2020, from https://cse-cst.gc.ca/en/media/2020-07-16

Connell, M., & Vogler, S. (2017). *Russia's Approach to Cyber Warfare*. Retrieved from https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf

Cosentino, G. (2020). Polarize and Conquer: Russian Influence Operations in the United States. In *Social Media and the Post-Truth World Order* (1st ed., pp. 33–57). Springer International Publishing AG. Retrieved from https://ebookcentral-proquest-com.ezproxy.leidenuniv.nl:2443/lib/leidenuniv/detail.action?docID=6135165#

Crowdstrike. (2020). CrowdStrike Global Threat Report, 1–32. Retrieved from papers3://publication/uuid/DCFC62BA-BD06-4255-9A01-BAD5DE94D643

CrowdStrike. (2013). *CrowdStrike Global Threat Report 2013 Year In Review*. Retrieved from papers3://publication/uuid/DCFC62BA-BD06-4255-9A01-BAD5DE94D643

D. Gallacher, J., & W. Heerdink, M. (2019). Measuring the effect of Russian Internet Research Agency information operations in online conversations. *Defence Strategic Communications*. https://doi.org/10.30966/2018.riga.6.5.

Darczewska, J. (2014). *The Anatomy of Russian Information Warfare. The Crimean Operation. A Case Study*. *Point of View* (Vol. May 2014).

Davis, C. (2002). Country survey XVI - The defence sector in the economy of a declining superpower: Soviet Union and Russia, 1965-2001. *Defence and Peace Economics*. https://doi.org/10.1080/10242690210978

Delcour, L., & Wolczuk, K. (2015). Spoiler or facilitator of democratization?: Russia's role in Georgia and Ukraine. *Democratization*, *22*(3), 459–478. https://doi.org/10.1080/13510347.2014.996135

Desouza, K. C., Ahmad, A., Naseer, H., & Sharma, M. (2020). Weaponizing information systems for political disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT). *Computers and Security*, *88*, 101606. https://doi.org/10.1016/j.cose.2019.101606

DFR Lab. (2019). Russian Op 3: The Blue Man and the Mole. Retrieved November 8, 2020, from https://medium.com/dfrlab/russian-op-3-the-blue-man-and-the-mole-3ba77b9eb955

DHS. Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security, Department Of Homeland Security § (2016). DHS Press Office. Retrieved from https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

DHS & FBI. (2016). *GRIZZLY STEPPE – Russian Malicious Cyber Activity Summary*. *Jar-16-20296*. Retrieved from https://www.us-cert.gov/tlp.

Director of National Intelligence. (2019). *STATEMENT FOR THE RECORD WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY*. Washington D.C. Retrieved from https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf?fbclid=IwAR34lXwDOCQshv9XAVqgJ3h3ZBFWpDw5xuWZZCU8V43RMSNZZt8E6KmrATc

Diresta, R., & Grossman, S. (2019). *Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019*. Stanford. Retrieved from https://cyber.fsi.stanford.edu/io/news/potemkin-pages-personas-blog

Dobbins, J., Cohen, R., Chandler, N., Frederick, B., Geist, E., DeLuca, P., … Williams, B. (2019). *Extending Russia: Competing from Advantageous Ground*. Santa Monica. Retrieved from https://www.rand.org/pubs/research_reports/RR3063.html

Dosenko, A., Gerachkovska, O., Shevchenko, V., & Bessarab, A. (2019). Media as a tool for forming the president's image (On the example of the 2019 election process). *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 1623–1628. https://doi.org/10.35940/ijitee.A4632.119119

Estonian Foreign Intelligence Service. (2018a). *INTERNATIONAL SECURITY AND ESTONIA*. Tallinn. Retrieved from https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

Estonian Foreign Intelligence Service. (2018b). *INTERNATIONAL SECURITY AND ESTONIA 2018*. Retrieved from https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

EU vs Disinformation. (2019). Year in review: 1001 messages of pro-Kremlin disinformation. Retrieved September 27, 2020, from https://euvsdisinfo.eu/year-in-review-1001-messages-of-pro-kremlin-disinformation/

Facebook. (2019). Removing Coordinated Inauthentic Behavior in Thailand, Russia, Ukraine and Honduras . Retrieved November 8, 2020, from https://about.fb.com/news/2019/07/removing-cib-thailand-russia-ukraine-honduras/

Faesen, L., Torossian, B., Mayhew, E., & Zensus, C. (2019). *Conflict in Cyberspace | Strategic Monitor 2019-2020*. Retrieved from https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/conflict-in-cyberspace/

FireEye. (2017). *Russia's APT 28 Strategically Evolves its Cyber Operations*. Milpitas. Retrieved from https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html

Franceschi-Bicchierai, L. (2016). Here's the Full Transcript of Our Interview With DNC Hacker "Guccifer 2.0." Retrieved October 29, 2020, from https://www.vice.com/en/article/yp3bbv/dnc-hacker-guccifer-20-full-interview-transcript

Galeotti, M. (2015). 'Hybrid War' and 'Little Green Men': How It Works, and How It Doesn't. In S. McGlinchey, M. Karakoulaki, & R. Oprisko (Eds.), *Ukraine and Russia: People, Politics, Propaganda and Perspectives* (1st ed., pp. 156–165). Bristol: E-International UK. Retrieved from https://shron2.chtyvo.org.ua/Zbirnyk_statei/Ukraine_and_Russia_People_

Politics_Propaganda_and_Perspectives_anhl.pdf?PHPSESSID=df316662ff482e1e0dfdea1bff842a83#page=164

Galeotti, M. (2016a). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? *Small Wars and Insurgencies*, *27*(2), 282–301. https://doi.org/10.1080/09592318.2015.1129170

Galeotti, M. (2016b). *Putin's Hydra: Inside Russia's Intelligence Services*. Berlin. Retrieved from https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf

Galeotti, M. (2019). The mythical 'Gerasimov Doctrine' and the language of threat. *Critical Studies on Security*. https://doi.org/10.1080/21624887.2018.1441623

Gardner, A., Stanley-Becker, I., & Viebeck, E. (2020). Officials stress security of election systems after U.S. reveals new Iranian and Russian efforts - The Washington Post. *The Washington Post*. Retrieved from https://www.washingtonpost.com/politics/2020-election-security/2020/10/24/4b290ef8-1479-11eb-ad6f-36c93e6e94fb_story.html

Gerasimov, V. (2013). The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military-Industrial Kurier*.

Gerring, J. (2011). *Social Science Methodology*. *Social Science Methodology*. Cambridge University Press. https://doi.org/10.1017/cbo9781139022224

Giles, K. (2011). "Information Troops"-a Russian Cyber Command? In *3rd International Conference on Cyber Conflict, Tallinn, 2011* (pp. 11–16).

Giles, K. (2016a). *HANDBOOK OF RUSSIAN INFORMATION WARFARE*. Rome. Retrieved from https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook%2C Russian Information Warfare.pdf

Giles, K. (2016b). *Russia's 'New'' Tools for Confronting the West.' Russia and Eurasia* (Vol. 1). https://doi.org/10.1515/sirius-2017-0037

Giuliano, E. (2018). Who supported separatism in Donbas? Ethnicity and popular opinion at the start of the Ukraine crisis. *Post-Soviet Affairs*, *34*(2–3), 158–178. https://doi.org/10.1080/1060586X.2018.1447769

Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, *8*(4), 597–606. Retrieved from http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf

Golovchenko, Y., Hartmann, M., & Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine: Citizen curators of digital disinformation. *International Affairs*, *94*(5), 975–994. https://doi.org/10.1093/ia/iiy148

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice ? *Strategic Studies Quarterly*, *155*, 102–135.

Greenberg, A. (2017). Hackers Gain Direct Access to US Power Grid Controls | WIRED. Retrieved September 26, 2020, from https://perma.cc/6BUT-5AYX

Greenberg, A. (2019). *Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers* (1st ed.). New York: Doubleday.

Greenberg, A. (2020). The Russian Hackers Playing "Chekhov's Gun" With US Infrastructure |. Retrieved November 29, 2020, from https://www.wired.com/story/berserk-bear-russia-infrastructure-hacking/

Hayden, M. V. (2011). The future of things cyber. *Strategic Studies Quarterly Spring*, *5*(1), 3–7. https://doi.org/10.2307/26270507

Heickerö, R. (2010). *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. Swedish Defense Research Agency (FOI). Retrieved from www.foi.sedefenceanalysisfax:+46855503100SE-16490Stockholm

Herszenhorn, D. (2014). Kiev Blamed for Blackout in Capital of Crimea. *New York Times*. Retrieved from https://www.nytimes.com/2014/03/25/world/europe/ukraine-pulls-all-its-forces-out-of-crimea.html

Hoepfl, M. C. (1997). Choosing Qualitative Research: A Primer for Technology Education Researchers. *Journal of Technology Education*, *9*(1), 47–63. https://doi.org/10.21061/jte.v9i1.a.4

Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2018). *Computational propaganda research project: The IRA, social media and political polarization in the United States, 2012-2018*. Oxford: Project on Computational Propaganda. Retrieved from https://digitalcommons.unl.edu/senatedocs/1/

Hulcoop, A., Scott-Railton, J., Tanchak, P., Brooks, M., & Deibert, R. (2017). *TAINTED LEAKS Disinformation and Phishing With a Russian Nexus*. Toronto. Retrieved from https://citizenlab.ca/2017/05/tainted-leaks-

Hultquist, J. (2016). Sandworm Team and the Ukrainian Power Authority Attacks . Retrieved October 10, 2020, from https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html

IEEE. (2016). Russian National Security Strategy, December 2015. Retrieved from http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf

Internet World Stats. (2020). Internet Growth Statistics 1995 to 2019 - the Global Village Online. Retrieved September 6, 2020, from https://www.internetworldstats.com/emarketing.htm

INTSIGHTS. (2019). *Russia's Most Dangerous Cyber Threat Groups*. Retrieved from http://wow.intsights.com/rs/071-ZWD-900/images/RussianAPTs.pdf

Jamieson, K. H. (2020). *Cyberwar: How Russian Hackers and Trolls Helped Elect a President—What We Don't, Can't, and Do Know* (1st ed.). New York: Oxford University Press. Retrieved from https://ebookcentral-proquest-com.ezproxy.leidenuniv.nl:2443/lib/leidenuniv/detail.action?pq-origsite=primo&docID=5497194

Jensen, B., Valeriano, B., & Maness, R. (2019). Fancy bears and digital trolls:

Cyber strategy with a Russian twist. *Journal of Strategic Studies*, *42*(2), 212–234. https://doi.org/10.1080/01402390.2018.1559152

Joint Chiefs of Staff USA. (2012). *JP 3-13, Information Operations*.

Jonsson, O., & Seely, R. (2015). Russian full-spectrum conflict: An appraisal after Ukraine. *Journal of Slavic Military Studies*, *28*(1), 1–22. https://doi.org/10.1080/13518046.2015.998118

Karlsen, G. H. (2019). Divide and rule: ten lessons about Russian political influence activities in Europe. *Palgrave Communications*. https://doi.org/10.1057/s41599-019-0227-8

Kofman, M., & Rojanksy, M. (2015). *A Closer look at Russia's "Hybrid War"* (Kennan Cables April 2015 No. 7). Washington D.C. Retrieved from https://www.wilsoncenter.org/sites/default/files/media/documents/publication/7-KENNAN CABLE-ROJANSKY KOFMAN.pdf

Koval, N. (2015). Revolution Hacking. In Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (pp. 55–59). Tallinn: NATO CCD COE Publications. Retrieved from www.ccdcoe.org

Lamont, C., & Boduszynski, M. P. (2020). *Research Methods in Politics and International Relations* (1st ed., Vol. 1st). London: SAGE.

Lee, R. M. (2017). *CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids*. Retrieved from https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/

Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case. *Electricity Information Sharing and Analysis Center*, 36. Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Lin, H. (2012). Escalation Dynamics and Conflict Termination in Cyberspace Terminology and Basic Concepts. *Strategic Studies Quarterly*, *6*(3), 46–70.

Lyngaas, S. (2019). Ukraine's president accuses Russia of launching cyberattack against election commission. Retrieved November 8, 2020, from https://www.cyberscoop.com/ukraines-president-accuses-russia-launching-cyberattack-election-commission/

Lyngaas, S. (2020a). German intelligence agencies warn of Russian hacking threats to critical infrastructure. Retrieved October 17, 2020, from https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

Lyngaas, S. (2020b). Industry alert pins state, local government hacking on suspected Russian group. Retrieved November 29, 2020, from https://www.cyberscoop.com/russia-temp-isotope-election-security-mandiant/

Marks, J. (2014). Hackers DDoS Ukraine elections. Retrieved November 6, 2020, from https://www.politico.com/tipsheets/morning-cybersecurity/2014/10/hackers-ddos-ukraine-elections-first-look-attacks-on-businesses-continue-to-rise-feinstein-intel-is-the-only-defense-against-lone-wolf-terrorists-212543

McCombie, S., Uhlmann, A. J., & Morrison, S. (2020). The US 2016 presidential election & Russia's troll farms. *Intelligence and National Security*, *35*(1), 95–114. https://doi.org/10.1080/02684527.2019.1673940

Mezzour, G., Carley, L. R., & Carley, K. M. (2016). Global Mapping of Cyber Attacks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2729302

Ministerie van Defensie. (2018). Persconferentie: MIVD verstoorde GRU cyberoperatie in Den Haag. Retrieved from https://www.youtube.com/watch?v=jMBdN1n2uBI

Modderkolk, H. (2019). Betrapt op het Rode Plein. In *Het is oorlog maar niemand die het ziet* (1st ed., pp. 178–189). Amsterdam: Podium.

Mueller, R. S. (2019). *Report On The Investigation Into Russian Interferece In The 2016 Presidential Election*. *U.S Depratment Of Justice* (Vol. 1 of 2). Washington D.C. Retrieved from https://www.justice.gov/storage/report.pdf

Nakashima, E. (2017). U.S. officials say Russian government hackers have penetrated energy and nuclear company business networks . *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?utm_term=.76c0a5624111

Newman, L. H. (2020). Russia's Hacking Frenzy Is a Reckoning. Retrieved December 18, 2020, from https://www.wired.com/story/russia-hack-supply-chain-reckoning/

Office of the D.N.I. (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections ": The Analytic Process and Cyber Incident Attribution*. *Office of the Director of National Intelligence*. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf

Office of the President of Ukraine. DECREE OF THE PRESIDENT OF UKRAINE No. 96, Pub. L. No. 96/2016 (2016). President of Ukraine official online representation. Retrieved from https://www.president.gov.ua/documents/962016-19836

Peisakhin, L., & Rozenas, A. (2018). Electoral Effects of Biased Media: Russian Television in Ukraine. *American Journal of Political Science*, *62*(3), 535–550. https://doi.org/10.1111/ajps.12355

Perlroth, N. (2020). Russians Who Pose Election Threat Have Hacked Nuclear Plants and Power Grid. *The New York Times*. Retrieved from https://www.nytimes.com/2020/10/23/us/politics/energetic-bear-russian-hackers.html

Pifer, S. (2017). How Ukraine views Russia and the West. Retrieved November 20, 2020, from https://www.brookings.edu/blog/order-from-chaos/2017/10/18/how-ukraine-views-russia-and-the-west/

Pomerantsev, P., & Weiss, M. (2014). The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. *The Interpreter*, 6. Retrieved from http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf

Popescu, N., Secrieru, S., Soldatov, A., & Borogan, I. (2018). *Hacks, leaks and disruptions: Russian cyber strategies*. *Chaillot Papers*. Paris. Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf%0A%0A

President of Russia. (2018). Interview to American TV channel NBC. NBC News. Retrieved from http://en.kremlin.ru/events/president/transcripts/57027

Rapid Response Mechanism Canada. (2019). *2019 Ukrainian elections final report*. Ottawa. Retrieved from https://www.international.gc.ca/gac-amc/publications/rrm-mrr/ukrainian-elections-ukrainiennes.aspx?lang=eng

Raymond, B. (2020). Forget Counterterrorism, the United States Needs a Counter-Disinformation Strategy. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2020/10/15/forget-counterterrorism-the-united-states-needs-a-counter-disinformation-strategy/

Red Hat. (2020). 14.3.3. Domain Controller. Retrieved October 17, 2020, from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/4/html/reference_guide/s2-samba-domain-controller

Renz, B. (2016). Russia and 'hybrid warfare.' *Contemporary Politics*, *22*(3), 283–300. https://doi.org/10.1080/13569775.2016.1201316

Reuters. (2019). Exclusive: Ukraine says it sees surge in cyber attacks targeting election. Retrieved November 7, 2020, from https://www.reuters.com/article/us-ukraine-cyber-exclusive/exclusive-ukraine-says-it-sees-surge-in-cyber-attacks-targeting-election-idUSKCN1PJ1KX

REUTERS. (2018). German intelligence sees Russia behind hack of energy firms: media report. Retrieved October 17, 2020, from https://www.reuters.com/article/us-germany-cyber-russia/german-intelligence-sees-russia-behind-hack-of-energy-firms-media-report-idUSKBN1JG2X2

Rid, T. (2020a). 2015-207: Leak. In *Active Measures* (1st ed., pp. 445–447). New York: Farrar Straus and Giroux.

Rid, T. (2020b). What is Disinformation. In *Active Measures* (1st ed., pp. 7–16). New York: Farrar Straus and Giroux.

Robinson, J. (2020). Cyberwarfare statistics: A decade of geopolitical attacks. Retrieved December 18, 2020, from https://www.privacyaffairs.com/geopolitical-attacks/#1

Salkind, N. (2012). *Encyclopedia of Research Design*. *Encyclopedia of Research Design*. SAGE Publications, Inc. https://doi.org/10.4135/9781412961288

Sanger, D., & Edmondson, C. (2019). Russia Targeted Election Systems in All 50 States, Report Finds - The New York Times. *The New York Times*. Retrieved from https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html

Sanger, David, E., Perlroth, N., & Schmitt, E. (2020). Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit . *The New York Times*. Retrieved from https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

Sanger, David E., & Perlroth, N. (2019). U.S. Escalates Online Attacks on Russia's Power Grid . *The New York Times*. Retrieved from https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

Schnaufer, T. A. (2017). Redefining Hybrid Warfare: Russia's Non-linear War against the West. *Journal of Strategic Security*, *10*(1), 17–31. https://doi.org/10.5038/1944-0472.10.1.1538

Schoen, F., & Lamb, C. (2012). Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. *INSS Strategic Perspectives*.

Schwirtz, M., & Frenkel, S. (2019). In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering. *The New York Times*. Retrieved from https://www.nytimes.com/2019/03/29/world/europe/ukraine-russia-election-tampering-propaganda.html

Sebenius, A. (2017). Will Ukraine Be Hit by Yet Another Holiday Power-Grid Hack? Retrieved November 14, 2020, from https://www.theatlantic.com/technology/archive/2017/12/ukraine-power-grid-hack/548285/

SecureWorks. (2016). Threat Group-4127 Targets Google Accounts . Retrieved November 1, 2020, from https://www.secureworks.com/research/threat-group-4127-targets-google-accounts

Selhorst, A. J. C. (2016). Russia's Perception Warfare: The development of Gerasimov's doctrine in Estonia and Georgia and its application in Ukraine. *Militaire Spectator*, *185*(4), 148–164. Retrieved from http://news.kremlin.ru/ref_notes/461.

Siggett, S., & Capstone, A. (2017). *THE CYBER COLD WAR: A LOOK INTO RUSSIA'S INFORMATION WARFARE CAPABILITIES*.

Silverman, C. (2016). This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook. Retrieved October 30, 2020, from https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook

Slowik, J. (2019). *Crashoverride: Reassessing the 2016 ukraine electric power event as a protection-focused attack. Dragos Inc.* Retrieved from https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly (Fall)*, *12*(3), 90–113. https://doi.org/10.2307/26481911

Smith, R. (2016). Cyberattacks Raise Alarm for U.S. Power Grid . *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/cyberattacks-raise-alarms-for-u-s-power-grid-1483120708

Soldatov, A., & Borogan, I. (2017). *The red web : the Kremlin's wars on the internet*. *PublicAffairs* (1st ed.). New York: Public Affairs.

State Statistics Committee of Ukraine. (2001). General results of the census: National composition of population. Retrieved December 8, 2020, from https://web.archive.org/web/20070706003257/http://www.ukrcensus.gov.ua/eng/results/general/nationality/

StopFake. (2019). Russian News Monitor: April 1-7, 2019 . Retrieved November 8, 2020, from https://www.stopfake.org/en/russian-news-monitor-april-1-7-2019/

Streltsov, L. (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research*, *2*(2), 147–184. https://doi.org/10.1007/s41125-017-0020-x

Symantec. (2017). *Dragonfly: Western energy sector targeted by sophisticated attack group*. *Symantec Web Site*. Retrieved from https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks+&cd=1&hl=nl&ct=clnk&gl=be

Szostek, J. (2018). Nothing Is True? The Credibility of News and Conflicting Narratives during "Information War" in Ukraine. *International Journal of Press/Politics*. https://doi.org/10.1177/1940161217743258

The Moscow Times. (2014). "Cyber Berkut" Hackers Target Major Ukrainian Bank. Retrieved from https://www.themoscowtimes.com/2014/07/04/cyber-berkut-hackers-target-major-ukrainian-bank-a37033

The White House. (2018). *National Cyber Strategy of the United States of America*. Washington D.C. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Theohary, C. A. (2020). *Defense Primer: Information Operations*. Retrieved from https://crsreports.congress.gov

Thomas, T. (2014). Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *Journal of Slavic Military Studies*, *27*(1), 101–130. https://doi.org/10.1080/13518046.2014.874845

Thomas, T. (2018). Russia's 21st century information war: working to undermine and destabilize populations. *Defence Strategic Communications*, *1*(1), 10–25. Retrieved from https://www.stratcomcoe.org/timothy-thomas-russias-21st-century-information-war-working-undermine-and-destabilize-populations

Thomas, T. L. (2010). RUSSIAN INFORMATION WARFARE THEORY: THE CONSEQUENCES OF AUGUST 2008. *Strategic Studies Institute*.

ThreatConnect. (2016a). Guccifer 2.0: All Roads Lead to Russia. Retrieved October 30, 2020, from https://threatconnect.com/blog/guccifer-2-all-roads-lead-russia/

ThreatConnect. (2016b). What's in a Name Server? . Retrieved October 30, 2020, from https://threatconnect.com/blog/whats-in-a-name-server/

Trend Micro. (2015). Hacktivist Group CyberBerkut Behind Attacks on German Official Websites. Retrieved November 7, 2020, from https://blog.trendmicro.com/trendlabs-security-intelligence/hacktivist-

group-cyberberkut-behind-attacks-on-german-official-websites/

U.S. District Court of Columbia. U.S. v. V. B. Netyksho et al, Pub. L. No. 1:18-cr-00215-AB, 1 (2018). United States of America. Retrieved from https://www.justice.gov/file/1080281/download

U.S. House of Representatives. (2017). *Interview of Shawn Henry (Crowdstrike)*. Washington D.C. Retrieved from https://intelligence.house.gov/uploadedfiles/sh21.pdf

UK Foreign Office. (2020). UK exposes series of Russian cyber attacks against Olympic and Paralympic Games . *Foreign, Commonwealth & Development Office and The Rt Hon Dominic Raab MP* . GOV.UK. Retrieved from https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games

UK NCSC. (2018). Reckless campaign of cyber attacks by Russian military intelligence service exposed. *NCSC News*. Retrieved from https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

UNIAN. (2019). Ukraine's Foreign Intel Service: Russia to spend US$350 mln for meddling in Ukraine elections. Retrieved November 8, 2020, from https://www.unian.info/politics/10421127-ukraine-s-foreign-intel-service-russia-to-spend-us-350-mln-for-meddling-in-ukraine-elections.html

US CERT. (2018). *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors | CISA*. Retrieved from https://us-cert.cisa.gov/ncas/alerts/TA18-074A

US CISA. (2018). Cyber-Attack Against Ukrainian Critical Infrastructure. Retrieved October 9, 2020, from https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

US Department of Justice. Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace , Pub. L. No. 10.19.2020 (2020). U.S. Department of Justice. Retrieved from https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

Votel, J. L., Cleveland, C. T., Connett, C. T., & Irwin, W. (2016). Unconventional Warfare in the Gray Zone. *JFQ*, *80*(1st), 101–109.

Weedon, J. (2015). Beyond "Cyber War": Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine. In K Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (pp. 67–77). Tallinn: NATO CCD COE Publications.

Wilhoit, K. (2016). KillDisk and BlackEnergy Go Beyond Energy Sector. Retrieved October 10, 2020, from https://www.trendmicro.com/en_us/research/16/b/killdisk-and-blackenergy-are-not-just-energy-sector-threats.html

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *WIRED*. Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

# Appendix 1

## Russian 'Information Troops'

Certain Russian units or desks responsible for cyber operations / computer network operations (CNO) have been mentioned over the course of this thesis. This appendix provides an image of the threat landscape of Russian hacker groups that are referred to in this research. These groups are known as Advanced Persistent Threats (APT) in the cybersecurity industry. This overview provides information about the (assessed) affiliation of these groups, their primary targets and known feats.

## GRU associated

***G**lavnoye **R**azvedyvatel'noye **U**pravleniye*, or Main Intelligence Directorate. Part of the General Staff of the Russian Federation's armed forces and Russia's foreign military intelligence service. Currently simply known as GU or Main Directorate. According to some sources, the GRU employs the most capable hackers of the entire Russian Federation. (Estonian Foreign Intelligence Service, 2018a; Greenberg, 2019)

[30]

### Unit 74455 "SANDWORM" (Telebots, Iron Viking, VooDoo Bear, Electrum)

SANDWORM is a commonly heard name given to a particular unit of Russia's military intelligence service GRU by cybersecurity researchers. The name SANDWORM is derived from the science fiction novel *Dune*. Reverse engineering of malware used by SANDWORM showed multiple unique fictional

[30] Figure 1: GRU emblem. Source: https://upload.wikimedia.org/wikipedia/commons/thumb/b/b8/Emblem_of_the_GRU.svg/1200px-Emblem_of_the_GRU.svg.png

names derived from *Dune* hidden in their code. The Sandworm is a vicious creature featured in this novel. (Greenberg, 2019, pp. 14–17)

According to several governmental and private sources, its official name is 85th Main Special Service Centre (GTsST), Unit 74455. This unit is headquartered at 22 *Kirova* street Moscow, near the city of Khimki. (US Department of Justice, 2020) SANDWORM is regarded as an aggressive cyber espionage and sabotage group, focussing on critical infrastructure and general military targets. Geographically it has targeted critical infrastructure predominantly in Ukraine. (Greenberg, 2019) Among the many cyber operations that have been attributed to Unit 74455 are:

- The 2016 United States DNC hack, in cooperation with Unit 2616, covered in this research.
- The 2017 NotPetya worm. Affecting businesses and governments worldwide, this worm was one of the most destructive pieces of malware ever released. It infected computers far beyond its intended target in Ukraine and caused billions of euros in damages worldwide. (Greenberg, 2019)
- The 2018 South-Korean Winter Olympic Games sabotage,
- Several attacks on the Ukrainian power grid, which will be covered in greater detail in the case study.

Both the United States and the UK have attributed these attacks to SANDWORM. The United Kingdom's National Cybersecurity Centre, based on independent research, claimed with 95%+ certainty that these operations were the responsibility of Unit 74455. (UK Foreign Office, 2020)

### Unit 26165 (APT28, Fancy Bear, Sofacy, Tsar Team, Strontium)

APT 28 is a second well-known name associated with the GRU 85th Main Special Service Centre Unit 26165. This unit is again located in Moscow, at *20 Komsomolsky Prospekt*. (Greenberg, 2019; Ministerie van Defensie, 2018) Techniques applied by APT28 include spear phishing, credential harvesting watering hole attacks as well as close access operations. Similar to Unit 74455 it targets foreign military and governmental entities with a global and geopolitical focus. Among the operations attributed to 26165 are:

- The 2014 and 2016 attacks on the German Federal Parliament (Bundestag)
- The 2015 French TV5 Monde digital hijacking (under Cyber Caliphate false flag)
- The 2016 World Anti-Doping Agency (WADA) close access operation in Lausanne, Switzerland.

- The foiled 2018 close access operation against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Hague, Netherlands.
- The 2016 US DNC leaks, covered in this research. (INTSIGHTS, 2019)

Some of the malware applied by Unit 26165 include CHOPSTICK, X-Tunnel, X-agent and Mimikatz. (FireEye, 2017)

## SVR associated

**S**luzhba **V**neshney **R**azvedki, or Foreign Intelligence Service, the primary civil foreign intelligence service of the Russian Federation. As such it is responsible for the collection of political and strategic intelligence on foreign governments and institutions.

[31]

### APT29 (Hammertoss, Cozy Bear, The Dukes)

APT29 is another intelligence agency unit conducting computer network operations (CNO). Several researchers have linked it to the SVR(Estonian Foreign Intelligence Service, 2018b; Modderkolk, 2019) Compared to APT28, this actor depends more on long term espionage and stealth operations, while its targets are political, academia as well as think thanks. Operations that APT29 is credited with include:

- The Democratic National Convention (prior to the GRU operation) (2016) (DHS & FBI, 2016)
- 2015 intrusion US Joint Chiefs of Staff (Modderkolk, 2019)
- 2017 intrusion into the Dutch Ministry of General Affairs (prime minister's office) (Modderkolk, 2019)
- 2020 Attempt to steal COVID-19 vaccine information (2020) (Communications Security Establishment, 2020)

[31] Figure 2: SVR emblem source: http://svr.gov.ru/local/templates/main/dist/images/logo.png

## FSB associated

***F**ederal'naya **S**luzhba **B**ezopasnosti (Rossiyskoy Federatsi)* The FSB is Russia's primary successor to infamous Soviet Security Service KGB, and it is the country's largest and most powerful security service. President Putin was director of the FSB before he turned to politics. In order to protect the Russian Federation from foreign threats, it also operates abroad. The FSB has considerable cyber capabilities. (Galeotti, 2016b)


[32]

### Dragonfly 2.0 (Energetic Bear, Berserk Bear)

Dragonfly 2.0 is a particularly secretive APT that has been attributed with the attacks on US critical infrastructure, including those cases that have been covered in this research. Cybersecurity companies and journalists have linked Dragonfly 2.0 to Russia Federal Security Service. (Gardner, Stanley-Becker, & Viebeck, 2020; Greenberg, 2020)

Other attacks that have been attributed to the Dragonfly 2.0 include:

- A 2017 Wi-Fi network hack of San Francisco airport (Perlroth, 2020)
- A foiled attack on a US nuclear power plant. (David E. Sanger & Perlroth, 2019)
- A broad attack on several US government websites including election support systems. (Lyngaas, 2020b)]

The different responsibilities of Russian intelligence and security services are explained well in the table below.

---

[32] *Figure 3: FSB emblem source: https://vk.com/doc480409308_473675860?hash=19c4c2a659ff7f9881*


33

[33] Figure 4: The overlap and differences in roles of the Russian intelligence community. (Galeotti, 2016b)