Cyber as An Instrument of Foreign Policy

By

Friday Ikechukwu Eze

A Thesis submitted to the Faculty of Graduate Studies of

The University of Manitoba

In partial fulfillment of the requirements for the degree of

MASTER OF ARTS

Department of Political Studies

University of Manitoba

Winnipeg

Acknowledgement

The work presented in this thesis was carried out at the University of Manitoba during August 2018 – October 2019.

I wish to express my sincere appreciation to members of the Faculty of Arts including my professors, students and members of staff of the faculty, without whom I would not find the push to go the extra mile on this thesis.

I am immensely grateful to my family; my dad for being a strong pillar of support, my late mum for her precious words of wisdom, my brother Emmanuel for constantly pushing me out of my comfort zone and the rest of my siblings for always supporting me through the trying times.

Finally, I would like to extend my deepest gratitude to my supervisor, Dr. James Fergusson, for introducing me to this topic and helping me see it to completion over the past one year. Without your excellence guidance, advice and assistance, I would not have been able to complete this thesis at all. For this, I am eternally grateful.

Abstract

Over the years, the subject of cyber and everything around it has increasingly come to the forefront. Several experts have given their own views on how cyber is conceptualized but the debate still waxes on. This master's thesis deals with the research question of how cyber is used in foreign policy relations. To answer this research question, a combination of qualitative research methods which includes case studies and use of existing literature are combined to identify and examine the salient roles that cyber plays in foreign policy relations. In this case, cyber should be viewed not just as a domain but as an instrument states employ in war, influence, internal interference, espionage and sabotage. For each of these instances, a unique case study is used to show the how cyber functions in foreign policy relations. The Georgia vs Russia is the first case study, which validates cyber's use as a tool in war. Cyber's use in influence is manifested in the Estonia vs Russia conflict case study, while the 2016 US election discusses the use of cyber in internal interference. Cyber in espionage and sabotage are discussed with the Iran and US vs China case studies respectively. Each of these case studies employs an analogical approach that identifies the salient aspects of each case, linking them to foreign policy actions to offer conclusions beyond reasonable doubt.

Table of Contents

List of Figures

List of Tables

Introduction

Cyber has evolved into a major issue in both international and domestic politics. In terms of politics, the literature is dominated by a variety of conceptualizations of cyber. Domestically, this relates to cyber-crime and criminal activities and also relate to hackers who are doing it for fun. In the international scene, the conceptualization of cyber largely flows around the debate on cyber war.

Several security experts have argued that if cyberwar is going to assume strategic importance, then it must be able to generate effects that are at least comparable to, and preferably more impressive than those available from conventional warfare. The question that throws open this debate is, can it?

There is a wide range of opinion on that score. People have worried about cyberwar for most of the last 20 years, and in all that time, not one person is known to have been killed by a cyber-attack. As for damage, estimates vary widely from several hundred million dollars a year to several hundred billion dollars a year (Libicki, 2011). The costliest single attack was probably the "I Love You" virus in 2000, whose costs have been estimated at as much as $15 billion, but which may be more realistically estimated at several hundred million dollars. Only one power plant is known to have been disabled by hackers, a system in southern Brazil in 2007, and even there, the power outage has been disputed by local authorities as soot buildup. The only two examples of a state's using cyber-attacks against another were Russia's attacks against Estonia in 2007 and Georgia in 2008, which would be discussed in subsequent chapters. Both caused disruption that can be measured at no more than the low millions of dollars, and both pulled their victims closer to rather than pushing them farther from NATO. The Stuxnet worm arguably did serious damage but it was closer in form to a onetime act of sabotage.

The act of sabotage mentioned above works in roughly the same way in the civilian world as it would in the military world. These days, networks and systems are established with some degree of security adequate only to deal with the day-to-day threats such institutions face. Banks, for instance, give a great deal of thought to security in large part because the motive to rob them is ever present. Bank security is fairly good, Bankers can reduce the damage to acceptable levels, which also puts a top bound on the damage a state-sponsored bank thief could carry out. Electric power companies, by contrast, are rarely attacked; what would be the point? Thus, unless they

have been prodded to isolate themselves by the deluge of threat scenarios over the last few years, the difference between a state-level threat and today's threat could be quite substantial, and these institutions mentioned above may not necessarily be so well prepared. But, if state sponsored hackers exist, many such institutions would learn quickly that the threat environment had changed and, with more time, learn how to survive and cope with such change. Coping with the worst attacks might be expensive and disruptive. But, at the very worst, the most primitive response to sever all internet connections, would return the world economies to the state they were in the mid-1990s, before networking became so ubiquitous. Being cyber-bombed back to the 1990s has its downside, but it hardly compares to being bombed back to the Stone Age (Curtis LeMay)[1] by nuclear weapons[2].

More to the point, for cyber to be a strategic weapon for coercive purposes, it has to be frightening to the population at large, or at least to their leaders; so frightening that the aggressors can actually reap some gains from the reaction or concession of their targets (Libicki, 2009). One motive for strategic cyberwar may be to threaten its use to modulate an ongoing conventional war, but that requires the effects of a cyber-attack to be significant relative to the cost, casualties, and damage of violent conflict. Another may be straightforward coercion prior to a war. Imagine a scenario in which Taiwan declares its independence. The Chinese plan to take the island, but want to forestall US intervention. China takes down power in a few US metropolitan areas as a way of suggesting that it can do worse (merely threatening to take down power may be much less impressive and hence less dissuasive, given the great uncertainties in what any given attack can do before one is demonstrated). So, would the United States accede to China's invasion of Taiwan? Or instead, would it regard the Chinese threat to be a strategic threat and thus regard the China-Taiwan struggle as strategic rather than local for having become entangled with that larger threat? US reactions to Pearl Harbor and 9/11 suggest the latter. Strategists, in turn, should not blithely assume other countries can be turned even if they cannot be; those other countries can also be quite stubborn.

It follows that if the use of cyber weapons is unimpressive at the strategic level, the fear that might come from the threat to use cyber weapons may be similarly unimpressive. It is difficult to make

[1] Curtis LeMay was the commander of the pacific air force in World War II who bombed basic level Tokyo and became security level commander. His nickname was "Bombs Away LeMay."

[2] Conventional weapons are those weapons that are not weapons of mass destruction. They include weapons such as armored fighting vehicles, armed helicopters, combat aircraft, artillery and warships. They can also include (but are not limited to small arms, ammunition, cluster munitions and land mines.

credible threats because the efficacy of cyber weapons is strongly, perhaps overwhelmingly, determined by features of those systems such weapons are targeted against. Once such weapons are used successfully, their credibility goes up, but then the attacker, (as well as the target) has to deal with the consequences of their use. Such consequences will complicate and may overwhelm the purely coercive/deterrent effect of threatening subsequent us

While the bulk of reactions to cyberwar emphasize dramatic dangers, some studies offer a more balanced perspective. Tim Maurer contrasts the gloomy picture provided by the bulk of writers with estimates of likely determinants of loss of life associated with a cyberattack (Maurer, 2011). Maurer lists the relative security of civilian infrastructure, participation of non-state actors, and the evolution of law regarding retaliation strategies. He concludes that loss of life from cyberattacks will generally be slight. Indeed, drawing on his estimates, Maurer asserts that "a digital Pearl Harbor would cost fewer lives than the attack 70 years ago."

Wesley Clark and Peter Levin anticipate an inevitable rise in cyberwarfare; one that will eventually involve broad sectors of society (Clarke & Levin, 2009). Populations will face "network-born disruptions of critical national infrastructure" including terrestrial and airborne traffic, energy generation and distribution, and the financial system. The authors note, however, that the United States and other nations are doing a great deal to mitigate the threat. In 2008, the United States pledged a reported $30 billion by 2015 as part of the Comprehensive National Cyber Security Initiative. In addition, Clark and Levin note lessons learned from previous attacks. The most effective electronic security strategy must operate under full disclosure (i.e. all necessary and relevant information concerning the security strategy must be reported to the relevant stakeholders). Experts in academic, industrial, and governmental sectors must quickly collaborate on a mitigation strategy. Yet, Clark and Levin also acknowledge that "electronic security works best when it is autonomous, adaptable, distributed and diversified."

Stephen Walt argues that a critical preliminary task is to separate out different dangers grouped under the common rubric of "cyber-warfare" (Walt, 2010) For Walt, cyberwarfare consists of four distinct issues: degrading an enemy's military capabilities, penetrating networks to shut down civilian infrastructure, web based criminal activity, and cyber espionage. These four issues help to frame cyberwarfare as an evolving, nuanced set of issues, each amenable to its own cost-benefit analysis.

Thomas Rid argues that cyberwar is not really war because it fails to conform to conventional definitions of conflict (Rid, 2012). Rid's chief point, mirroring in an interesting manner Maurer's argument, is that cyberwar is not sufficiently violent or casualty-producing to be considered war. As such, cyberwar is a misnomer. This perspective risks becoming a purely academic exercise, however, if cyber conflict eventually supplants military violence as the ultimate arbiter of international politics. Cyberwar does not need to be war to make war obsolete. Instead, it must fulfill the existing functions of terrestrial warfare if it is to rival the utility of existing forms of conflict.

When carefully analyzed, each of these elements of cyber relative to the domestic and international politics are important to consider, assess and debate the technologies behind all these issues relative to these dominant conceptualizations. However, the international dimension has not been adequately understood or located within a broader understanding. In this context, cyber should be simply understood as an instrument of foreign policy like a range of other instruments of foreign policy but new in the sense of a new technology in a new space.

A country's foreign policy consists of self-interest strategies chosen by the state to safeguard its national interests and to achieve goals within its international relations milieu. The approaches are strategically employed to interact with other countries. The study of such approaches is called foreign policy analysis (Morin & Paquin, 2018).

In recent times, due to the deepening level of globalization and transnational activities, states also have to interact with non-state actors. The aforementioned interaction is evaluated and monitored in attempts to maximize the benefits of multilateral international cooperation. Since national interests are paramount, foreign policies are designed by the government through high-level decision-making processes. National interests can occur as a result of peaceful cooperation with other nations, or through exploitation (Smith et al, 2008).

Usually, creating foreign policy is the job of the head of government and the foreign minister (or equivalent). In some countries, the legislature also has considerable effects. Foreign policies of countries have varying rates of change and scopes of intent, which can be affected by factors that change the perceived national interests, or even affect the stability of the country itself. The foreign policy of a country can have a profound and lasting impact on many other countries and on the course of international relations as a whole, such as the Monroe Doctrine conflicting with

the mercantilism policies of 19th-century European countries and the goals of independence of newly formed Central American and South American countries (Hill, 2003).

While there are many possible topologies for classifying foreign policy of nations, the most commonly used is that dividing the Foreign Policy instruments into political, economic and military. The main political instruments are diplomacy and international alliances and organizations. Economic instruments include foreign aid, economic and trade policy and economic sanctions. The military instruments may take either a persuasive (military pressure or threat) or a coercive form (war) (Morin & Paquin, 2018).

The main political instruments of foreign policy are mainly diplomacy and international alliances and organizations. Diplomacy is the art or practice of conducting international relations. It is important not to equate diplomacy and foreign policy, as the first is merely one of the instruments for the advancement of the latter. The use of diplomacy may include arbitration, either informal (where a group of diplomats are gathered to hear all sides of an issue, and come to a decision potentially based on international law), or formal (where the International Court of Justice at The Hague takes this role); international conferences (where solutions are found on the basis of political discussion, without much resort to international law), negotiations (without the formalities of a conference), and informal diplomacy (such as the use of non-officials or non-mandated officials).

Diplomatic relations and rules are set out by the Vienna Convention on Diplomatic Relations. The Declaration was signed in 1961 and is considered a key document in the history of international relations. The Convention forms the rule-book of diplomacy and has been ratified by nearly every country in the world. It defines the rules of diplomatic relations to be observed between states. It also specifies the rights and immunities for diplomats and rules to be followed in case of resolutions and meeting international agreements (Morin & Paquin, 2018).

Alliances are agreements between two or more actors of foreign policy to cooperate on issues of common interest. Alliances can be open, when publicly known, or covert, when maintained secret, formal, when creating bodies to support and manage them, or informal, when no structures are created (Morin & Paquin, 2018).

The main economic instruments are foreign aid, foreign economic policy and economic sanctions. Foreign aid refers to the voluntary and intentioned transfer of resources, typically, although not always, from one State (donor) to another (recipient). Foreign aid is in itself divided into different categories depending on the objective pursued by the use of the transferred resources which include humanitarian aid (to relieve human suffering during and after man-made or natural disasters, without tackling the original causes of the vulnerability), development aid (to contribute to the economic and social development of the recipient in the long term without necessarily alleviating immediate suffering) and military aid (dedicated to the strengthening of the military capabilities of the recipient).

Although foreign aid is sometimes considered as a non-coercive instrument of foreign policy, mostly dedicated to human, economic and social development, the instrument may be used, and is often used, in a coercive manner. A link is established between the recipient of aid and certain policy objectives of the donor to which the recipient should contribute and by the threat of discontinuing the supply of aid if such contribution does not take place. Foreign aid has often been used to support ideologically closed regimes that have then used that aid to repress their population or enter into aggressive militarist policies towards other States. Additionally, there has been widespread criticism as to the efficiency of aid to achieve its pursued objectives (Hill, 2003).

Trade is defined as the exchange of goods and services between state actors, and is considered to be one of the most relevant instruments of foreign policy in current times. As with all other foreign policy instruments, trade may be used in a cooperative way, where all parties get some benefit, or a coercive way where the benefits or, rather, their absence due to a possible discontinuation of a certain trade policy, may be used to coerce a state actor to operate in a certain manner. While trade policy was in the past a typically bilateral instrument, it has become increasingly multilateral in recent years, with the creation of trade blocks such as the European Economic Community (now European Union), and, especially, the World Trade Organization, (WTO) (Hill, 2003).

Economic sanctions are coercive measures intended by states (imposer, the sanctioning actor) to cause economic damage to another state (target, the sanctioned actor) and thus force it to pursue a certain course of action. They may include tools such as embargoes, boycotts, freezing of funds and assets and other trade or economic restrictions and may be bilateral or multilateral.

The use of sanctions has been refined with the use of the so-called 'smart' sanctions, targeted at specific sectors of the economy or specific persons. The objective of these smart sanctions is to force compliance on the target without unnecessarily damaging the society as a whole, including those parts which may have nothing to do with the policies that the sanctions aim to prevent.

The European Union[3] follows sanctioning regimes imposed by the UN and complements them with further sanctions. It also imposes its own sanctioning regimes. The European Union has imposed sanctions on Iran, Syria, Ivory Coast, Congo, Egypt, Tunis, Libya, etc (Hill, 2003).

There are two types of military instruments, depending on whether or not force is actually used. When force is used, it is warfare, whereas if force is not used it is about military pressure or threat. Military pressure or threat is defined as the threat of use of military force by a foreign policy actor against another foreign policy actor in order to achieve certain objectives, without having to use actual military force.

The use of military pressure has proved quite efficient in reaching natural objectives, avoiding more damaging conflict and maintaining peace at large. It nevertheless entails high risks, such as that of escalating a conflict and ending up in a situation of actual warfare. Additionally, the use of military threat as a foreign policy instrument must include the possibility of actual warfare in order to be credible.

Whereas war has been classically considered as one of the main instruments of foreign policy, such position has gone under pressure in recent times. The use of war as an instrument of foreign policy intends to achieve foreign policy objectives by the coercion of other foreign policy actors, achieved by the use of threat or military force.

It is important to bear in mind that, unlike other foreign policy instruments, the use of war as a foreign policy instrument entails an enormous amount of risk and cost. Risks include the possibility of a military defeat which would render impossible the achievement of the pursued foreign policy objectives, the compromise of other foreign policy interests and objectives and may even put at stake vital interests. Another possible risk is the lack of public support for the war

[3] The European Union, EU is a useful indication of the employment of smart sanctions.

effort, ultimately leading to the demise of a government. It is important to bear in mind that, under international law, war is a legitimate course of action, even if it is confined to self-defense (Article 51 of the UN Charter). International law has aimed at the reduction of the human and economic costs of war.

War may be divided into conventional (open warfare with the use of conventional weapons), unconventional (covert warfare or with the use of non-conventional weapons, such as nuclear, biological or chemical) and asymmetric. Conventional warfare is a form of war conducted by using conventional weapons and battlefield tactics between two or more states in open confrontation. The forces on each side are well-defined, and fight using weapons that target the opponent's military. Unconventional warfare, on the other hand, is a form of warfare that supports foreign insurgency, or it is a resistance movement against its government or an occupying power. Whereas conventional warfare is used to reduce the opponent's military capability directly through attacks and maneuvers, unconventional warfare is an attempt to achieve victory indirectly through a proxy force. Asymmetric differs from both conventional and unconventional warfare in that the parties involved in conflict differ greatly in their military capabilities (Hill, 2003).

Conclusions

Considering all the above instruments of foreign policy, cyber can be used as an instrument of foreign policy in a variety of ways. First, as an instrument in war. This is discussed in detail in chapter two with the Georgian - Russian war used as a case study to show how cyber can be used in modern day war. Second, as a tool for influence (evident in chapter three) in the Estonia - Russia conflict as a case study to establish how cyber can be used as an instrument by one state to influence the policies of another State. Third, as an instrument for interference using Russia's perceived meddling in the US presidential election of 2016 as a case study in chapter four. As an instrument for sabotage, chapter five discusses the attack on Iran's nuclear facilities in 2010 using the Stuxnet virus that is used as a case study to show the impact of cyber when used in espionage and sabotage. Lastly, the China - US case study discusses the impact of cyber as used in espionage activities.

Chapter I
The Cyber World

Introduction

The internet has revolutionized the computer and communications world like nothing before. Following the invention of the telegraph, telephone, radio and computer, the stage has been set for an unprecedented integration of capabilities. The internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. Cyber is synonymous with the concept of the information age.

The roots of the Internet can be found in the 1960's. The Advanced Research Projects Agency Network (ARPANET) was an experimental computer network that was the forerunner of the Internet. The Defence Advanced Research Projects Agency (DARPA), an arm of the U.S. Defense Department, funded the development of ARPANET in the late 1960s. Its initial purpose was to link computers at Pentagon-funded research institutions over telephone lines (Featherly, 2016).

At the height of the Cold War, military commanders were seeking a computer communications system without a central core, with no headquarters or base of operations that could be attacked and destroyed by enemies thus blacking out the entire network in one fell swoop. ARPANET, the grandfather to the Internet, was designed as a computer version of the nuclear bomb shelter. ARPANET protected the flow of information between military installations by creating a network of geographically separated computers that could exchange information via a newly developed technology called Network Control Protocol (NCP). ARPANET's purpose was always more military than academic, but, as more academic facilities connected to it, the network did take on the tentacle-like structure military officials had envisioned. The Internet essentially retains that form, although on a much larger scale (Featherly, 2016).

Originally, there were only four computers connected when ARPANET was created. They were located in the respective computer research labs of UCLA (Honeywell DDP 516 computer), Stanford Research Institute (SDS-940 computer), University of California, Santa Barbara (IBM 360/75) and the University of Utah (DEC PDP-10). The first data exchange over this new network occurred between computers at UCLA and the Stanford Research Institute. On their first attempt

to log into Stanford's computer by typing "log win," UCLA researchers crashed their computer when they typed the letter 'g' (Bellis, 2018)

As the network expanded, different models of computers were connected, which created compatibility problems. The solution rested in a better set of protocols called Transmission Control Protocol/Internet Protocol (TCP/IP) that were designed in 1982. The protocol worked by breaking data into Internet Protocol (IP) packets, like individually addressed digital envelopes. Transmission Control Protocol (TCP) then makes sure the packets are delivered from client to server and reassembled in the right order.

Under ARPANET, several major innovations occurred. Some examples are electronic mail (email), a system that allows for simple messages to be sent to another person across the network (1971), telnet, a remote connection service for controlling a computer (1972) and file transfer protocol (FTP), which allows information to be sent from one computer to another in bulk (1973). As non-military uses for the network increased, more and more people had access and it was no longer safe for military purposes. As a result, MILnet, a military only network, was started in 1983.

IP software was soon being placed on every type of computer. Universities and research groups also began using in-house networks known as Local Area Networks (LANs). These in-house networks then started using IP software so one LAN could connect with other LANs.

In 1986, one LAN branched out to form a new competing network called National Science Foundation Network (NSFNET). NSFNET first linked together the five national supercomputer centers, then every major university. Over time, it started to replace the slower ARPANET, which was finally shutdown in 1990. NSFNET formed the backbone of what is called the Internet today (Bellis, 2018).

During these first years of increasing information freedom and technology advances several world players shared a contradictory view on the development. On the one hand, information should be freely shared, and shared to all. But on the other hand, information access should be limited and restricted. This contradiction between world players arose because states tried to protect themselves against possible misuse (Powers & Jablonski, 2015). From that moment on innovations and changes occurred quickly. Beginning in 1970, it was made possible to send electronic mail. Apart from the ARPANET, other networks started to emerge. Later on these networks got

connected with each other, creating one ‘internet’. This single network was known as a structure made up of many linked networks, collectively to create the Internet’s backbone (Kelsey, 2008). At this point there was no sign of cybercrimes or cyber-security.

Launched in 1994, Netscape was the first commercial browser. This browser was followed by Microsoft’s breakthrough, the Internet Explorer. With this, the decade of personal computers was born. Several Internet Service Providers entered the market and offered Internet for anyone who had a personal computer and anyone with a connection to a conventional phone line. After the commercialization of the Internet, it grew exponentially. More and more countries entered the Internet world and it became a worldwide phenomenon (Yar, 2013).

The first undertaking of investment in cyber-security occurred during the Cold War era, with nation-states beginning to approach cyber-security as a response to the changing technologies. In order to fully protect themselves against new innovations and weapons of mass disruption, state actors focused for the first time on cyber-security (Kelsey, 2008).

Several attempts have been made to find the starting point of a cyber conflict era. Back in November 1988, Robert Tappan Morris, son of the famous cryptographer Robert Morris Sr. (Bortnik, 2013), was a 20-something graduate student at Cornell who wanted to know how big the internet was – that is, how many devices were connected to it. So he wrote a program that would travel from computer to computer and ask each machine to send a signal back to a control server, which would keep count.

The program worked well – too well, in fact. Morris had known that if it traveled too fast there might be problems, but the limits he built in weren’t enough to keep the program from clogging up large sections of the internet, both copying itself to new machines and sending those pings back. When he realized what was happening, even his messages warning system administrators about the problem couldn’t get through (Kehoe, 1992).

His program became the first of a particular type of cyber-attack called “distributed denial of service” (Guri et al, 2017), in which large numbers of internet-connected devices, including computers, webcams and other smart gadgets, are told to send lots of traffic to one particular address, overloading it with so much activity that either the system shuts down or its network connections are completely blocked.

In many ways, Morris's program, known to history as the "Morris worm," set the stage for the crucial, and potentially devastating, vulnerabilities in what can simply be called the coming "Internet of Everything." Worms and viruses are similar, but different in one key way: A virus needs an external command, from a user or a hacker, to run its program. A worm, by contrast, hits the ground running all on its own. For example, even if you never open your email program, a worm that gets onto your computer might email a copy of itself to everyone in your address book (Shackelford & Bradner, 2018).

In an era when few people were concerned about malicious software and nobody had protective software installed, the Morris worm spread quickly. It took 72 hours for researchers at Purdue and Berkeley to halt the worm. By that time, it infected tens of thousands of systems – about 10 percent of the computers then on the internet (Bortnik, 2013). Cleaning up the infection cost hundreds to thousands of dollars for each affected machine.

In the clamor of media attention about this first event of its kind, confusion was rampant. Some reporters even asked whether people could catch the computer infection (Lee, 2013). Sadly, many journalists as a whole haven't gotten much more knowledgeable on the topic in the intervening decades. Morris wasn't trying to destroy the internet, but the worm's widespread effects resulted in him being prosecuted under the then-new Computer Fraud and Abuse Act[4] (Graham, 2017). He was sentenced to three years of probation and a US$10,000 fine. In the late 1990s, though, he became a dot-com millionaire and is now a professor at MIT.

The internet remains subject to much more frequent and more crippling Distributed Denial of Service (DDoS) attacks[5]. With more than 20 billion devices of all types, from refrigerators and cars to fitness trackers connected to the internet, and millions more being connected weekly, the number of security flaws and vulnerabilities exploded.

In October 2016, a DDoS attack using thousands of hijacked webcams – often used for security or baby monitors – shut down access to a number of important internet services along the eastern

[4] The Computer Fraud and Abuse Act (CFAA) – Title 18 U.S.C., Statute 1030 – is a law designed to address legal and illegal access to federal and financial IT systems. It was intended to reduce cracking of computer systems and to address federal computer-related offences.

[5] Distributed Denial of Service (DDoS) attack occurs when multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource.

U.S. seaboard. That event was the culmination of a series of increasingly damaging attacks using a botnet, or a network of compromised devices, which was controlled by a software called Mirai (Wolf, 2016). Today's internet is much larger (and will continue to grow as figure 1 shows below) but not much more secure, than the internet of 1988.

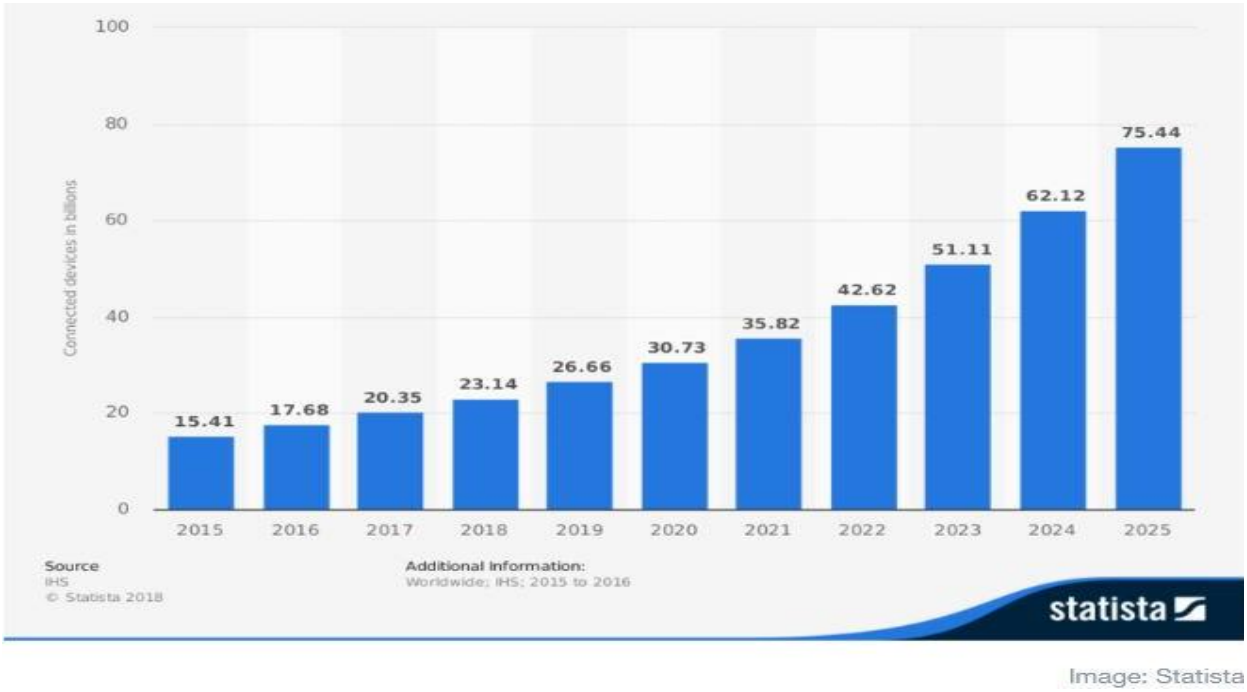


Image: Statista

Figure 1: Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) (Statista, 2015)

Some things have actually gotten worse. Figuring out who is behind particular attacks is not as easy as waiting for that person to get worried and send out apology notes and warnings, as Morris did in 1988. In some cases, the ones big enough to merit full investigations, it's possible to identify the culprits. A trio of college students, for example was ultimately found to have created Mirai to gain advantages when playing the "Minecraft" computer game (Graff, 2017). But technological tools are not enough, and neither are laws and regulations about online activity, including the Computer Fraud and Abuse act under which Morris was charged. The dozens of state and federal cybercrime statutes on the books have not yet seemed to reduce the overall number or severity of attacks, in part because of the global nature of the problem (Fruhlinger, 2018).

Although the Morris worm of 1988 is recognized as the official starting point for the first cyber-attack, a considerable number of authors (Geers, 2014; Kelsey, 2008; Milosevic, 2015; et. al.) have agreed upon the Kosovo war in 1999 as the first internet conflict. This war started in March as an armed conflict between the Federal Republic of Yugoslavia and the Kosovo Liberation Army. The latter received air support from the North Atlantic Treaty Organization (NATO). A pro-Serbian hacker group, named Black Hand, performed several DoS[6] attacks against NATO, the US and the UK. They took down several websites owned by the Kosovo Liberation Army that published propaganda and they took the official website of NATO offline. Several Serbian hackers were also helped by Russian hackers to take down US military and navy websites. After NATO attacked the Chinese Embassy in Belgrade, Chinese hackers joined the group of Serbian and Russian hackers. Although the conflict ended officially in June of that year, several attacks continued in cyber-space (CNN, 1999; Geers, 2014).

Cyber-security[7] has largely come to prominence after big events. There was an exponential change in cyber-security after the events of 9/11. Substantial soft and hard measures have been taken to enable surveillance and control of suspected cyber-dangers to the society. In 2003 President George Bush signed a National Security Directive that was created to develop guidelines for offensive cyber-warfare (Levi & Wall, 2004).

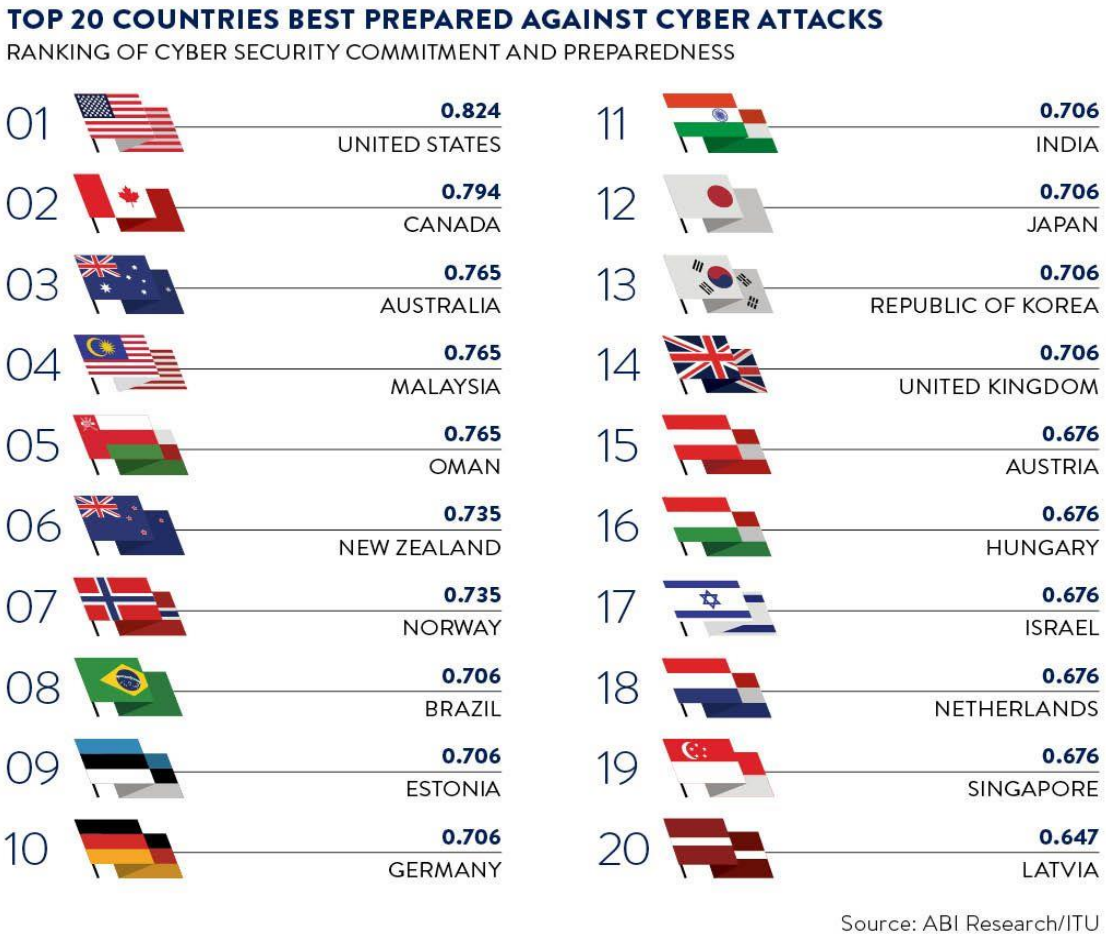
During the last decade more cyber-attacks have been conducted and as a result, a significant amount of state actors has started investing in cyber-security. It must be noted that this process was a very slow and gradual one. It was only with a change in reality was there a change in mind-set. State and non-state actors increasingly got interested in securing cyber and even starting to invest in defense capabilities. During the Warsaw Summit in July 2016, NATO adopted a strategy on its role in the fight against hybrid warfare methods. This is to be implemented in coordination with the European Union (EU). The strategy is meant for the enhancement of their cyber-defense capabilities as well as to counter disinformation. NATO recently even claimed cyber-defense is part of its core task of collective defense (NATO, 2017).

[6] A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.

[7] Cyber security or information technology security involves the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

At this moment the US, China, Israel, Iran, North Korea, the UK and Russia are states in possession of cyber-defense capabilities (Breene, 2016; NATO, 2017; Royal Higher Institute for Defence, 2017). Surprisingly, according to Table 1 published in 2015 on the website of the World Economic Forum, the ten states best prepared against cyber-attacks, with the exception of the United States of America, has none of the above-mentioned states who possess cyber-defense capabilities. This shows again that there is an uncertainty existing around knowledge of cyber-security.

Table 1: Countries best prepared against cyber-attacks (S. Ranger, 2016)



It is clear that the number of cyber-attacks in the world has increased over the years (Kepes, 2016). However, it is very difficult to determine the exact number of attacks, the strength of the security and the impact of defense capabilities. This is because most attacks are never reported and security and capability measurements are not openly shared. Recent studies have shown every state

nowadays gets attacked repeatedly on a daily basis. Individuals or organizations often remain unaware that they have been attacked since the purpose of many cyber-attacks is precisely to hack unnoticeably into computers or systems. There is also an increase in cyber threats because of the further and on-going digitalization of worldwide societies and this also happens in vital sectors. The growth in existing devices and their mutual interconnection makes the world even more dependent on cyber technology. Consequently, society is more vulnerable against cyber threats. However, a worldwide increase of awareness has also led to a need for investment in cyber-security and protection against these cyber threats.

One can implement viruses for example in water devices, infect military equipment, or turn off electricity in hospitals, in the whole world from every given location. The Internet gave the opportunity to think the unthinkable, imagine the unimaginable, do the impracticable and destruct the indestructible. Apart from land, sea, air and space, the Internet has created a fifth military domain: cyberspace. In this domain there are no rules, no policing and no boundaries.

The (spider) web of definitions

When existing research is compared, it is easy to try and visualize the whole cyber-world. The most efficient way to start off is with the concept of cyberspace. Cyber-space is the interdependent network of information technology infrastructures. This includes the Internet, telecommunications networks, computer systems, embedded processors and controllers in critical industries. Cyber-space can be compared to outer space. Both are characterized by an absence of boundaries and regulations. Different sorts of crimes can threaten this cyber-space. Some crimes are more visible than others and some are more destructive than others (Carr, 2009; Office of the National Counterintelligence Executive, 2011).

In this interdependent network several actions can be executed. The least damaging action within this cyber-world is cyber activism. Cyber activism is simply the normal, non-disruptive use of the internet in order to follow or support a certain agenda. Every person who looks something up or who browses the web is at that moment a cyber activist (Denning, 2001). Cyber activism cannot be perceived as a cyber-attack, however.

A Cyber-attack, in contrast, can be described as a malicious and deliberate attempt by an individual or organization to breach the information system of another individual, or organization. These attacks are socially, politically or criminally and financially motivated and carried out through the

cyberspace. The attacks involve the use of networks or information systems, executed on a vast number of potential victims in order to gain unauthorized access, damage and interfere in computer systems and to obtain financial or other advantages (Advisory Council on International Affairs, 2011; Broadhurst, 2006).

Before going deeper into the definition of cyber-attack, it is necessary to discuss first who can conduct a cyber-attack. Political scientist Joseph Nye (2011) makes a rough estimation of who can be an actor in cyber-space. He divides the actors in cyber-space into three categories: governments, organizations with highly structured networks, individuals and lightly structured networks. Regardless, a cyber-attack can be conducted by practically anyone. Someone who has conducted a cyber-attack is commonly referred to as a hacker. Cyber hacktivism is a form of activism where certain targets are attacked through hacking techniques. Hackers are persons who deliberately gain unauthorized access to computer systems. Cyber hacktivism occurs in order to disrupt normal operations but is not meant to cause serious damage or harm. A hacker can work individually or in a group. The most famous hacking group is Anonymous. This hacking group, known for their Guy Fawkes masks used in the movie V for Vendetta, hacks every website or device that is a property of someone or something they don't agree with (Denning, 2001; Furnell & Warren, 1999; Panorama, 2012).

Cyber-attacks can exist in all forms and sizes. The scope of attacks can vary, stretching from hacking into a Facebook account of an ex-boyfriend to conducting an intrusion of a nuclear device. In order to fully understand and imagine what the range of cyber-attacks consists of, the conceptual model a strategic analyst at the Belgian Federal Police, Mrs. Delplace, is useful (Figure 2).

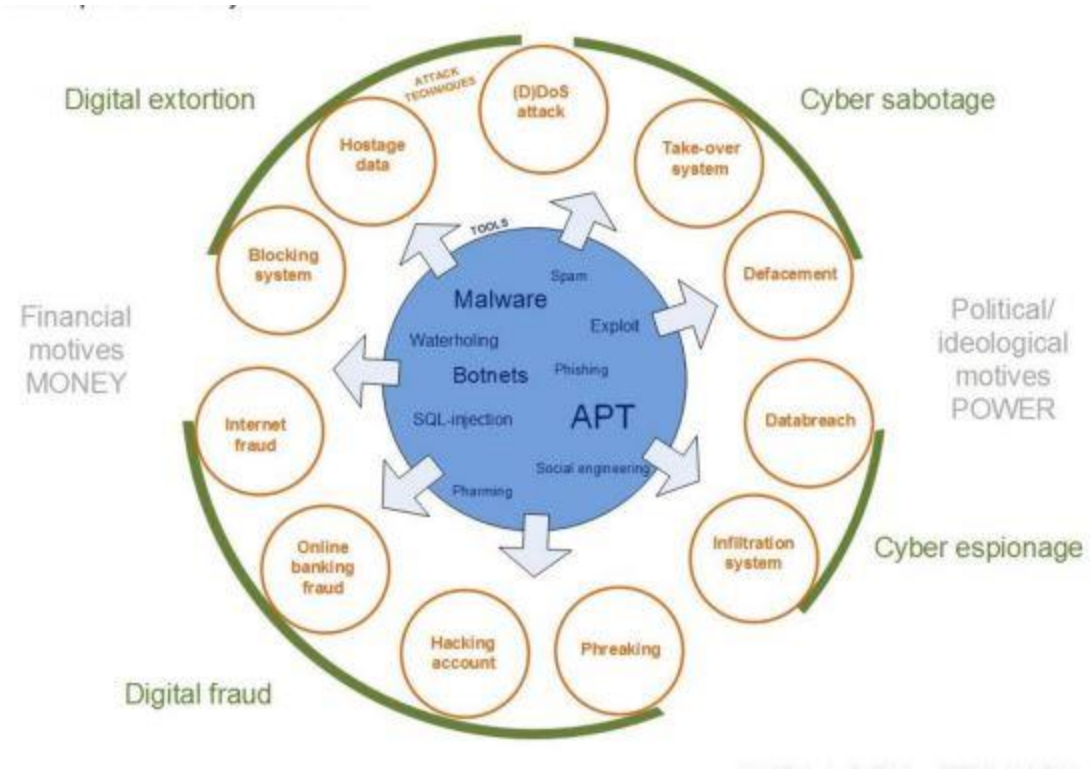


Figure 2: Cyber-attacks (W. Coenraets, 2017)

According to Deplace, there are three different circles, namely the inner, the middle and the outer circle. The inner circle represents the tools, followed by the middle circle representing the techniques, ending with the outer circle representing the goals. On both sides of the circle there are two motives to be found - financial and political. All the following cyber-attacks can be conducted against anyone, which means individuals, companies, governments and critical infrastructure.

Starting at the inner circle, all the tools with which cybercriminals can proceed to conduct an attack are presented. The size of each word represents its importance and frequency. The bigger the word the more frequently they are used, consequently reflecting their level of importance.

Malware, or malicious software, is the most well-known tool. The appearance of malware can be in form of viruses or worms. Another tool is Advanced Persistent Threats (APT). These types of threats are made to conduct a very deep intrusion. They stay as long as possible under the radar in a certain system, in order to collect data and information. Advanced forms of APTs can even adapt themselves to the cyber-environment, meaning that they can remain unnoticed for a longer period.

Botnets are a collection of infected systems that work together to attack a certain device. They are distributed computer platforms that can function like computer robots. They use several types of malicious software programs, such as email viruses, and infect other devices with this infected software.

The above-mentioned tools are the most important ones. With these tools a hacker can proceed to organize an attack. These attacks are all conducted with a certain goal. There are four goals: digital fraud, digital extortion; cyber-sabotage, and cyber-espionage. Reaching one of the stated goals is stimulated by two different motives. The first motive is a financial, where the attackers' main goal is money. Attacks driven by the first motive can have enormous impacts. For example, a recent cyberattack was the Bangladesh Bank heist, where about 100 million dollars was stolen by hackers through a sophisticated cyber-attack on the National Bank of Bangladesh in 2016. Hackers breached the bank's system and used the Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging network to order the transfer of money from the National Bank of Bangladesh to the New York Federal Reserve. For now, the case has not been cracked. However, many are suspicious that help was given by North Korea (Farah, Shojol, Hassan, & Alam, 2016). Although the main plotters of this heist have not been caught yet and nor is there any evidence found of money reaching North Korea, it remains an interesting case. It shows a potential shift to state-sponsored cyber-attacks with a financial motive. The fact that this cyber-attack could have been state-sponsored actually makes the motive unclear. The underlying motive could be more politically tinted (Farah, Shojol, Hassan, & Alam, 2016; Lema & Gopalakrishnan, 2017; "The investigation into the Bangladesh Bank heist continues," 2017).

The second motive for a cyber-attack is political or ideological. Here the attackers' main goal is to obtain power[8]. At the end of 2016 the capital of Ukraine's power grid was hit by a cyber-attack. This left the northern part of Kiev temporarily without electricity. Ukraine started an investigation to find the perpetrators. After tracking down the attack, the Ukrainian government found out it was linked to the Russian intelligence agencies, although it has never been completely confirmed. The investigation of the Ukrainian government unfolded two possible motives behind the attack. One was that Russia had conducted this attack to show off the power of the Russian Federation in order to prove to the people of Ukraine that the Ukrainian government was not able to protect them fully.

[8] Here, the power is political/ideological as its aim is to influence the conduct (behavior) of others.

The second possible motive was that there was something else happening at the same time and that Russia was in need of a cover-up to assist another operation to succeed (Polityuk, 2016). However, both motives are politically steered and are not for the sake of stealing money. The aforementioned cyber-attacks can be achieved by several attack techniques as shown in the middle circle of figure 2 above.

Digital extortion is best explained as hostage data also called ransomware. Ransomware is computer software which uses a method of blackmail. Certain viruses are installed on a computer, the computer programs are blocked and the computer is taken hostage. One can only free the computer by paying money (Benschop, 2017; De Bruycker, 2010; Marjz, 2006; "Ransomware," 2012). In most cases the user of a device receives a message saying it has no access to its data any longer unless it pays a certain amount of money. Once the money is paid the device is to be freed. Sometimes downloading an anti-virus program on a USB stick followed by plugging this stick in the infected device can tackle this problem. But more recent and advanced forms of malware, such as crypto ware, have the ability of encrypting all the files on a device. This means that all the files are locked and cannot be used or touched anymore. Without a decryption key, there is no possibility of unblocking the system. The act of decrypting a virus is complicated and sophisticated that it can take up multiple years of work. For this reason, even ICT experts cannot solve the problem. Thus, if a user has not backed up their files, they lose everything they have unless money is payed to the hackers. Recently a hacker named The Dark Overlord stole the newest season of the popular Netflix-series Orange Is the New Black. This hacker uploaded the first episode of the season to an illegal file-sharing website. The normal release date was set out on the 9th of June 2017. The hacker demanded Netflix pay a modest ransom for additional episodes not to be released. Netflix did not concede and the season was effectively posted online (De Wolf, 2017).

Digital fraud also known as online banking fraud can be summarized as fraudulent online banking activities. These fraudulent activities are becoming more and more sophisticated, threatening the cyber-security and trust of online banking business. The danger of these frauds is that it could affect customers worldwide, as well as other high-profile websites and it can lead to massive losses (Wei, Li, Cao, Ou, & Chen, 2013). Only recently, German hackers exploited a vulnerability in a global telecom network called Signal System 7 (SS7). Several cyber-attackers exploited the Signal System 7 to steal funds from bank accounts. This system helps mobile networks across the world

route calls and texts. This could be done by for example keeping calls connected as users drive on highroads, switching from signal tower to signal tower. It can also be used by hackers to redirect data and they have now found a way to intercept the two-stage authentication codes sent out by banks. These codes are used to verify the identity of customers attempting to log into their accounts or to place online transactions. They are usually sent in the form of SMS messages and by intercepting these codes through the SS7 service, hackers can empty funds from bank accounts (Schwartz, 2017).

Conclusion

Looking at the literature surrounding the domain of cyber, what constitutes a cyber-attack and the forms cyber criminals can take to perpetrate a cyber-attack, it can be deduced that the activities of cyber criminals can, in extreme cases, lead to serious conflict amongst States. This is possible if the services of these hackers are sought after by a nation aiming to promote its self-interest at the expense of another State. As can be seen in the next chapter, cyber, as an instrument in the wrong hands can very well lead to war.

Chapter II

Cyber as a tool for war

Introduction

One of the dominant debates in international relations largely revolves around the concept of cyberwar. For over two decades, the dominant perception has been: "Cyberwar is coming!" To the surprise of scholars familiar with the Realist theory of International Relations, the idea of cyberwar emerged alongside cyberspace conceptualization and then realization. History and philosophy show that scientific developments do not alter human nature enough to eradicate violent conflict. While the potential for using cyberspace in a conflict is obvious, the currently prevailing properties of cyberspace make fundamental concepts of attack, defense, and ultimately war inadequate. However, even experienced defense and IT professionals all too often confuse acts of cyber-crime and espionage with cyberwar. Failing to conceptualize what cyber warfare is and, more importantly, what it is not, skews perception and results in faulty policymaking. It is thus important to turn to a critical examination of the major issues in the cyber war debate.

The unique properties of information and cyberspace make some of the familiar concepts in the cyberwar debate inadequate. This paradoxical state of affairs testifies to the fundamental novelty of cyberspace that renders even millennia-old concepts unsatisfactory. Stuxnet (as will be seen in a subsequent chapter) demonstrated just how sophisticated and precise cyber weapons could be, but to evaluate all cyber weapons' strategic effectiveness according to this specific case assumes too narrow a perspective. Website defacement, distributed denial-of-service (DDoS), massive cyber espionage is labelled "attacks." Some espionage operations often upgraded to the "advanced persistent threat" moniker, and the whole scene is called "cyberwar."

War is a central experience of mankind that always had gruesome properties. "War is an act of force to compel the enemy to do our will." War is a continuation of politics by other means. It consists of several universal elements, famously formulated by Clausewitz. Centrally, war is a violent act, where the threat of force and violence is instrumental to achieving a political goal. Neither denial-of-service, web hacking, nor espionage are even potentially violent, even when Stuxnet is considered, no cyber incident has yet been violent nor caused loss of human life. Tabansky posits that since none of the cyber events have yet met the requirements to constitute a war, the "cyberwar" metaphor should be relinquished, at least for the time being (Tabansky, 2015). This issue is still very much up for debate till date.

This chapter discusses the use of cyber as an instrument in modern warfare. In this case, it explains that cyber should be understood as a tool that conflicting nations use to advance their self-interests. The first section dissects the earliest notion of war and gives meaning to this notion of war through its history. This aim of this history is to help create an understanding of the origin of war and how it has advanced over the years especially when considering the advancement of tools used in prehistoric war down to modern war. This creates a base for understanding the role cyber plays as an instrument in modern war. The second section then examines the Georgian cyber-attacks as a case study to make sense of the use of cyber in warfare. The evolvement, tactics, motives and results are properly analyzed to create a proper understanding of the role cyber played in the Georgia - Russia war.

War and Cyber

The earliest evidence of warfare is traced back to the prehistoric Mesolithic cemetery Site 117, which has been determined to be approximately 14,000 years old. About forty-five percent of the skeletons there displayed signs of violent death (GCHQ, 2019). Since the rise of political entities some 5,000 years ago, military activity has occurred over much of the globe. Aggrieved nation states seeking redress sought the battle field to settle their differences. A lot of money was spent to equip the military with the required tools to be able to withstand the rigors of warfare.

The greatest interpreter of war, Carl von Clausewitz, defined war as:

> *A social activity that involves mobilization and organization of individual men, almost never women, for the purpose of inflicting physical violence. It entails the regulation of certain types of social relationships and has its own particular logic* (Clausewitz, 1989, p. 202).

Today this definition is outdated especially because of the study of the war fought in the cyber domain.

A number of definitions of cyberwar have been proposed, with no single definition being widely adopted. Clarke (2011), defines it as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption (Clarke, 2011). Libicki (2009) defines two types of cyberwar: strategic, and operational. Strategic involves "a campaign

of cyberattacks one entity carries out on another". Operational cyberwarfare involves the use of cyberattacks on the other side's military in the context of a physical war (Libicki, 2009).

With different researchers having differing views of what cyber war entails, what is most common is that nation states are moving away from the physical form of foreign policy relations as it relates to the military. They are leaning towards the cyber domain as a subtler and less expensive form of war.

Can a conventional war be compared to a cyber-war? This is a crucial question in warfare studies. There is an overlap existing between both types when the fundamental elements that construct a war, conflicting actors, weapons and victims, are analyzed. There are also motives and goals involved. Of course, there are differences as well.

Cyberwar capabilities are not only relatively new, when discussing them on their own merits, but they change the way conventional war is carried out as well (Andress & Winterfeld, 2014). Cyber war can have great impact on the way physical war is waged. Given that even strictly physical war, in the sense of boots on the ground, depends a great deal on technologies, these things are vulnerable to cyber-attack. Support for physical operations depends on supplies being delivered properly, soldiers being moved from one place to another on a tight schedule, communications functioning, and any number of other factors. If one or more of these activities does not take place, or, worse yet, is intentionally altered in order to engineer a weakness then physical warfare can quickly degenerate into chaos.

By comparison, cyber warfare activities are very vulnerable to physical effects. If communications lines are severed, power is unavailable, environmental conditions cannot be maintained, or any of a number of other conditions cannot be met then the relatively fragile computer systems and infrastructure become so much dead weight. In either case, conventional war can affect or be affected by cyber-attacks. When the physical component is ignored in cyber war, a large portion of the entire picture is potentially lost. Cyber war is indeed a distinct dimension of warfare, but isolating it from the other dimensions renders its capabilities incomplete, at best.

In as much as the comparison between conventional warfare and cyber warfare throws up contrasting views of the makeup and complexities of both forms of war, what is clear is that cyber war is a new war trend that is fast evolving with the issue of attribution being at the fore front. The

cyber-attacks on Georgia in 2008 is a pertinent case study for analyzing the role cyber plays in conventional war while also analyzing the issue of attribution and how it creates a sort of refuge for conflicting nations.

The Georgia Case

The use of cyber elements such as the DDoS attacks in the 2008 Russia-Georgia war was a direct and well-organized accompanying process to conventional action, aiming to simplify the implementation of military tasks for the Russian armed forces, create an informational vacuum, gain informational superiority and establish the Russian narrative about the conflict. In order to study the transformation of Russian cyber operations in modern conflicts, it is important to reconstruct the nature of the cyber-attacks used in the 2008 Russia-Georgia war, their chronology and the measures aimed at the minimization of their effect.

It is safe to say that tensions between Russia and Georgia spiked as far back as 1991 when the decided to leave the Soviet Union. Back then, Georgian opposition pressure on the communist government was manifested in popular demonstrations and strikes, which ultimately resulted in an open, multiparty and democratic parliamentary election being held on October 28, 1990. They were won by the round table coalition headed by the leading dissident Zviad Gamsakhurdia, who became the head of the Supreme Council of the Republic of Georgia. On March 31, 1991 Gamsakhurdia wasted no time in organizing a referendum on independence, which was approved by 98.9 percent of the votes. Formal independence from the Soviet Union was declared on April 9, 1991, although it took some time before it was widely recognized by outside powers such as the United States and European countries. Gamsakhurdia's government strongly opposed any vestiges of Russian dominance, such as the remaining Soviet military bases in the republic. After the collapse of the Soviet Union, his government declined to join the Commonwealth of Independent States (CIS) (Abkhazia, 1992).

Gamsakhurdia was elected president on May 26, 1991 with 86 percent of the votes. He was widely criticized for what was perceived to be an erratic and authoritarian style of government, with nationalists and reformists joining forces in an uneasy anti-Gamsakhurdia coalition. A tense situation was worsened by the large amount of ex-Soviet weaponry available to the quarreling parties and by the growing power of paramilitary groups. The situation came to a head on December 22, 1991, when armed opposition groups launched a violent military coup d'etat,

besieging Gamsakhurdia and his supporters in government buildings in central Tbilisi. Gamsakhurdia managed to evade his enemies and fled to the breakaway Russian republic of Chechnya in January 1992 (Abkhazia, 1992).

The new government invited Eduard Shevardnadze to become the head of the State Council, in effect, president, in March 1992, putting a moderate face on the somewhat unsavory regime that had been established following Gamsakhurdia's ouster. In August 1992, a separatist dispute in the Georgian autonomous republic of Abkhazia escalated when government forces and paramilitaries were sent into the area to quell separatist activities. The Abkhaz fought back with the help of paramilitaries from Russia's North Caucasus regions and alleged covert support from Russian military stationed in a base in Gudauta, Abkhazia. In September 1993 the government forces suffered a catastrophic defeat which led to them being driven out and the entire Georgian population of the region being expelled. Around 14,000 people died and another 300,000 were forced to flee.

Ethnic violence also flared in South Ossetia but was eventually quelled, although at the cost of several hundred casualties and 100,000 refugees fleeing into Russian-controlled North Ossetia. In south-western Georgia, the autonomous republic of Ajaria came under the control of Aslan Abashidze, who managed to rule his republic from 1991 to 2004 as a personal fiefdom in which the Tbilisi government had little influence.

On September 24, 1993, in the wake of the Abkhaz disaster, Zviad Gamsakhurdia returned from exile to organize an uprising against the government. His supporters were able to capitalize on the disarray of the government forces and quickly overran much of western Georgia. This alarmed Russia, Armenia and Azerbaijan, and units of the Russian Army were sent into Georgia to assist the government. Gamsakhurdia's rebellion quickly collapsed and he died on December 31, 1993, apparently after being cornered by his enemies. In a highly controversial agreement, Shevardnadze's government agreed that it would join the CIS as part of the price for military and political support (Chumburidze, 2010).

Shevardnadze narrowly survived a bomb attack in August 1995 that he blamed on his erstwhile paramilitary allies. He took the opportunity to imprison the paramilitary leader Jaba Ioseliani and ban his Mkhedrioni militia in what was proclaimed as a strike against "mafia forces". However, his government, and his own family, became increasingly associated with pervasive corruption

that hampered Georgia's economic growth. He won presidential elections in November 1995 and April 2000 with large majorities, but there were persistent allegations of vote-rigging.

The war in Chechnya caused considerable friction with Russia, which accused Georgia of harboring Chechen guerrillas. Further friction was caused by Shevardnadze's close relationship with the United States, which saw him as a counterbalance to Russian influence in the strategic trans Caucasus region. Georgia became a major recipient of U.S. foreign and military aid, signed a strategic partnership with NATO and declared an ambition to join both NATO and the EU. In 2002, the United States sent hundreds of Special Operations Forces to assist the local military fight guerrilla fighters. Perhaps most significantly, the country secured a $3 billion project to build a pipeline carrying oil from Azerbaijan to Turkey via Georgia; the so-called "Baku-Tbilisi-Ceyhan" or BTC pipeline (Chumburidze, 2010).

Due to Georgia's starkly pro-Western policies, the Kremlin started preparing a military operation in 2006-2007. The formulation of the mechanisms and the scenario for the cyber-attack probably took place in the same period. Parallel to the large-scale attacks waged by Russian land, naval and airborne forces, a mass DDoS attack was waged against Georgia's communication grids - paralyzing the banking sector, transport companies, telecommunication providers and government websites.

On July 19th 2008, the official website of the President of Georgia went offline for almost 24 hours as a result of a DDos attack. This attack can also be regarded as the main rehearsal of the following mass cyber-attacks. In the same period, Russian actors were constantly scanning Georgian communication grids.

On August 8th 2008, Russian armed forces invaded Georgia after which the main phase of the cyber-attack commenced[9]. There are two phases of the Russian cyber campaign against Georgia.

[9] The websites of the President of Georgia, Government of Georgia, Ministry of Foreign Affairs of Georgia and the Parliament of Georgia as well as informational portals (apsny.ge, news.ge) and non-Georgian yet Georgia-friendly media websites and forums came under attack on August 8.
TBC Bank, which was the largest commercial bank in Georgia at that time, was attacked on August 9.
A new wave of cyber-attacks took place against the Parliament of Georgia and the President of Georgia on August 10.
Most of the governmental websites, excluding that of the President, were not functional on August 11. A defacement attack was undertaken on the President's website on the same day, placing fascist symbols on it, as well as photos equating President Saakashvili with Hitler.

The first phase commenced on the evening of the 7th of August when Russian hackers targeted Georgian news and government websites (Bumgarner & Borg, 2009). A Russian Military Forecasting Center official, Colonel Anatoly Tsyganok, said these first actions were a response to Georgians hacking South Ossetian media sites earlier in the week (Tsyganok, 2008). The fact that the alleged Russian cyber-attacks occurred only one day prior to the ground campaign has led many security experts to suggest the hackers knew about the date of the invasion beforehand.

In the first phase of the attack, the Russian hackers primarily launched DDoS attacks. As noted in Chapter One, a denial of service attack is a cyber-attack that attempts to prevent the legitimate use of a computing resource. When multiple computers achieve this goal, a distributed denial of service attack has occurred. One way to categorize DDoS attacks is to differentiate between semantic and brute force attacks. A semantic DDoS takes advantage of either a feature or bug in some software on the target system. A brute force or "flooding" DDoS attack occurs when the target system receives more internet traffic than it can handle, which exhausts the command and control resources of the server, rendering it unavailable (Mirkovic & Reiher, 2004).

In this phase, the attacks primarily targeted Georgian government and media websites. The Russian botnets relied on a brute force DDoS to attack these targets (Nozario, 2010). The Georgian networks, due to their fragile nature, were more susceptible to flooding than the Estonian networks Russian hackers attacked a year earlier (Bumgarner & Borg, 2009).

Similar attacks were undertaken against the websites of the National Bank and the Ministry of Foreign Affairs of Georgia, placing photos of 20th century dictators there.

It is important to note that those Azerbaijani websites that were covering the conflict objectively, neutrally or in Georgia's favor (www.day.az, www.today.az, www.ans.az) also suffered defacement attacks.

The same was true for Russian opposition websites and personal websites of Russian opposition-minded politicians (http://www.skandaly.ru, http://www.newsgeorgia.ru, http://www.kasparov.ru/).

The DDoS attacks during this phase were also carried out by botnets (Nozario, 2010). A botnet is a group of computers on the Internet (termed "bots" or "zombies") that have been infected with a piece of software known as malware. The malware allows a computer "command and control" server to issue commands to these bots. Often, botnets launch spam email campaigns, but they can also be used to launch wide-scale DDoS attacks. The hijacking of the zombie computers typically occurs in the same manner as infections with other viruses (e.g., email scams, fake websites, infected documents). Communication from the command and control computer to the zombies can be conducted over seemingly innocuous channels on the network (such as a channel normally used for Internet chat) to prevent discovery (Jahanian & Mcpherson, 2005). Criminal organizations, such as the Russian Business Network (RBN), use and lease botnets for various purposes (Carr, 2009). The botnets used in the onslaught against Georgian websites were affiliated with Russian criminal organizations, including the RBN (Corbin, 2009).

In the second phase, Georgian media and government websites continued to receive the attacks, but the Russian cyber operation sought to inflict damage upon an expanded target list including financial institutions, businesses, educational institutions, Western media (BBC and CNN), and a Georgian hacker website (Jahanian & Mcpherson, 2005). The assaults on these servers not only included DDoS, but defacements of the websites as well (e.g., pro-Russian graffiti on government sites such as a picture likening Georgian President Mikheil Saakashvili to Adolf Hitler). In addition, several Russian hackers utilized publically available email addresses of Georgian politicians to initiate a spam email campaign.

To carry out website defacements, the Russian hackers resorted to another type of attack known as an SQL injection[10], which uses a text field on a webpage to communicate directly with the back end database (normally, a common SQL data- base—hence the name). A system susceptible to this type of vulnerability essentially gives the hacker total access to the database, including the list of user login IDs, financial transactions, or website content (Ullricha & Lamb, 2008).

[10] SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.
The impact SQL injection can have on a business is far-reaching. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

During this phase of the operation, much of the cyber activity shifted to the recruitment of "patriotic" Russian computer users, often referred to as hacktivists (Danchev, 2010). According to postings on some Russian hacker websites, many hacktivists were thought to be members of Russian youth movements (Carr, 2009). The recruitment was primarily done through various websites, the most infamous of which was StopGeorgia.ru, which went online on the 9th of August 2008 (Jahanian & Mcpherson, 2005). One hacktivist notes that the instructions provided to the recruited hacktivists were very accessible, even for a novice user (Morozov, 2010). For example, StopGeorgia.ru provided easy-to-use tools and instructions to launch DDoS from private machines. It even featured a user-friendly button called "FLOOD" which, when clicked, deployed multiple DDoS on Georgian targets. Although many of the hacktivist assaults relied on a different weakness than those of the botnet actions, they all aimed to overload Georgian servers by brute force (Bumgarner & Borg, 2009). The tools provided were also very versatile. For instance, some could assail up to seventeen Georgian servers simultaneously. These hacktivist websites also featured target lists of Georgian systems, including specifications on whether it was accessible from Russia as well as the Georgian system's known vulnerabilities. This included susceptibility to SQL injection. It is also noteworthy that some security experts have linked StopGeorgia.ru to Russian organized crime (Carr, 2009).

Another interesting aspect of the Russian hacker websites is their administrators' professionalism. Not only did they provide novice hacktivists with timely advice, they also policed their sites very well. During the conflict, administrators of Russian hacker site XAKEP.ru promptly responded to port scans by the U.S.-based open-source security project called Project Grey Goose by temporarily blocking all U.S Internet Protocol (IP) addresses. This was done to remove any footprints that could be traced back to them. There was also evidence showing that the hackers quickly cleaned up the server, in one instance removing a post containing the keyword "ARMY" in a matter of hours (Jahanian & Mcpherson, 2005). The precautions of the administrators were well founded. One security organization identified a fake tool uploaded to a Russian hacker website described to launch attacks against Georgian targets. However, this particular piece of software turned out to target Russian systems. The experts concluded that Georgian hackers uploaded the software in an effort to launch a cyber counterattack, although there was no evidence that this tool caused significant damage (Bumgarner & Borg, 2009).

The Georgian reaction to the Russian attacks first consisted of filtering Russian IP addresses, but the Russian hackers quickly adapted and used non-Russian servers or spoofed IP addresses. The Georgians then moved many of their websites to servers out of the country (mainly to the United States). Nevertheless, even these offshore servers were still susceptible to flooding exploitation owing to the extremely high volume of the Russian brute force assault (Jahanian & Mcpherson, 2005).

Corbin argues that the goals of the Russian cyber-attacks were to "isolate and silence" the Georgians (Corbin, 2009). The assaults had the effect of silencing the Georgian media and isolating the country from the global community. The reports on the event and the target lists provided on the Russian hacker websites give credence to Corbin's hypothesis. Furthermore, the Georgian population experienced a significant informational and psychological defeat, as they were unable to communicate what was happening to the outside world.

While careful not to attribute the cyber-attacks to the Russian government, the head of the Russian Military Forecasting Center, Colonel Anatoly Tsyganok, describes the Russian cyber campaign as part of a larger information battle with the Georgian and Western media (Tsyganok, 2008). Russian journalist Maksim Zharov describes cyber warfare as only a small part in a larger information campaign that also included bloggers and media outlets (Thomas, 2009). At one point, Russian sympathizers even flooded a CNN/Gallup poll with over 300,000 responders stating that the Russian cause was justified. Many analysts believe that the primary goal of the first phase of the Russian CNA was to prevent Georgian media from telling their side of the story. This seems to align with the Russian emphasis on information warfare (Corbin, 2009).

Isolating Georgia from the rest of the world may also explain the attacks on Georgian banks that occurred during the second phase of cyber operations. At this time, several banks were flooded with fraudulent transactions. International banks, wanting to mitigate the damage, stopped banking operations in Georgia during the conflict (Corbin, 2009). As a result, Georgia's banking system was down for ten days (Bumgarner & Borg, 2009). This also led to a shutdown of cellphone services in the country, further isolating Georgia from the rest of the world (Corbin, 2009). Russian hackers targeting Georgian business websites, also during the second phase, may have aimed to cause similar economic damage.

The objectives of "isolate and silence" were limited in scope. They avoided doing permanent damage to Georgian networks and to Supervisory Control and Data Acquisition (SCADA)[11] targets (Bumgarner & Borg, 2009). SCADA systems are designed for real-time data collection, control, and monitoring of critical infrastructure, including power plants, oil and gas pipelines, refineries and water systems (Fernandez &Fernandez, 2005). Obviously, disruption to these systems would have serious implications for the Georgian infrastructure. Since the Russian hackers most likely had the capability to attack these targets, it is reasonable to assume they exercised some restraint to make sure they did not harm them. Further, Georgia's physical connection to the internet remained largely unaffected. At the time of the attacks, Georgia connected to the internet by landlines through Turkey, Armenia, Azerbaijan, and Russia. No evidence points to an attempt to sever these connections in either the physical or virtual world including the connections running through Russia (Zmjewski, 2010). This could suggest that the Russian aggressors did not intend to inflict permanent damage on Georgia's internet infrastructure, but rather to target particular servers to meet their "isolate and silence" objectives.

As wars historically go, the Georgian-Russian cyber war was not very big as it did not involve vast amount of military forces, nor did it last very long. But what cannot be take away from this conflict is the intent from the Russians to use cyber as a tool to perpetrate actions which were detrimental to the policies of the Georgian nation.

Conclusion

Unsurprisingly, Russia denied any involvement in these cyber-attacks on Georgia. This is somewhat telling that Russia still denies involvement in the cyber domain while being very obviously involved in an open conflict with Georgia. Some of the cyber-attacks that occurred, to

[11] **Supervisory Control and Data Acquisition** (**SCADA**) is a control system architecture that uses computers, networked data communications and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controller (PLC) and discrete PID controllers to interface with the process plant or machinery. The use of SCADA has been also considered for management and operations of project-driven-process in construction

The SCADA concept was developed as a universal means of remote access to a variety of local control modules, which could be from different manufacturers allowing access through standard automation protocols. In practice, large SCADA systems have grown to become very similar to distributed control systems in function, but using multiple means of interfacing with the plant. They can control large-scale processes that can include multiple sites, and work over large distances as well as small distance. It is one of the most commonly-used types of industrial control systems, however there are concerns about SCADA systems being vulnerable to cyberwarfare/cyberterrorism attacks.

include the defacement of the Parliament websites, were prepared years in advance. This is not the planning of a fair-weather hacker getting in on the fun of a Russian conflict. The question then becomes, what is more likely: Russia utilizing a cheap, effective means of attack that it is perfectly capable of using in an open war against Georgia, or that a large band of disorganized Russian armature hackers planned years in advance to attack Georgia via cyber in a way that coincided perfectly with Russian operational and tactical objectives? Russia undoubtedly wishes to keep its capabilities in the cyber domain "off the radar," but it is at best naïve for Russia to continue to deny any involvement in said attacks.

Chapter III

Cyber as Tool for Influencing the Policy of another State

Introduction

Every State seeks to achieve autonomy in decision making especially when it concerns the policy making process. As much as these states strive to protect authority and keep foreign influence away, it is almost impossible to guarantee that foreign nations, especially those with peculiar motives, would avoid attempting to make a play to influence the internal policies of other states when possible. This chapter discusses the role cyber plays as a tool states use in attempts to influence the foreign policy of other states. The Estonia v Russia conflict is used as a case study because of the nature of activities Russia used to influence the internal policies of Estonia to suite its self-interests. The question of attribution in this case is also interesting especially as it is a common characteristic of cyber when used as a tool in foreign policy relations.

Nation-state political influence activities can be understood as coordinated and deniable activities that are initiated by a state actor and which are aimed at influencing decisions, perceptions, the behavior of political leaders, the population or particular target groups (such as experts and the media) with the objective of achieving the state actor's foreign policy objectives, often with actions tailored for the purpose that is being pursued. These actions can come in various forms especially with the help of foreign policy instruments. Several foreign policy instruments can be used by one nation state to influence the manner in which other nation states take their decisions. Arguably, the most dominant foreign policy instruments which nation-states use is economic instruments with foreign aid and foreign economic policy prominent. These foreign policy instruments are primarily meant to be used in a non-coercive manner especially dedicated to human, economic and social development but is now often used coercively by the establishment to link the reception of aid and certain policy objectives of the donor to which the recipient should contribute and by the threat of discontinuing the supply of aid if such foreign policy objectives are not met by the recipient of the aids. As Hill (2003) rightly posited, foreign aid has been often used to support ideologically closed regimes that have often used that aid to repress their population or enter into aggrieved militarist policies towards other states.

As much as the above-mentioned foreign policy actions may seem effective in getting one nation state to do the bidding of another nation state, but traditional tools leave traces of attribution. This,

thus, defeats the purpose of anonymity. Cyber as a tool of influence presents a viable solution to this problem.

One of the main attractions of cyberspace is the shield of anonymity it offers, at least in the short term. Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity. In the case of suspected state-sponsored actions, it is difficult to establish beyond any doubt that the order to attack originated in the executive, or presidential office, let alone a capital city. Further, the difficulties of attribution allow a degree of plausible deniability. Perpetrators can cover their own tracks and implicate others, particularly when third-party servers and botnets in unrelated countries can be used to originate attacks and provide cover for the actual attacker.

Cyber influence is designed to create the sense of a momentous strike without actually executing one. In this case, it gives the perception of a possible imminent attack but only with the purpose of influencing the target state to act in favor of the state exerting such influence. Cyber influence attacks are meant to instill a sense of insecurity and a lack of control, compromising sovereignty with an inability to safeguard a normative way of life. Examples of such attacks include crippling government sites, sending damaging messages to civilians and shutting down media sites for limited stretches of time (Assaf & Siboni, 2016).

Cyber is not only used to instill a sense of insecurity, It is also an attempt to disrupt the opponent's information environment by striking their cyber information infrastructure. These activities are mounted against computer systems designed to impact the target population's access, behavior and decision-making processes by controlling information distributed through these systems. This category of attacks includes distributed denial-of-service attacks (crashing a particular site by flooding it with information, or DDoS attacks), exposing the classified/ personal details of an organization or of individuals by publishing confidential documents and hacking into information systems, as well as more sophisticated and strategic attacks on critical infrastructure core operational systems (Brangetto & Veenedaal, 2016).

Cyber allows the state actor of interest to exert its influence on another state, achieving its aims and all the while leaving no room for direct attribution. The Russia-Estonia case is a typical case study.

The Background to the Estonia Case

Introduction

Russia's dispute with Estonia entails two elements; the issue of the border between Russia and Estonia and Estonia's decision to move the statue of a Russian war-hero to a new location. The first element deals with issues of territory. Territorial issues between Estonia and Russia have long clouded Estonia-Russia relations. After the dissolution of the Soviet Union, Estonia had hoped for the return of more than 2,000 square kilometers of territory annexed to Russia after World War II in 1945.

After the collapse of the Russian Empire due to the October Revolution, the territorial delineation between Soviet Russia and the newly independent Estonia was determined by the 1920 Tartu peace treaty[12]. On the onset of World War II, Estonia was annexed by the Soviet Union in the form of Estonian SSR, as part of the overall occupation of the Baltic States. Soon it was overtaken by Nazi Germany and re-occupied by the Soviet Union for the period of 1944–1991.

After Estonia regained its independence from the Soviet Union following the Singing Revolution[13], Estonian and Russian negotiators reached a technical agreement on the Estonia–Russia border in December 1996, with the border remaining substantially the same as the one drawn by Joseph Stalin in 1945, with some minor adjustments. The border treaty was initialed in 1999.

On May 18, 2005, Estonian Foreign Minister Urmas Paet and his Russian colleague Sergei Lavrov signed in Moscow the "Treaty between the Government of the Republic of Estonia and the Government of the Russian Federation on the Estonian-Russian border" and the "Treaty between the Government of the Republic of Estonia and the Government of the Russian Federation on the Delimitation of the Maritime Zones in the Gulf of Finland and the Gulf of Narva". The Riigikogu (Estonian Parliament) ratified the treaties on 20 June 2005, with a reference to the

[12] The Tartu Peace Treaty (Estonian: *Tartu rahu*, literally "Tartu peace") or Treaty of Tartu is a peace treaty between Estonia and Soviet Russia signed on 2 February 1920, ending the Estonian War of Independence. The terms of the treaty stated that *"Russia unreservedly recognizes"* the independence of the Republic of Estonia *de jure* and renounced in perpetuity all rights to the territory of Estonia. Ratifications of the treaty were exchanged in Moscow on 30 March 1920. It was registered in *League of Nations Treaty Series* on 12 July 1922

[13] The **Singing Revolution** is a commonly used name for events between 1987 and 1991 that led to the restoration of the independence of Estonia, Latvia, and Lithuania. The term was coined by an Estonian activist and artist, Heinz Valk, in an article published a week after 10–11 June 1988, spontaneous mass evening singing demonstrations at the Tallinn Song Festival Grounds.

1920 Tartu Peace Treaty in the preamble of the ratification law, placing the new border treaty in the context of internal Estonian law as amending the original 1920 border objected by Russia (Wayback, 2009). The President of Estonia, Arnold Rüütel proclaimed the treaties on June 22, 2005.

After yet another attempt at signing a border treaty in 2005, the border conflict between Estonia and Russia preserves the traditional territorial dimension, rather its aspects are associated with borders as social processes, such as controversial identity building practices, that have been responsible for the construction of Estonia's and Russia's subject positions as incompatible. The enthusiasm and solidarity across ethnic and administrative divides that marked the break-up of the Soviet Union proved to be short-lived and by 1992/1993, it gave way to more exclusive and antagonistic state and national identity building (Paasi, 1999).

With half-a-century of Estonia's history denied legitimacy, the restoration of Estonia's independence was viewed as a return to the status quo ante, including the borders of the inter-war Estonia defined by the 1920 Tartu Peace Treaty with Soviet Russia. Being the first international treaty concluded by the newly independent state, the Tartu Peace Treaty is often regarded as Estonia's birth certificate and is considered indispensable for Estonia's political and national identity, and not just in historical terms: one Estonian MP referred to the Tartu Treaty as regulating Estonian-Russian relations in the present tense as recently as January 2005 (Lukas, 2005).

The current de facto border or, as the Estonian state border law defines it, 'control line', between Estonia and Russia, however, runs well west of the 1920 borders, following the boundary drawn in the course of Stalin's 1944/1945 administrative reform after Estonia's incorporation in the Soviet Union. Thus, the problematic nature of the Tartu Peace Treaty as an important identity marker becomes evident given that it entails Estonia's territorial claims to Russia. But far more important than the territorial issue which was dropped from border negotiations in 1995 for Estonia's identity is the recognition of its political continuity from the interwar state embodied in the Tartu Treaty and of the historical injustice that it suffered at the hands of the Soviet Union (Ilves, 1998).

For Russia, the full extent of Estonia's political insecurity is difficult to fathom, and yet Russia itself has been drawn into the logic of identity conflict. Whereas the objective importance of the entire set of issues in its relations with Estonia is relatively insignificant on the scale of problems

Russia faces at its borders with other neighboring countries, Estonia's provocative rhetoric and behavior often receive disproportionate attention in the media, fueling the feelings of offence among the population and sustaining the perception of inexplicable hostility that Estonia nurtures towards Russia.

The closing of the border in 1994, despite the fact that it was done on Russian President Yeltsin's initiative (Berg and Oras, 2003), caused immense irritation among the inhabitants of Russian regions adjacent to Estonia, which was actively stimulated by Russian federal and regional-level politicians. Most crucially, however, both public and political discourses in Russia indicate immense difficulties in coming to terms with the fact that a country of such insignificant size and standing as Estonia can even begin to formulate an independent foreign policy of its own that is divergent from, and sometimes in direct opposition to, Russia's interests (Tüür, 2005). Although there are objective reasons for Russia's intransigence with regard to the issue of the 1920 borders, they often become overshadowed by identity-driven reasoning.

Thus, not only did Russia refuse to recognize the 1920 border with Estonia, as a further impingement on its shrinking territory, and question the Tartu Peace Treaty as a basis for the present-day bilateral agreement, given that many other historical treaties would favor Russia considerably more; it also persistently resisted any mention of the Treaty in the new border agreement, fearing that an indirect recognition of one historical injustice will set a dangerous precedent for border negotiations with Russia's other neighbors. Russia has also resisted Estonia's claims to its former territory on ethnic grounds. The present border runs across the area populated by the Seto, a distinct Finno-Ugric ethnic group Estonia considers part of its nation (Nikiforova and Viktorova, 2001), whereas the Tartu Peace Treaty border is narrated as the eastern border of Setomaa (Seto-land). Countering this claim, Russia has attempted to 'appropriate' the Seto as part of its own cultural heritage by playing a better 'ethnic patron' to them, and to highlight how much the contested borderlands belong to Russia by narrating Pskov region and the contested Petseri/Pechory district as sites of crucial events in Russian history. However, the Seto political narrative and enactment of Seto identity aligns far better with Estonian geopolitical interests, and Estonia remains an uncontested gateway for Seto political activism (Makarychev, 2004).

The second element emerged in 2007 when the Estonian parliament accepted the Military Graves Protection Act of the Geneva Conventions of 1949; an international agreement which protects

victims and graves of armed conflicts. After its adoption, the Estonian government decided to transport one of the Russian or Soviet-related statues to a different location. The reason given for the relocation were that the site of the statue was unsuitable, and that the statue created a divisive public interest which did not ensure peace for Estonians. Moving the statue was seen as an offense by the Russian Government as dishonoring the Russian soldiers who died in World War II. After this event, the Russian-speaking minority in Estonia were encouraged by Russian state sponsored TV channels to lend their voice to the perceived injustice and prevent the horrible actions of the Estonian government (Sinisalu, 2008).

On the day the statue was moved, later called the Bronze Night event[14], street riots occurred in central Tallinn, as well as in the city of Jõhvi north-east of the country. About hundred people were injured and one person died during the riots, while the police arrested 1300 people. It also generated a serious political crisis between Russia and Estonia. Russia denied any involvement in the riots.

Estonia in 2007 was regarded as the most advanced nation in digitization and internet penetration in Europe (Czosseck, 2013). The country's territory was 98 percent covered with internet by different means. Estonia's economy relied on all its ICT sectors such as e-government, e-banking, e-media and mostly interestingly e-voting service which made Estonia the first in the world to implement online voting for parliamentary elections. According to some numbers, 99 percent of banking transactions were made through online banking (Czosseck, 2013). With the introduction of these services on the internet, the country also became susceptible to cyber-attacks.

The attacks

The attacks started on Friday the 27th of April, 2007 with strikes against several websites of the Estonian government and government agencies. This initial attempt was quite simple. It used ping flooding[15] to consume all the resources of the target machines to bring them down. Through some

[14] Bronze Night: the name came from moving the Bronze Soldier statue from Tõnismägi area to the Soviet soldier's cemetery in Tallinn - capital of Estonia

[15] Ping flood, also known as ICMP flood, is a common Denial of Service (DoS) attack in which an attacker takes down a victim's computer by overwhelming it with ICMP echo requests, also known as pings.
The attack involves flooding the victim's network with request packets, knowing that the network will respond with an equal number of reply packets. Additional methods for bringing down a target with ICMP requests include the use of custom tools or code, such as hping and scapy.

Russian internet forums, several requests to the Russian internet users were made to launch ping flood attack containing a huge pay load in the ping request (Ottis, 2016).

After sometime, executable batch files were created for users to simply download and run them to launch the attack and also IRC chat relays were used for the same purpose. According to Ottis (2016), around 3700 distinct IP addresses were found from the batch files after the attack. Out of these 3700 IPs, 2900 were from Russia, 200 from Ukraine, 130 from Latvia and 95 from Germany.

By Monday the 30th, there were attempts to halt the entire public sector communication network. Tuesday and Wednesday, the 1st and 2nd of May, saw three larger scale attacks, the last of which occurred at 1 AM on Wednesday night, after which the volume of the attacks became steady (Tikk et al, 2010).

On Thursday the 3rd of May, attacks against government and government agency websites, especially large-scale DDoS attacks, continued, but they were accompanied by attacks against Estonian media outlet and private enterprise websites. There was also an increase in the amount of spam email[16]. These attacks continued in relatively similar fashion with a small dip seen on Saturday and Sunday the 5th and 6th of May. On Tuesday the 8th of May, a larger and longer attack mainly against government websites and communications networks were carried out. It was believed that traffic targeting governmental institutions was almost 400 times higher than the normal traffic and was generated from outside Estonia. It was also reported that some Russian hackers managed to hack gradually the Estonian Reform Party's website and placed an official apology (in the Russian language) as it was undersigned by Andrus Ansip, the Estonian Prime Minister. (Tikk et al, 2010).

On Wednesday and Thursday, the 9th and 10th of May, attacks against both private and government websites appeared to try to block the communication between Estonia and the outside world. On the weekend of 12th to 13th of May, the volume of the attacks subsided again (Tikk et al, 2010).

This strains both the incoming and outgoing channels of the network, consuming significant bandwidth and resulting in a denial of service.

[16] Spam email, also known as junk email, is unsolicited messages sent in bulk by email (spamming). The name comes from Spam luncheon meat by way of a Monty Python sketch in which spam is ubiquitous, unavoidable, and repetitive.

On Monday the 14th of May, there was a large-scale attack against SEB Eesti Ühis bank, the second largest bank in Estonia. By midnight of Wednesday 16th of May the volume of attacks had lowered to the same level it was on the weekends. The attacks finally died down on Friday the 18th of May, overall lasting for twenty-two days (Tikk et al, 2010).

The cyber terror attack on Estonia was more than just a temporary nuisance. Rather, it was a mild version of a new form of digital violence that could halt public services, commerce, and government operations. Estonian Defense Minister Jaak Aaviksoo observed that successful cyber-attacks "can effectively be compared to when your ports are shut to the sea" (Ruus, 2008). A blockade is a fitting analogy, as future cyber-terrorist attacks may disrupt a country's water and electricity supplies, as well as telecommunications by severing its connections to the world, and national defenses.

The seriousness of the attacks on Estonia generated a rapid international response. Estonia had few formal cyber-defense preparations outside of its framework for countering traditional acts of terrorism, (Sieber & Bruust, 2007). The government Computer Emergency Response Team (CERT) sought Finnish, German, Israeli, and Slovenian assistance to restore normal network operations (Ruus, 2008). NATO CERTs provided additional assistance, while the EU's European Network and Information Security Agency (ENISA) offered expert technical assessments of the developing situation. Further, a high level of intelligence sharing took place among western countries during the crisis. While Russian-speaking hackers employed the internet as a weapon and tool of mobilization, Estonia and its allies used digital networks to counter successfully the attacks.

Aftermath

During and after the DDoS strikes, NATO and EU member states began to debate new directions for cyber security and appropriate punishments for states found to have engaged in digital warfare. Sanctions were one punishment option that received fairly widespread support. Additionally, one German official even recommended that NATO consider extending its Article 5 security guarantees to the realm of cyberspace (Lewis, 2009). At its Bucharest Summit in April 2008, NATO adopted a unified Policy on Cyber Defence and created the Brussels-based Cyber Defence Management Authority (CDMA) to "centralize cyber defense operational capabilities across the

Alliance" (Hughes, 2008). In August 2008, Tallinn became home to the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE); the Atlantic Alliance's cyber-security headquarters. On the EU front, in November 2010, the organization released its Internal Security Strategy, which called for integrated responses to cyber-security threats and significant expansion of ENISA's duties beyond its previously limited analytical role (European Commission, 2010).

Beyond these efforts, throughout 2010 and in the early months of 2011, both organizations announced a series of concrete long-term plans aimed at countering cyber-attacks. The EU's new Digital Agenda for Europe revealed plans to establish CERTs for EU institutions, hold multinational cyber-defense simulations, and create a joint European cyber-crime platform (Ibid, 2010). NATO adopted a new Strategic Concept in Lisbon in November 2011, which indicated that the alliance would take steps to develop strong, integrated internet defense capabilities (NATO, 2010). To that end, General Stéphane Abrial, head of NATO's Allied Command Transformation, confirmed that the NATO Computer Incident Response Capability Technical Centre (NCIRC TC) in Mons, Belgium would become operational in 2012 (Abrial, 2011). These EU and NATO actions are indicative of the growing recognition of the severity of today's digital threats. As U.S. Deputy Secretary of Defense William Lynn warned when discussing NATO vulnerabilities in light of the Estonian case, "The potential exists for capabilities that are much more destructive…We're largely in the exploitation/denial phase, but history will tell you that somebody will take it to the extreme" (Garamone, 2011 pg 102).

The multinational responses to the 2007 attacks on Estonia indicated that countries would not remain detached and complacent as states or non-state actors threatened the sovereignty of their allies by using cyber as a tool of influence. Still, it is important to note that the international response to the events in Estonia occurred within the confines of preexisting security communities. At a minimum Russia tolerated and encouraged the cyber-attacks, and the Kremlin may have even colluded with the hackers responsible for the strikes. China addressed the matter as an internal Estonian security dilemma and eschewed involvement in the resultant international cybersecurity discussions. Regardless of any secret complicity or participation in the Estonian cyber-attacks, Moscow and Beijing surely analyzed the situation, assessed Tallinn's vulnerabilities and western responses, and improvedage upon their own cyber-warfare capabilities and strategies as a result.

The underlying reason for the attack on Estonia was not unconnected to the decision of the Estonian government to relocate a statue of a Russian Soldier from a square in the capital city of Tallinn to a more secluded location. But in all truth, it was more than that. One of the main aims of the attack was to unite the Russian people against a common enemy which in this case were the Estonians. This probably holds true considering the bad blood that had been building up between both nations since the fallout from the earlier treaty between both nations. It appeared that Estonia had never completely accepted the Russians due the boundary issues between both nations.

Another reason for the attack was to destabilize Estonian society and to undermine the Estonian economy in an effort to weaken its ties to the European Union and the North Atlantic Treaty Organization. Yet another is a proof of concept on the digital people's war idea while supporting the overall political campaign surrounding the statue.

Even though EU and NATO technical experts were unable to find evidence of Russian involvement in the Estonian cyber-terror incident, it certainly would have been in Moscow's interests to organize DDoS strikes. After the movement of the Bronze Soldier and clashes between police and demonstrators, Russian officials accused Tallinn of human rights violations and demanded that Prime Minister Andrus Ansip apologize and resign from office (Terlikowski, 2007). While Russia categorically denied any involvement in the attacks, one unnamed NATO official did not mince words: "I won't point fingers. But these were not things done by a few individuals. This clearly bore the hallmarks of something concerted" (Ruus, 2008 pg 76). Because of economic interdependence and the threat of nuclear escalation, Russia cannot risk attacks on NATO member states, (Keohane & Nye, 1987) perhaps making un-attributable cyber strikes an attractive alternative. In addition to the fact that NATO's conventional military forces significantly outnumber those of the Russian Federation, (International Institute for Strategic Studies, Military Balance, 2010) Estonia serves as a key transit country for Russian oil and natural gas supplies to Central and Western Europe. For all the rhetoric about Russia's coercive energy politics, Moscow exports over 90 percent of its gas and oil to Europe, (Stent, 2008) fostering a situation of mutual economic interdependence. A conventional Russian attack on Estonia would trigger a NATO Article 5 response and could compromise the energy wealth that has led to growing Russian influence on the international stage. In a world of deterrence and interdependence, virtually

untraceable digital displays of force could allow states to subvert the constraints of the international system.

While one may never know the true extent of Kremlin involvement in the cyber-attacks on Estonia, it is clear that Russian officials encouraged the hackers by accusing Tallinn of altering history, perpetrating human rights violations, and encouraging fascism. The Russian authorities also turned a blind eye as pro-Kremlin activists blockaded the Estonian embassy in Moscow for days. Although it would have served Russian national interests to test Moscow's cyber-war capabilities on Estonia, the general consensus among experts is that sophisticated "hacktivists" in Russia and possibly throughout the global Russian diaspora perpetrated the attacks. The alarming reality of the situation is that, in the cyber domain, computer-savvy individuals can now threaten the sovereignty of nation-states, oftentimes from the comfort of their own homes.

Conclusions

In all, it can be argued that Russia's motives of creating a sort of imbalance in the Georgian federation due to the relocation of the statue may have been fruitless. This is arguably true since Estonia did not return the bronze statue to its previous location even after the numerous cyber-attacks it suffered on its infrastructure. What is certain though is that Estonia emerged from this incident better than before.

Chapter IV
Cyber as internal interference

Introduction

Cyber interference involves a particular State meddling in the internal affairs of another State. Attempts to interfere are not new, nor is cyber interference per se. The former concerns attempt by foreign governments or their proxies to exert inappropriate influence on, and to undermine the sovereignty of institutions and the decision-making of nation-states. Such attempts at foreign interference are part of a wider global trend that has affected other democracies. Foreign interference shapes the actions of decision-makers and public opinion to achieve an outcome favorable to foreign interests.

The latter, on the other hand, as seen in the US general election case study, is distinct from general cyber-attacks in the nature of the target, the nature of the attack, the nature of the damage and the lack of an appropriate remedy, either in international law or domestic law. This chapter discusses cyber with respect to election interference. The first section makes a clear distinction between the concepts of conventional cyber-attacks and cyber interference. The second section narrows the narrative to cyber as involved in election interference with Russia's perceived involvement in the 2016 US general elections as a case study.

Often cyber-attacks have functioned much like a kinetic attack. A state has used lines of code to damage, destroy, or cause to malfunction a piece of equipment in another state for the attacking state's benefit. Some of these benefits have been out of military necessity. For example, the alleged United States hack of the Iranian centrifuge system in order to secure more time to negotiate a nuclear agreement favorable to U.S. interests (as discussed in depth in a subsequent chapter). Other cyber-attacks have targeted private corporations as petty punishment. For example, North Korea's efforts to hack and destroy the Sony computer system in order to gain personal retribution for the release of a film offensive to North Korean leaders.

Cyber interference is distinct, however, in at least two ways. First, the targets are publically (owned by the state or government), not privately owned. As such, any attack on an arm of the state raises questions about violations of sovereignty, both in the abstract, nature-of-a-state sense, and in the concrete violations of borders sense.

Second, and distinctly, some of the targets are not computers. They are citizens. Unlike in the Sony or Stuxnet hack, the intrusive piece of data is propaganda, designed not to affect computer systems, but rather individuals. Information, whether true of false, is released to make citizens of a sovereign state function differently, and thus damage the state. It is the intimate target of cyber interference in elections, touching the state's apparatus and its citizens, that makes it distinct from other forms of cyber-attacks.

Cyber election interference shares some traits to other commonly known cyber-attacks. However, it is distinct in one substantial way. Cyber interference in elections constitutes not only hacking, but also information campaigns. The majority of cyber-attacks that states have faced in the past have largely involved kinetic damage to a particular physical asset. It becomes more complicated when the hearts and minds of civilians are targeted by another state's cyber operations.

Cyber election interference does share similar characteristics to other cyber-attacks, though the stakes appear to be higher in the election context. The stakes appear to be higher because a state's foreign and economic polices depend on the integrity of its electoral process. Any compromise of this process could have detrimental effects moving forward. Cyber-attacks are generally not visible, which generally raises concerns both about identifying the attack close to the moment in time that it occurs, and correctly attributing the attack to the attacker, in order to exact punishment and demand recompense.

Being blind to the moment of the attack and the identity of the hacker raise particular concerns in the election context. First, because elections are held at a particular moment in time, identifying security breaches and improper influences as close to the moment of their introduction is critical to ensure election integrity. A later identification of the problem has the potential to provoke a crisis of constitutional proportions. For example, a belated announcement that votes were improperly tabulated, and the victory should have been given to another candidate would raise questions even larger than those of Bush v. Gore[17] (Newman, 2016).

[17] ***Bush v. Gore***, 531 U.S. 98 (2000), was a decision of the United States Supreme Court that settled a recount dispute in Florida's 2000 presidential election. The ruling was issued on December 12, 2000. On December 9, the Court had preliminarily halted the Florida recount that was occurring.
In a *per curiam* decision, the Court ruled that the use of different standards of counting in different counties violated the Equal Protection Clause, and ruled that no alternative method could be established within the time limit set by Title 3 of the United States Code (3 U.S.C.).

Second, the thorny issue of identification of hackers becomes even more concerning in the international context. To the extent that international law does speak to cyber election interference, states cannot either exact retribution or ask for reparations without a clear idea of both who the actor is, and whether the actor was under state control. Neither of those factors are clearly visible in the cyber election interference context, but the stakes are higher as the consequences for election interference may be higher than those of a hack in the private sector.

Unlike an attack such as Stuxnet, the scope of the damage from cyber election interference has the potential to be unquantifiable. Contrast this to the situation in Stuxnet, where the damage was confined, at least originally to the Iranian nuclear program centrifuges. The scope of cyber election interference, however, has the potential to be far broader. A hack of state voting systems might be bounded to the physical computer systems, but the dissemination of fake news to influence citizen votes, however, is difficult to map or quantify. Moreover, cyber interference in the election process, once known, has the potential to undermine citizen confidence in the democratic process and in the integrity of their government. Cyber election interference keeps citizens from being able to meaningfully participate (due to voter apathy) in their chosen form of government. If citizens are not able to participate meaningfully in a democratic government, democracy itself is threatened.

Both hacks on public apparatus and attacks on citizens raise substantial questions and justifiable concerns about improper intrusion into objects, and subjects of state power. When these kinds of questions are raised in the physical world, states do not hesitate to go to war to protect such critical targets. It is by the same logic that similar arguments are raised in the context of cyber election interference. Yet international law does not permit sovereigns to lawfully use force in response to such intrusions[18]. The lack of a remedy has the potential to motivate states to use force unlawfully, or else stretch existing international law to places where it does not naturally, or justifiably, extend.

2016 Attack on the US Election

[18] See UN article 51: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

The best example of cyber interference is Russia's meddling in the 2016 U.S. election. As of the time of this writing, reports analyzing the hack have indicated that Russia interfered in four major ways: through information theft, selective dissemination of information, a propaganda campaign against Hilary Clinton, and efforts to hack into voting systems across the country.

Russia used various cyberespionage teams to hack into computers and email systems in the 2016 U.S. election. Additionally, it is known that Russian cyberespionage teams took some of the information it found in these computers and systems, because some of the information and emails it discovered through unauthorized access were later published.

A Russian cyberespionage team, colloquially known as "Cozy Bear" or "A.P.T. 29," hacked computers at the Democratic National Committee and penetrated the email account of Clinton's presidential campaign chair, John Podesta (Forcese, 2016). Russia also hacked the Republican National Committee emails using a Russian unit called "Fancy Bear," or "A.P.T. 28" (Lipton, Sanger & Scott Shane, 2016). In addition, Russia conducted a massive operation to target hundreds to thousands of non-governmental organizations and nonprofits (N.Y Times, 2017). Russian intelligence officials took the emails and private documents procured through the DNC hack, and posted them to WikiLeaks and other websites in July 2016 (Lipton, Sanger & Scott Shane, 2016). R.N.C. emails, on the other hand, were not disseminated.

Russian dissemination of information arguably had significant impact on congressional races, and citizen trust in the democratic process more generally. The fallout from the dissemination of D.N.C. emails was immediate. Debbie Wasserman Schultz, the chair of the D.N.C., was forced to resign, along with her top aides (Lipton, Sanger & Scott Shane, 2016). At the state level, confidential documents taken from the Democratic Congressional Campaign Committee relating to congressional races in a dozen states were published, tainting many affected races with accusations of scandal.

Russian interference was also done through the Internet Research Agency (IRA)[19] waging a social media campaign that favored presidential candidate Donald J. Trump and disparaged presidential

[19] The Internet Research Agency (IRA) is a Russian company, based in Saint Petersburg, engaged in online influence operations on behalf of Russian business and political interests.

candidate Hillary Clinton (France-Presse, 2019). The IRA also sought to provoke and amplify political and social discord in the United States.

By February 2016, internal IRA documents showed an order to support the candidacies of Donald Trump and Bernie Sanders, while IRA members were to use any opportunity to criticize Hillary Clinton and the rest of the candidates (Thomsen, 2019). From June 2016, the IRA organized election rallies in the U.S. often promoting Trump's campaign while opposing Clinton's campaign (Lindstrom, 2019). The IRA posed as Americans, hiding their Russian background, while asking Trump campaign members for campaign buttons, flyers, and posters for the rallies. The IRA spent $100,000 for over 3,500 Facebook advertisements, which included anti-Clinton and pro-Trump advertisements (Broderick, 2019).

The IRA also created groups on Facebook, including a purported conservative group (e.g. Tea Party News), purported Black social justice groups (e.g. Blacktivist), LGBTQ groups (e.g. 'LGBT United'), and religious groups (e.g. United Muslims of America) (Prohov, 2019). The IRA Twitter accounts included @TEN_GOP (claiming to be related to the Tennessee Republican Party), @jenn_abrams, and @Pamela_Moore13 (both claimed to be Trump supporters and both had 70,000 followers).[73] Several Trump campaign members (Donald J. Trump Jr., Eric Trump, Kellyanne Conway, Brad Parscale, and Michael Flynn) linked or reposted material from the IRA's @TEN_GOP Twitter account listed above. Other people who responded to IRA social media accounts include Michael McFaul, Sean Hannity, Roger Stone, and Michael G. Flynn (Michael Flynn's son) (Kiely & Robertson, 2019).

Russia also allegedly targeted the voter registration systems in over 20 state election systems. Four of the twenty systems were, in fact, breached (Kurtzleben, 2016). Recent reports indicate that Russian interference in the election went far beyond misinformation campaigns, and instead constituted attempts to breach the core systems of the American voting apparatus (Riechmann & Byoum, 2017). A classified National Security Agency report, published online by The Intercept, states that Russian hackers, part of the GRU military agency, attempted to send spear-phishing

emails[20] to over 100 local election officials at VR systems, a Florida-based technology firm that sells equipment and software for voter registration (Greenburg, 2017).

Russian attempts to interfere in the election were first disclosed publicly by members of the United States Congress on September 22, 2016, confirmed by United States intelligence agencies on October 7, 2016, and further detailed by the Director of National Intelligence office in January 2017. According to U.S. intelligence agencies, the operation was ordered directly by Putin. The Federal Bureau of Investigation (FBI) opened the Crossfire Hurricane investigation of Russian interference on July 31, 2016, including a special focus on links between Trump associates and Russian officials and suspected coordination between the Trump campaign and the Russian government. The FBI's work was taken over in May 2017 by former FBI director Robert Mueller, who led a Special Counsel investigation until March 2019 (Breuninger, 2019). Mueller concluded that Russian interference "violated U.S. criminal law", and he indicted twenty-six Russian citizens and three Russian organizations. The investigation also led to indictments and convictions of Trump campaign officials and associated Americans, for unrelated charges. The Special Counsel's report, made public on April 18, 2019, examined numerous contacts between the Trump campaign and Russian officials but concluded that there was insufficient evidence to bring any conspiracy or coordination charges against Trump or his associates.

Russian interference activities triggered strong statements from American intelligence agencies, a direct warning by then U.S. President Barack Obama to Russian President Vladimir Putin, renewed economic sanctions against Russia, and closures of Russian diplomatic facilities and expulsion of their staff. The Senate and House Intelligence Committees conducted their own investigations into the matter. Trump denied that the interference occurred, contending that it was a "hoax" perpetrated by Democrats to explain Clinton's loss. He dismissed FBI Director James Comey in part over his investigation of Russian meddling.

The Russian government interfered in the 2016 U.S. presidential election with the goal of harming the campaign of Hillary Clinton, boosting the candidacy of Donald Trump, and increasing political

[20] **Spear phishing** is an **email** or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.

or social discord in the United States. Putin's motives for wanting Trump to win are simple: Trump champions many foreign policies that Putin supports. Trump's pro-Kremlin proposal to "look into" the recognition of Crimea as a part of Russia has been hugely criticized by several members of the American public. President Obama and nearly every member of Congress, Republicans and Democrats, have rejected the idea vigorously. Only Afghanistan, Cuba, Nicaragua, North Korea, Syria and Venezuela have recognized Russia's annexation of Crimea. Naturally, Putin would love to see the United States join that list (Pager, 2016).

Trump also has made clear his disdain for the United States' alliances around the world. Demonstrating his misunderstanding of how NATO works, Trump has demanded that other NATO members essentially should pay the U.S for protection, making many of the U.S allies, especially in the eastern part of Europe, nervous about his commitment to defend them. Trump has also been accused of disparaging American allies in Asia (Washington Post, 2016), creating new opportunities for Russian influence. On trade, Trump's promises to disrupt the U.S trade agreements with China and Mexico also plays right into Putin's agenda. From Putin's perspective, there could be nothing better than a trade war between the United States and China or Mexico (Washington Post, 2015).

On the whole, Trump appears to advocate isolationist policies and an abdication of U.S. leadership in the world. A U.S. retreat from global affairs fits precisely with Putin's international interests. Experts suggest that if President Trump tried to implement his radical ideas regarding immigration or walling off the southern border of the United States, a serious push-back effort would ensue both in Congress and in the country as a whole (Washington Post, 2015). A United States convulsed by infighting over Trump's deeply divisive policy proposals gives Putin more freedom to act around the world.

If a Trump victory would serve Putin's interests, a President Hillary Clinton would not. Putin and his government already knew Clinton from her four years as Secretary of State. They remember the tough line she took in seeking to negotiate a political transition in Syria; her efforts, though failed, to get Russia to support U.N. Security Council resolutions regarding the Syrian humanitarian tragedy; and her early advocacy for arming Syria opponents of Bashar al-Assad, Moscow's ally. They remember her public criticism of irregularities in Russia's December 2011 parliamentary election, which Putin described as a signal to Russian protesters to take to the streets

against him. They remember her portrayal of Putin's prized foreign policy project, the creation of the Eurasia Economic Union, as a move to re-Sovietize the region (Radio Liberty, 2012). It should be no surprise that Putin and his government would prefer see Trump in the White House.

It can be argued that Russia's motives in the 2016 US general election may have been successful. After all, the Russians wanted a Trump presidency which later came to fruition. As to whether the Trump presidency has helped to ease relations between Russia and the US, that remains to be seen as the tension between the two countries does not appear to be cooling off anytime soon.

Conclusions

In summary, the Russian government's investment in influence and network exploitation operations, built on the back of a new and fragmented media environment, created a space for new forms and techniques in cyber interference. But states are not the only entities that have been watching this phase of cyber interference, and the techniques demonstrated by the Russian government are readily replicable with a high return on investment. The dividends from such interference are too great to ignore, posing a question: what will the next phase of cyber interference look like, and who will be involved?

Chapter V
Cyber as a tool for espionage

Introduction

On April 16, 2018, the US authorities issued a warning that government-backed Russian hackers were using compromised routers and other network infrastructure to conduct espionage and potentially lay the groundwork for future offensive cyber operations (Gutman, 2018). While the issue of nation-states engaging in espionage dates back a long way, what is interesting is the new domain in which these espionage activities are undertaken. Research by cyber-threat intelligence firm, CYFIRMA, puts it clearly: "The rise in state-sponsored cyber-attacks on critical infrastructure will continue its upward trajectory during 2019" (Bannister, 2018 pg 203) Alarmingly, and entirely unsurprisingly, CYFIRMA also expects espionage activities to increase in intensity.

Although it has taken some time to manifest, nation-states have realized the potential for cyber espionage to have a major impact on the foreign policy of nation states. The first section of this chapter makes a distinct case for cyber used as an important tool in espionage especially as espionage plays a key role as an instrument of self-interest. To build on this, the second section looks at the Chinese v US as a case study. The first part of the discussion focusses on the attempts by China to secretly obtain information from the US. The second part of the study explores the steps the US would have used to retaliate on China. The chapter concludes by giving recommendations on the ways to avoid future occurrence.

Background to Espionage

States have long employed espionage as an instrument to advance their interests and shore up their defenses against threats in the international system. In the early days, espionage was largely human derived. Back then it was more common for one state actor to send out spies to obtain information from another state. The information obtained from such espionage efforts were used by the acting state to further its foreign policy objectives. These foreign policy objectives could be economic, that is to improve its economic policies at the expense of the other state or these policy objectives could even be coercive. They could be coercive in the sense of the acting state using the information obtained from the other state to gain an advantage in cases of war between both nations. But over time, the use of espionage as an instrument for self-interest has started to evolve

to require more of a technical aspect, for example, with the emergence of satellite spying[21]. Cyber has emerged as a new instrument and perhaps arguably the most useful tool for national espionage efforts.

The first formally documented case of cyber espionage pre-dated the web itself. In 1986, Clifford Stoll, who at the time was managing computers at Lawrence Berkeley National Laboratory in California, noticed some strange activity in computing time records. This eventually led him to a hacker who appeared to be systematically targeting computers at military bases around the U.S. looking for military secrets. He eventually created a trap for the attacker, luring him in with a cache of fake information. The hacker fell for the bait and was identified as Markus Hess, a West German who had been selling stolen information to the KGB (O'Brien, 2017).

Earlier still, the CIA is alleged to have caused the explosion of a Siberian gas pipeline in 1982 by duping Soviet agents into stealing booby-trapped industrial control software, which caused the pipeline to malfunction. The incident was long the subject of rumor but appeared to be confirmed in 2004 when Thomas Rid, a former member of Ronald Reagan's National Security Council, wrote about it . However, Rid's account has been disputed by some experts, including well-known cyber security researcher Jeffrey Carr.

According to Carr, an informed source from one of the three-letter agencies reported that the explosion had nothing to do with CIA sabotage and everything to do with a Russian engineer who, when discovering a leak in the pipeline, simply kept increasing pressure to maintain the flow of natural gas. The gas leak kept building and building until a passing Russian train sparked the gas cloud and exploded. Carr suggested that it was a true disaster and did not qualify as a key event in cyber history (Carr, 2012).

The case that really brought cyber espionage to public attention was Moonlight Maze, the name given to attacks against US government targets, which became public in 1999 with the publication of a story in *Newsweek*. An FBI investigation found that the group responsible had compromised the US Navy, Air Force, Department of Energy, and NASA, among other targets, and stolen so

[21] Spy satellites are a special type of artificial satellites intended primarily for espionage purposes. They largely operated in low Earth Orbit.

many documents that, if stacked, they "would be taller than the Washington Monument" (O'Brien, 2017).

While Moonlight Maze was one of the first operations to be uncovered, it certainly was not the only one underway at this time. While the activities of the Equation Group, a highly advanced, well-resourced cyber espionage group, only became public in 2015, available evidence suggests that it was operating as early as 2001.

Although not immediately apparent at the time, at least to the public, the level of activity began to really increase in subsequent years, with many of the major cyber espionage groups first showing signs of life between 2005 and 2010. It took a few years to join the dots, but by the end of the decade cyber espionage was in the spotlight, this time with Google disclosing that it and at least 20 other large companies had been targeted by a group called Aurora (known to Symantec as Hidden Lynx). By estimation, Hidden Lynx had approximately 50 to 100 operatives at its disposal and was capable of carrying out hundreds of simultaneous attacks against diverse targets, indicating how cyber espionage operations had scaled up over the years (O'Brien, 2017).

The scaling of cyber espionage gives credence to China's emergence as a major global power in reshaping the cyber domain. The country has the world's largest internet-user community, a growing economic footprint and increasingly capable military and intelligence services. Harnessing these assets, it is pursuing a patient, assertive foreign policy that seeks to determine how information and communications technologies are governed and deployed. This policy is likely to have significant normative impact, with potentially adverse implications for a global order that has been shaped by Western liberal democracies. Even as China goes out into the world, there are signs that new technologies are also becoming powerful tools for domestic social control and the suppression of dissent abroad. With China continually seeking to improve its economy and remain relevant in the global scheme of things, it has several times sought to obtain information from other perceived power super nations. This is where the next case study is of significance.

The Chinese v US Case:

Even the most casual observer of the Western media will have been struck in recent times by the growing attention being paid to cyber espionage efforts and losses of information being suffered by both public and private entities. In particular, accusations have been levied against China for

alleged state-sponsored cyber espionage directed at U.S. governmental and business interests. After years of discreet avoidance of naming China as the culprit in these cyber-attacks, the U.S. Government decided to identify Beijing as the principal perpetrator of these attacks and to call upon it to desist. The U.S. Department of Defense has been especially vocal in accusing China of being behind these cyber intrusions and linking them to the compromise of several American weapon systems. U.S. Secretary of Defense, Chuck Hagel, referred to cyber threats as "terribly dangerous" and called for talks with China and others to "establish international norms of responsible behavior in cyberspace" (Alexander, 2013 pg 147).

The issue of cyber espionage has figured prominently in US-China bilateral relations and has found its way onto the agenda of the highest levels of discussion, such as the summit between Presidents Obama and Xi in June 2016. It would appear though that the political attention to the problem has not yielded sufficient results. In May 2014, the US Department of Justice took the unprecedented step of indicting five serving officers of the People's Liberation Army (PLA) for engaging in cyber espionage against American corporations. There were also reports that US authorities considered denying visas to Chinese nationals who had intended to attend popular hacker conferences held in the US in August 2014. Chinese officials angrily denied these charges and even suggested that the U.S. "fabricated" the evidence against the PLA officers (RajapalenPag, 2014).

These publicized actions represent a significant escalation over the previous reliance on behind the scene diplomatic protests or expressions of concern during high-level discussions. It is noteworthy that even as the U.S. military moved to enhance significantly its cyber security capacities, including its capabilities for offensive cyber operations with the creation of US cyber command, the US Defense Secretary in 2014, Chuck Hagel, advocated for an alternative approach to address potential cyber espionage efforts. This approach is premised on diplomatic rather than military initiatives and would seek to agree on "rules of the road" to govern state behavior in cyber space. Whether global and regional cyber security will be characterized by adversarial or cooperative approaches may depend on the success or failure in the near term of efforts to develop these norms of responsible state behavior.

The cyber-attacks against the United States Office of Personnel Management (OPM) resulted in the theft of personal information of more than 20 million Americans, mostly current and former officials of the US federal government. The American Federation of Government Employees

believes that the hackers are now in possession of all personnel data for every federal employee (UN Institute for Disarmament Research, 2013). These data include names, addresses, birth dates, job and pay histories, and insurance and pension information. In most cases, the information stolen from the OPM derived from application forms of individuals who had applied for non-sensitive, public trust or national security positions since 2000, either as federal government employees or as contractors. In 1.1 million instances, the stolen data included the applicants' fingerprints (Fung, 2014). According to The New York Times, the Obama Administration believed that the Chinese government was behind this instance of cyber espionage, which it regarded as being of such a large scale and serious nature that retaliation was required (Presidential Policy Decisions, 2014).

The two OPM hacks differ from many other cyber-attacks, in the sense that they were neither aimed at stealing commercial or military data, nor at inflicting direct damage. In fact, it is not very clear what they were aimed at. Until it is known definitively who stole these data, it is hard to determine the motive for the attacks. According to The New York Times, US officials are convinced that the attack was carried out or sponsored by the Chinese authorities, even though they have not formally accused China. Still, on one occasion, Director of National Intelligence James Clapper did publicly refer to 'China' as the perpetrator. Clapper suggested that China was the "leading suspect" in the attacks.

Interestingly, the US government makes a distinction between intelligence operations for national security purposes and government sponsored cyber-espionage for commercial gain (International Strategy for Cyberspace, 2011). The United States has (at least implicitly) acknowledged to be doing the first, which it calls legitimate, and has accused China of doing also the second, which it considers illegitimate (International Code of Conduct for Information Security, 2011). The OPM hacks seem to fit the first category more than the second. Indeed, Michael Hayden, former director of both the NSA and the CIA said in an interview with The Wall Street Journal that "the current story is" the Chinese Ministry of Public Security was responsible for the OPM hacks and that "those [OPM] records are a legitimate foreign intelligence target."

Whether China is actually responsible cannot be determined on the basis of publicly available information. Should the Chinese government indeed have acquired personal data on a large number of US officials, this could provide Beijing with the possibility of stealing further information from government agencies through the use of false identities, or at least with an

improved ability to monitor actions by the US federal bureaucracy. If detection of the OPM hacks was planned, they could even have been Chinese retaliation for US cyber-espionage operations in China, such as those outlined in documents leaked by former contractor Edward Snowden (UN General Assembly Resolution, 2012). In other words, the OPM hacks could have been partly aimed at deterring the United States from continuing its own cyber-attacks against China.

As evident in the cyber world, attribution is a fundamental issue with regard to cyber-attacks. Without the ability to identify an attacker, deterrence is not possible. Obtaining complete certainty about the source of a cyber-attack is often impossible (UN General Assembly Resolution, 2013). Even if compelling evidence is found by US investigators, it may not be possible to bring this into the open without harming the future use of American intelligence instruments or sources. In the OPM case, US officials seem to believe that China is behind the cyber theft, but they have not disclosed any details on what they know about the attacker's identity. By retaliating against China, the United States risks escalation, as well as international condemnation of the retaliatory action.

The US cyber strategy states that the United States will retaliate against major cyber-attacks, either with cyber tools or by other means. With no response to the cyber-attack against the OPM, the credibility and thus the deterrence function of the cyber strategy may thus be damaged. The following overview discusses the main policy options that are relevant for retaliating and deterring major cyber-attacks by foreign states, including their risk of escalation.

The first option would be passive deterrence. This option is the least complicated, although it is not very realistic in the current situation. It signifies doing nothing directly towards China. The United States could simply acknowledge that its cyber security measures in this case were not adequate, but also communicate that lessons have been learned and that its security systems have been improved and will receive on-going attention. This option prevents any escalation; China cannot accuse the United States of retaliating against something that it wrongly blames China for without any evidence.

Improving cyber security measures acts as a so-called passive deterrent; raising the costs of any future cyber intrusions may lower the chance that they will occur. The risk, however, is that China (or whoever was responsible for the OPM attacks) will consider this response to be an invitation to continue its cyber-espionage activities on an even larger scale. If no negative consequences are involved, it could persuade potential attackers to raise threat activities to a higher level. Deterrence

by denial, as raising the barriers for potential enemies is often called, is only effective if it changes the costs–benefits calculus of these enemies. In this case, the attackers might consider it worthwhile increasing their efforts to surpass the improved cyber security measures.

A largely symbolic response with hardly any risk of escalation could be diplomatic protests. Additionally, some Chinese officials could be expelled from the United States. China, however, may do the same in response. Although this kind of retaliation may damage China's international reputation to some extent, these actions would not be very harmful to China. This harmlessness in turn perfectly indicates the negative side of this policy option: it would probably not deter China – or any other cyber enemy – from continuing similar cyber-attacks.

Legal action against Chinese organizations or individuals is another option. The United States has used this tool before. In 2014 as noted above, five officers of the Chinese PLA were indicted on the charge of theft of intellectual property from US-based companies via cyber espionage (Tiezzi, 2018). As with diplomatic protests, however, legal measures are mostly of a symbolic nature. Indicted individuals can only be arrested when they visit the United States or a US ally, and organizations might just change their identity. Moreover, this option entails the risk that such a legal track could result in a court case in which the United States is forced to expose sensitive intelligence operations in order to provide evidence. This would hurt more than it merits. Moreover, China might retaliate by starting 'symbolic' indictments of US organizations and individuals as well. US companies doing business in China could be vulnerable targets. Similar to the second option above, this option may to some extent be damaging to China's reputation and suggest the United States' ability to identify cyber attackers. It is doubtful, however, whether this will have a deterring effect.

Another option would be economic sanctions. After the US government blamed North Korea for active involvement in the hacking of Sony Pictures Entertainment in 2014, it retaliated by strengthening existing economic sanctions against the North Korean regime. Such economic retaliation might have some value as a deterrent, especially for countries like China with an economy that is highly dependent on exports. However, once the sanctions are installed or strengthened, the sanctioned state has little reason to change its behavior unless there are guidelines on how to ease or get rid of the sanctions. Far more important in the Chinese case is that the US economy is heavily dependent on interaction with China. If China was to retaliate with economic

counter-sanctions, this would significantly hurt the United States as well, and one could question whether such economic damage would outweigh the deterrent effect regarding cyber-attacks.

The threat of serious retaliation would prove to be an effective deterrent. By retaliating, the United States would show that future cyber intrusions of this scale will not be tolerated. The most obvious option regarding retaliation is to strike back in the same dimension that the offender used – cyberspace. The United States could, for example, try to steal and publish information from the Chinese government. A cyber-attack to indicate that certain cyber infrastructures of the Chinese government could be paralyzed would also be an option, showing that the United States is capable of, and will not refrain from, starting offensive cyber operations in many ways. However, a serious risk emerges here of starting a cycle of escalation and retaliation.

An almost unrealistic option is retaliation through conventional military means, such as a strike against a specific location that is related to Chinese cyber forces. Such an action would probably trigger a military response from the Chinese and could culminate in a dangerous process of escalation. This option seems likely to be considered only in the case of more destructive cyber-attacks, and/or if the country involved is less powerful than China.

A final option is the use of covert retaliation in cyberspace. It is the invisibility, and therefore unpredictability, of covert retaliation that might deter China – if it attacked the OPM in the first place – from conducting similar cyber-attacks. On the other hand, this option still carries with it the risk of escalation; China might respond with covert operations against US targets, or with retaliatory actions in other domains, such as hurting the United States economically.

All these options are to some extent problematic, almost all of them carry a risk of escalation, and none of them may be truly effective in deterring future cyber-espionage. Yet if no action is taken, the credibility of the US cyber security strategy diminishes. Although the United States has not formally accused China, the fact that major Western media believe that the US government thinks that China is the perpetrator already raises questions regarding the feasibility of deterring Chinese cyber-attacks. In this context, Washington might decide that covert retaliation through cyber means is the most appropriate type of response. One of the possible targets mentioned in The New York Times' report involves undermining the Chinese government's ability to censor the use of the internet by Chinese citizens. Adam Segal of the Council of Foreign Relations outlined three possibilities for such a retaliatory act: expose information to embarrass the Chinese authorities;

allow Chinese citizens to access blocked foreign websites, and undermine restrictions on domestic flows of information on the internet (UN General Assembly, 2014). Of course, a combination of two or three of these options could also be possible.

A major US cyber operation aimed at threatening key interests of the Chinese government, even if covert and well calibrated, could have serious consequences. In the short term, it would carry the risk of provoking Chinese counter-attacks that would destabilize the already complex Sino–US relationship. In addition to the existing risk of an (inadvertent) military incident in the South or East China Sea, further insecurity and volatility would result from even a limited and covert cyber conflict. Moreover, if other countries observe that the United States is likely conducting covert cyber operations against China as a retaliatory measure, in the longer run the use of covert cyber-attacks by states against other states may become a de facto accepted norm. Both developments are dangerous and would contribute to less stability and more insecurity in the international system. While it is questionable whether cyber deterrence can actually be achieved in this instance, except perhaps at a very high cost, it seems clear that retaliation carries major risks. This makes it more difficult for the United States to act, thereby undermining the credibility and effectiveness of its cyber security strategy.

Conclusion

At first sight, the costs of a retaliatory action may seem high, given the benefits that Western intelligence communities have long enjoyed because of their superior technological and financial resources. Yet the United States and its allies should ask themselves whether, in a world in which cyber-attacks and cyber espionage are becoming ever more damaging and within closer reach of new actors, their national security interests are better served by a proliferation of state-sponsored espionage and covert cyber operations, or by norms that aim at limiting such activities.

Chapter VI
Cyber as a tool for Sabotage

Introduction

Predicting the future is hardly possible, but stating that cyber sabotage will be a continuing threat to international security and stability in the coming years seems a safe forecast. Cyber sabotage primarily causes economic damage. These economic damages could be in the form of physical damage to a state's infrastructure or even the compromise of an institution's hardware and software facilities. In addition to economic consequences, such as weakening the competitive economic position of a state, cyber sabotage is also a security issue in that it can be used by potential enemies, whether state or non-state actors, to create weaknesses in the national security of states.

This chapter deals with the question of how states can cope with the threat of cyber sabotage from a foreign policy perspective, focusing on cyber sabotage conducted or sponsored by state actors. The cyber-attack on Iran's nuclear facilities is used as a case study. The first section of the case study examines the background of Iran's nuclear program. The second section discusses the attack on Iran's nuclear facilities in Natanz and the concluding sections explores the aftermath of the cyber sabotage attacks with particular reference to the Iran nuclear deal of 2015.

The most dramatic developments in the world of cyber sabotage occurred with the discovery of Stuxnet. It was probably the first real-world example of the kind of ambitious and highly destructive cyber-attack that had always been seen as theoretically possible but had hitherto only been the subject of doom laden warnings.

Stuxnet is a malicious computer worm, first uncovered in 2010. Thought to have been in development since at least 2005, Stuxnet targets Supervisory Control and Data Acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to Iran's nuclear program. Although neither country has openly admitted responsibility, the worm is believed to be a jointly built American/Israeli cyber weapon (Nakashima, 2012)

Stuxnet specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery and industrial processes including centrifuges for separating nuclear material. Exploiting four zero-day flaws, (ZDNet, 2010) Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Stuxnet reportedly compromised Iranian

PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart, by targeting control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade (David, 2014). Stuxnet's design and architecture are not domain-specific and it could be tailored as a platform for attacking modern supervisory control and data acquisition (SCADA) and PLC systems (e.g., in factory assembly lines or power plants), the majority of which reside in Europe, Japan and the US (Karnouskos, 2014).

Background to the Iran Case

For years, an enduring mystery has surrounded the Stuxnet virus attack that targeted Iran's nuclear program. This mystery surrounds the manner in which the U.S. and Israel got their malware onto computer systems at the highly secure uranium-enrichment plant. The first-of-its-kind virus, designed to sabotage Iran's nuclear program, effectively launched the era of cyber sabotage and was unleashed in 2007, after Iran began installing its first batch of centrifuges at a controversial enrichment plant near the village of Natanz.

The courier behind that intrusion, whose existence and role has not been previously reported, was an inside mole recruited by Dutch intelligence agents at the behest of the CIA and the Israeli intelligence agency, the Mossad. An Iranian engineer recruited by the Dutch intelligence agency AIVD provided critical data that helped the U.S. developers target their code to the systems at Natanz. That mole then provided much-needed inside access when it came time to slip Stuxnet onto those systems using a USB flash drive (Zetter & Modderkolk, 2019).

The Dutch were asked in 2004 to help the CIA and Mossad get access to the plant, but it wasn't until three years later that the mole, who posed as a mechanic working for a front company doing work at Natanz, delivered the digital weapon to the targeted systems. The Dutch mole was the most important way of getting the virus into Natanz. The revelation of Dutch involvement harkens back to a time when there was still extensive cooperation and strong, multilateral agreement among the U.S. and its allies about how to deal with the Iranian nuclear program, a situation that changed in 2018 after the Trump administration pulled out of the hard-won nuclear accord with Tehran.

The Stuxnet Olympic Games operation was primarily a joint U.S.-Israel mission that involved the NSA, the CIA, the Mossad, the Israeli Ministry of Defense and the Israeli SIGINT National Unit, Israel's equivalent of NSA. But the U.S. and Israel had assistance from three other nations, hence the covert codename that gave a nod to the five-ring symbol of the world's most famous

international sporting event. Two of the three participating players were the Netherlands and Germany. The third is believed to be France, although U.K. intelligence also played a role (Zetter & Modderkolk, 2019).

Germany contributed technical specifications and knowledge about the industrial control systems made by the German firm Siemens that were used in the Iranian plant to control the spinning centrifuges. France is believed to have provided intelligence of a similar sort. But the Dutch were in a unique position to perform a different role, delivering key intelligence about Iran's activities to procure equipment from Europe for its illicit nuclear program, as well as information about the centrifuges themselves. This is because the centrifuges at Natanz were based on designs stolen from a Dutch company in the 1970s by Pakistani scientist Abdul Qadeer Khan. Khan stole the designs to build Pakistan's nuclear program, then proceeded to market them to other countries, including Iran and Libya (Winer, 2019).

The Dutch intelligence agency, known as AIVD, along with U.S. and British intelligence, infiltrated Khan's supply network of European consultants and front companies who helped build the nuclear programs in Iran and Libya. That infiltration did not just involve old-school tradecraft but also employed offensive hacking operations being developed as part of the burgeoning field of digital espionage.

The request to the Dutch for help with this came toward the end of 2004, when a Mossad liaison working out of the Israeli Embassy in The Hague and a CIA official based at the U.S. Embassy met with a representative from AIVD. There was no talk yet about inserting a digital weapon into the control systems at Natanz; the aim at that time was still just intelligence.

But the timing was not random. In 2003, British and U.S. intelligence had landed a huge coup when they intercepted a ship containing thousands of centrifuge components headed to Libya; components for the same model of centrifuges used at Natanz. The shipment provided clear evidence of Libya's illicit nuclear program. Libya was persuaded to give up the program in exchange for the lifting of sanctions, and also agreed to relinquish any components already received.

By March 2004, the U.S., under protest from the Dutch, had seized the components from the ship and those already in Libya and flown them to the Oak Ridge National Lab in Tennessee and to a

facility in Israel. Over the next months, scientists assembled the centrifuges and studied them to determine how long it might take for Iran to enrich enough gas to make a bomb. Out of this came the plot to sabotage the centrifuges. The Dutch intelligence agency already had an insider in Iran, and after the request from the CIA and Mossad came in, the mole decided to set up two parallel tracks, each involving a local front company, with the hope that one would succeed getting into Natanz.

Establishing a dummy company with employees, customers and records showing a history of activity, takes time, and time was in short supply. In late 2005, Iran announced it was withdrawing from the suspension agreement, and in February 2006 it began to enrich its first batch of uranium hexafluoride gas in a pilot plant in Natanz. The Iranians ran into some problems that slowed them down, however, and it wasn't until February 2007 that they formally launched the enrichment program by installing the first centrifuges in the main halls at Natanz.

By then, development of the attack code was already long under way. A sabotage test was conducted with centrifuges in 2006 and presented to President George Bush, who authorized the covert operation once he was shown it could actually succeed. By May 2007, Iran had 1,700 centrifuges installed at Natanz that were enriching gas, with plans to double that number by summer. But sometime before the summer of 2007, the Dutch mole was inside Natanz. The first company the mole established had failed to get into Natanz, there was a problem with the way the company was set up and the Iranians were already suspicious (Winer, 2019).

The second company, however, got assistance from Israel. This time, the Dutch mole, who was an engineer by training, managed to get inside Natanz by posing as a mechanic. His work did not involve installing the centrifuges, but it got him where he needed to be to collect configuration information about the systems there. He apparently returned to Natanz a few times over the course of some months.

Stuxnet was reportedly meant to be a precision attack that would only unleash its sabotage if it found a very specific configuration of equipment and network conditions. Using the information provided by the mole, the attackers were able to update the code and provide some of that precision. According to the security firm Symantec, which reverse-engineered Stuxnet after it was discovered, the attackers made updates to the code in May 2006 and again in February 2007, just

as Iran began installing the centrifuges at Natanz. But they made final changes to the code on September. 24, 2007, modifying key functions that were needed to pull off the attack, and compiled the code on that date. Compiling code is the final stage before launching it. The code was designed to close exit valves on random numbers of centrifuges so that gas would go into them but couldn't get out. This was intended to raise the pressure inside the centrifuges and cause damage over time and also waste gas (Winer, 2019).

This version of Stuxnet had just one way to spread, via a USB flash drive. The Siemens control systems at Natanz were air-gapped, meaning they were not connected to the internet, so the attackers had to find a way to jump that gap to infect them. Engineers at Natanz programmed the control systems with code loaded onto USB flash drives, so the mole either directly installed the code himself by inserting a USB into the control systems or he infected the system of an engineer, who then unwittingly delivered Stuxnet when he programmed the control systems using a USB stick.

Once that was accomplished, the mole did not return to Natanz again, but the malware worked its sabotage throughout 2008. In 2009 the attackers decided to change tactics and launched a new version of the code in June that year and again in March and April 2010. This version, instead of closing valves on the centrifuges, varied the speed at which the centrifuges spun, alternatively speeding them up to a level beyond which they were designed to spin and slowing them down. The aim was to both damage the centrifuges and undermine the efficiency of the enrichment process. Notably, the attackers had also updated and compiled this version of the attack code back on September 24, 2007, when they had compiled the code for the first version, suggesting that intelligence the Dutch mole had provided in 2007 may have contributed to this version as well.

By the time this later version of the code was unleashed, however, the attackers had lost the inside access to Natanz that they had enjoyed through the mole or perhaps they simply no longer needed it. They got this version of Stuxnet into Natanz by infecting external targets who brought it into the plant. The targets were employees of five Iranian companies, all of them contractors in the business of installing industrial control systems in Natanz and other facilities in Iran, who became unwitting couriers for the Stuxnet virus.

The Attack

Ralph Langner, the researcher who identified the Stuxnet infected Iranian PLCs speculated publicly in September 2010 that the malware was of Israeli origin, and that it targeted Iranian nuclear facilities (Cherry & Langner, 2010). However, Langner more recently, in a TED Talk recorded in February 2011, stated that, "My opinion is that the Mossad is involved, but that the leading force is not Israel. The leading force behind Stuxnet is the cyber superpower – there is only one and that's the United States" (Langner, 2011). Kevin Hogan, Senior Director of Security Response at Symantec, reported that the majority of infected systems were in Iran (Macmillan, 2010) which has led to speculation that Stuxnet may have been deliberately targeting "high-value infrastructure" in Iran including either the Bushehr Nuclear Power Plant or the Natanz nuclear facility (Zelter, 2010; Woodward, 2010). Langner called the malware "a one-shot weapon" and said that the intended target was probably hit, although he admitted this was speculation (Langner, 2011). Another German researcher and spokesman of the German-based Chaos Computer Club, Frank Rieger, was the first to speculate that Natanz was the target (Joseph, 2011).

According to the Israeli newspaper Haaretz, in September 2010 experts on Iran and computer security specialists were increasingly convinced that Stuxnet was meant "to sabotage the uranium enrichment facility at Natanz where the centrifuge operational capacity had dropped over the past year by thirty percent" (Melman, 2010 pg 100). On 23 November 2010 it was announced that uranium enrichment at Natanz had ceased several times because of a series of major technical problems (Globalsecuritynewswire.org, 2010). A serious nuclear accident, supposedly the shutdown of some of its centrifuges, occurred at the site in the first half of 2009, which is speculated to have forced the head of Iran's Atomic Energy Organization, Gholam Reza Aghazadeh, to resign (WikiLeaks, 2009). Statistics published by the Federation of American Scientists (FAS) show that the number of enrichment centrifuges operational in Iran mysteriously declined from about 4,700 to about 3,900 beginning around the time the nuclear incident WikiLeaks mentioned would have occurred. The Institute for Science and International Security (ISIS) suggests, in a report published in December 2010, that Stuxnet is a reasonable explanation for the apparent damage at Natanz, and may have destroyed up to 1,000 centrifuges 10 percent overall capacity sometime between November 2009 and late January 2010 (Institute for International Security, 2010). The authors conclude:

> *The attacks seem designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge. If its goal was to quickly destroy all the centrifuges in the FEP [Fuel Enrichment Plant], Stuxnet failed. But if the goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the FEP, while making detection difficult, it may have succeeded, at least temporarily.*

The ISIS report further notes that Iranian authorities have attempted to conceal the breakdown by installing new centrifuges on a large scale.

The worm worked by first causing an infected Iranian IR-1 centrifuge to increase from its normal operating speed of 1,064 hertz to 1,410 hertz for 15 minutes before returning to its normal frequency. Twenty-seven days later, the worm went back into action, slowing the infected centrifuges down to a few hundred hertz for a full 50 minutes. The stresses from the excessive, then slower speeds caused the aluminum centrifugal tubes to expand, often forcing parts of the centrifuges into sufficient contact with each other to destroy the machine (Holger, 2011).

According to The Washington Post, IAEA cameras installed in the Natanz facility recorded the sudden dismantling and removal of approximately 900–1,000 centrifuges during the time the Stuxnet worm was reportedly active at the plant. Iranian technicians, however, were able to quickly replace the centrifuges and the report concluded that uranium enrichment was likely only briefly disrupted (The Washington Post, 2011).

On 15 February 2011, the ISIS released a report concluding that:

> *Assuming Iran exercises caution, Stuxnet is unlikely to destroy more centrifuges at the Natanz plant. Iran likely cleaned the malware from its control systems. To prevent re-infection, Iran will have to exercise special caution since so many computers in Iran contain Stuxnet.*
>
> *Although Stuxnet appears to be designed to destroy centrifuges at the Natanz facility, destruction was by no means total. Moreover, Stuxnet did not lower the production of low-enriched uranium (LEU) during 2010. LEU quantities could have certainly been greater, and Stuxnet could be an important part of the reason why they did not increase significantly. Nonetheless, there remain important questions about why Stuxnet destroyed*

only 1,000 centrifuges. One observation is that it may be harder to destroy centrifuges by use of cyber-attacks than often believed.

(Institute for Science and International Security, 2011).

While they may have had help from countries like Netherlands, Germany and even France, the U.S and Israel are still considered by many experts to have been the major masterminds behind the cyber sabotage of the Iranian nuclear facilities. As reported earlier the United States, under one of its most secret programs, initiated by the Bush Administration and accelerated by the Obama administration, sought to destroy Iran's nuclear program by novel methods such as undermining Iranian computer systems. A diplomatic cable obtained by WikiLeaks showed how the United States was advised to target Iran's nuclear capabilities through 'covert sabotage'. A New York Times article as early as January 2009 credited a then unspecified program disguised to prevent an Israeli military attack on Iran where some of the efforts focused on ways to destabilize the centrifuges. A wired article claimed that Stuxnet is believed to have been created by the United States (Zetter, 2011).

John Bumgarner, a former intelligence officer and member of the United States Cyber-Consequences Unit (US-CCU), published an article prior to Stuxnet being discovered or deciphered, that outlined a strategic cyber strike on centrifuges and suggests that cyber-attacks are permissible against nation states which are operating uranium enrichment programs that violate international treaties gives some credibility to these claims. Bumgarner pointed out that the centrifuges used to process fuel for nuclear weapons are a key target for cybertage[22] operations and that they can be made to destroy themselves by manipulating their rotational speeds (Bumgarner, 2010).

Israel, through Unit 8200[23], has been speculated to be the country behind Stuxnet in many media reports and by experts such as Richard A. Falkenrath, former Senior Director for Policy and Plans within the US Office of Homeland Security (Markoff, 2010). Yossi Melman, who covers intelligence for the Israeli daily newspaper *Haaretz* and is writing a book about Israeli intelligence,

[22] Cybertage is sabotage committed in cyberspace. It is a deliberate damage caused to a computer system or to data stored on a computer system by a computer hacker or by a deliberately planted computer virus.

[23] Unit 8200 is an Israeli Intelligence Corps unit responsible for collecting signal intelligence and code decryption. Military publications include references to Unit 8200 as the Central Collection Unit of the Intelligence Corps, and it is sometimes referred to as Israeli SIGINT National Unit.

also suspected that Israel was involved, noting that Meir Dagan, the former (up until 2011) head of the national intelligence agency, Mossad, had his term extended in 2009 because he was said to be involved in important projects. Israel expected that Iran would have a nuclear weapon in 2014 or 2015, at least three years later than earlier estimated. (Bronner & Broad, 2010).

Israel has not publicly commented on the Stuxnet attack but confirmed that cyberwarfare is now among the pillars of its defense doctrine, with a military intelligence unit set up to pursue both defensive and offensive options. When questioned whether Israel was behind the virus in the fall of 2010, some Israeli officials broke into wide smiles, fueling speculation that the government of Israel was involved with its genesis (Broad et al, 2010). American presidential advisor Gary Samore also smiled when Stuxnet was mentioned, although American officials have indicated that the virus originated abroad (Broad et al, 2010). According to *The Telegraph*, Israeli newspaper *Haaretz* reported that a video celebrating operational successes of Gabi Ashkenazi, retiring IDF Chief of Staff, was shown at his retirement party and included references to Stuxnet, thus strengthening claims that Israel's security forces were responsible (Christopher, 2011).

Aftermath

The majority of the world powers like the US, China, France and Germany had been attempting to get Iran to sign a nuclear deal even way before the Stuxnet attack of 2010. When Iran refused to back down on its nuclear program, the country was slammed with sanctions by the UN in 2006 which were followed by similar sanctions by the US and the EU. These sanctions, primarily on Iran's oil business, weapons sales and financial transactions, severely hurt Iran’s economy. As one of the largest producers of crude oil, prices went through a volatile period which hurt the Iranian economy (Seth, 2019).

After the Stuxnet attack of 2010, Iran came to the negotiating table to discuss its nuclear program. The deal laid out a lengthy process spanning over 15-25 years that would be supervised by an eight-member committee, including Iran, the US, Britain, France, Germany, Russia, China, and the EU. In a nutshell, the agreed-upon nuclear deal aimed at limiting Iran's ability to produce a nuclear weapon, in exchange for the removal of various sanctions imposed on it internationally.

The supporters of the nuclear deal at the time which include the US and its allies affirm benefits, which include the best-possible guarantee from Iran that it will refrain from producing a nuclear arsenal. It was, at the time, an important step toward establishing peace in the Middle East region, particularly in the context of ISIS and the role of oil in Middle East economies.

To make nuclear bombs, the uranium ore mined from the earth needs enrichment to either uranium-235 or plutonium. Uranium ore mined from the earth is processed via devices called centrifuges to create uranium-235. Uranium ore is processed in the nuclear reactors which transform it into plutonium. Under the deal, Tehran would reduce the number of centrifuges to 5,000 at the Natanz uranium plant – half the current number. Nationwide, the number of centrifuges would reduce from 19,000 to 6,000. The enrichment levels would be brought down to 3.7 percent, which was much lower than the 90 percent needed to make a bomb. The stockpile for the low-enrichment uranium would be capped to 300 kilograms for the next 15 years, down from the present 10,000 kilograms. All these measures served to restrict Iran's capability to make a nuclear bomb and would ensure nuclear power usage is limited to civilian use only (Seth, 2019).

As the deal was finalized, a UN Security Council resolution was agreed upon. By August 15, 2015, Iran would submit written responses to the questions raised by the International Atomic Energy Agency (IAEA), about its nuclear program and developments. Additionally, it allowed monitoring of its facilities by IAEA inspectors on or before October 15, 2015.

After the deal was signed by Iran, the oil embargo that prevented the import of oil from Iran was removed, which was not without its effects. The U.S. and EU lifted oil and trade-related sanctions. Foreign companies began to purchase oil from Iran, U.S. companies located outside the U.S. were authorized to trade with Iran, and imports of selected items from Iran were permitted, which had a particular effect on international business (Bajpai, 2015).

Simultaneously, sanctions on Iran’s banking and financial systems were dropped. It enabled the immediate release of around $100 billion currently lying frozen in Iranian bank accounts overseas. Immediately after the announcement, government officials from major European countries began visits to Iran to explore business opportunities (Seth, 2019).

Some of the main challenges faced by Iran during the sanction period were Iran's shrinking GDP, high inflation (between 50 percent to 70 percent in 2013), and the nation being cut-off from

world economic systems. All such economic challenges drastically improved after the agreement. Lifting sanctions allowed the movement of huge supplies of oil from Iran, which was thought to be sitting on large stockpiles due to years of imposed sanctions. International oil companies like France's Total and Norway's Statoil operated in Iran for years before sanctions were imposed, changing the tide for those countries and other top oil producers in the world (Investopedia, 2019).

Conclusions

In conclusion, activities of sabotage have always been part of the armory of conflicting nations. The only difference now is that it has evolved into the cyber domain. Due to the evasiveness and difficulty in attribution involved in this domain, it has become somewhat easier for nation-states to maintain a level of anonymity while also achieving their self-interest objectives. While the common practice at the moment is that the so-called power supper nations wield the higher cyber capabilities, it is hard to argue that the future of sabotage lies in the cyber domain and as such smaller nation states may be making a play to level the playing field.

While it may be difficult to say for sure who the original mastermind of the Stuxnet attack on Iran's nuclear facilities could be. Fingers have been pointed at both the US and Israel but due to the difficulty of attribution involved in cyber cases, one cannot say for sure the role both parties played in the grand scheme of things. What appears certain though is that back in 2010, both U.S. and Israel wanted Iran to give up its nuclear program. It is believed the U.S. and Israel share similar motives designed not to destroy Iran's nuclear program outright but to set it back for a while to buy time for sanctions and diplomacy to take effect. While Stuxnet didn't significantly set back the Iranian program, due to its premature discovery, it did help buy time for diplomacy and sanctions to bring Iran to the negotiating table. That strategy was successful in helping to bring Iran to the negotiating table, and ultimately resulted in an agreement with the country in 2015.

Stuxnet also changed the nature of warfare and launched a digital arms race. It led other countries, including Iran, to see the value in using offensive cyber operations to achieve political aims, a consequence the U.S. has been dealing with ever since. Further arguments can be made of the success and failure of the Stuxnet worm but what is certain is that cyber played a major role in sabotaging a great deal infrastructure in Iran's nuclear facilities and for that reason, cyber's role as a major instrument in sabotage was greatly vindicated.

Conclusion

Introduction

At the beginning of this thesis, the aim was to establish how cyber as a tool was used in foreign relations. After comprehensive studies on cyber in war, as a tool for interference, as a tool for influence and as tool for both espionage and sabotage, it is safe to say that justice has been done to the subject matter. In each of the cases studied, there was motive behind the use of cyber to achieve self-interest objectives. Whether these objectives were successful or not remains a debate.

Due to the problems existing in cyber-space, such as the problem of attribution, smaller countries could perceive this space as a place where they could increase and enforce their power in international relations. On the other hand, bigger countries still have more sources to invest in cyber capabilities and will have a lower level of reluctance for conducting a counter attack. So even though there might be reasons why a small state would prefer engaging in a cyber-war over a conventional war, the existing power balance between smaller and bigger states is still present in cyber-space. This is evident in the Russia-Georgian case study where Russia is seen as a power who can easily engage in and defeat a smaller country like Georgia.

The primary objective of Russia in the Georgian case study was to "isolate and silence" the Georgians. The assaults from the cyber-attacks had the effect of silencing the Georgian media and isolating the country from the global community. One glitch in the Russian masterplan was their failure to put into perspective that as of 2008 Georgia was not highly dependent on informational technology, seven internet users per hundred people as compared to fifty-seven per hundred in Estonia and thirty-two per hundred in Lithuania (Rondeli, 2009). The cyber-attack had no serious detrimental effect for the state. However, the Kremlin still partly managed to muffle the information channels and establish a Russian narrative about the Russia-Georgia war.

The use of cyber for influence as seen in the Estonia case study may be said to have had positive outcomes. Prior to the incident, cyber-attacks had not been seriously considered as an imminent threat to the state or its citizens. There was no common code of conduct or universal agreement between policy makers. For example, it was not defined if this kind of an offence would qualify as an attack against a member state of NATO and hence activate collective defense under Article 51. It was not even clear if a state could legitimately respond to cyber-attacks.

But there is no bad without good. The country learned and gained from the experience. Now, over a decade later, Estonia has become a global heavyweight in cyber security-related knowledge, advising many other states on the matter. The country has signed agreements on developing training and cooperation in cyber security with Austria, Luxembourg, South Korea and NATO. In December 2016, NATO organized its largest cyber defense exercise in Estonia. Named Cyber Coalition 2016, the three-day event attracted more than 700 cyber defenders and legal experts, government officials and military officers, academics and industry representatives, participating from dozens of locations across the alliance and partner nations (e-estonia, 2017).

While the main objective of Russia for allegedly orchestrating the attacks was to destabilize the Estonian society and to undermine the Estonian economy in an effort to weaken its ties to the European Union and the North Atlantic Treaty Organization, it can be argued that Russia's efforts ended driving Estonia to NATO and the EU. Today, Estonia is much stronger than it was before the cyber influence from Russia.

The case of cyber interfering in the affairs of another state creates a real complicated situation. This is so because the case study, the US election, involves two nations with strong cyber counter attacking capabilities. The fact that cyber was used to influence an election process makes it all the more intricate. Russia's reasons for favoring Trump ahead of Clinton is very much due to the fact that Russia perceived a Trump presidency might throw the U.S into chaos and leave Russia to reign after the ruins. It is still early days of the Trump's presidency, but nothing shows that the U.S would be crippling Russia anytime soon.

What is certain from the Russia vs US case study is that states can counter cyber election interference. They can protect a voting infrastructure. They can also enlist the private sector to help counter the dissemination of information emanating from foreign adversaries. But each of these solutions is, admittedly, incomplete. This is, in part, due to the framework of international law in which states can operate in order to redress wrongdoing surrounding election interference. States' most critical prerogative, then, should be recognition of limitations of what an international legal structure built for kinetic attacks can do. Because of the limitations of the present system, states should be incentivized to contribute to the development of new law addressing cyber

interference in elections. Importantly, states should start by reexamining the test for violations for the norm of non-intervention and for violations of sovereignty.

The Stuxnet attack on Iranian nuclear facilities was an interesting case study. Despite the swift and effective disarmament of the virus and the physical harm of the attack that was limited to covertly disabling Iranian centrifuges, the use of cyber for sabotage in this case revealed several fundamental questions. The attack had the capability of starting a war and can be perceived as possible cyber-warfare. There was no on-going armed conflict, which means the U.S. executed an attack in peacetime. The Iranian infrastructures could have been physically damaged. The consequences could even go further than this. When one anticipates a cyber counter attack, the outcomes are endless. Iran could attack United States' installations and troops in surrounding countries such as Iraq. It could have disrupted the flow of oil out of the Gulf region, with escalating oil prices as an aftereffect. The international community could have gotten involved, accelerating and sophisticating this conflict. This event has definitely given incentives to countries to arm themselves more against these attacks and invest in cyber capabilities, whether offensive or defensive. The possibility of a back and forth conflict with potential disastrous outcomes.

The use of the China vs US case study of the cyber in espionage was pertinent particularly because of the tensions between the two nations. China and the U.S. currently compete in terms of trade, technology, nuclear power and several other important sectors of the world order. The U.S. prides itself on being the world superpower while holding a firm notion of being ahead of China in all of the sectors mentioned above. It can be argued that China wanted to get even with the U.S. and thus its reason for using cyber in its espionage efforts to steal state secrets from the U.S. How successful were their efforts remains to be seen but what is certain is that relations between both nations have never been more volatile as they are now.

A more credible strategy of cyber deterrence, which could be extended to U.S. allies and thus strengthen the alliance system, would result from a greater focus on how the United States deals with the issues of attribution and norms. At the moment, either the U.S. government has no reliable evidence that China is behind the OPM thefts, or it does have such evidence, but it cannot disclose this without damaging the intelligence instruments with which the evidence was collected. In the latter case, the United States should at least say so and build up a track record of making credible statements on suspected cyber attackers, which should be supported by publicly available evidence

as soon as possible. Moreover, if the U.S. government no longer promoted the notion that foreign intelligence-gathering for national security purposes is legitimate, and at least scaled down its intelligence operations against foreign governments, it would become easier to take action in instances such as the OPM breach. While the danger of escalation would still be there, this would open the way for the United States to take overt rather than covert measures against China (assuming the Chinese government is indeed responsible and that the United States has evidence of this).

Collusions

The only, and a rather far-fetched, way of stopping a potential cyber-war is limiting the free open internet, where everyone can be anonymous and express their selves or do anything they want. This infringes upon a cornerstone of democracy, where freedom of speech is granted. Limiting the use of cyber in the West (US, Canada and the likes) is not an obvious given and will bump into huge waves of protest. This also applies looking at the difference in efforts for cyber regulations. Countries of the East (Russia, China and the like) are more occupied in regulating the open internet, while the regulation of cyber in the West is an extremely difficult, controversial and sophisticated action. It all depends upon how a country reacts to another country. This reaction is stimulated by political standpoints and based on a state's own principles. Information is something the West perceives as a strength, in comparison to the East where information is seen as a danger and exploited as a weapon to manipulate foreign governments.

The argument over the role which cyber plays in foreign policy of nation States might carry on for a while but what is most important is that cyber is a tool. How nations choose to use it remains open for debate.

References

Abrial, S. (2011). "NATO Builds Its Cyberdefenses," International Herald Tribune, February 28, 2011, available through LexisNexis.

Abkhazia, S. (1992). *The history of Georgia: post-communist Georgia.* Retrieved from: https://sites.google.com/site/historyofgeorgia/home/post-communistgeorgia

Advisory Council on International Affairs. (2011*). Advisory reports on cyberwarfare*. Retrieved April 5, 2017, from http://aivadvies.nl/6ct/publications/advisory-reports/cyber-warfare.

Alex Michael. (2010). *Cyber probing: the politicization of virtual attack*

Alexander, D. (2013). *Cyber threats pose 'stealthy, insidious' danger*. Reuters May 31, 2013

Andress J. & Winterfeld S. (2014). *Cyber Warfare (Second Edition).* Retrieved on 2nd September, 2019 from: https://www.sciencedirect.com/topics/computer-science/conventional-warfare

Andy Greenburg (2017), *Everything We Know About Russian Election-Hacking, Wired* Retrieved from: https://www.wired.com/story/russia-election-hacking-playbook/.

Arimatsu, L. (2012*). A treaty for governing cyber-weapons: Potential benefits and practical limitations. In 2012 4th International Conference on Cyber Conflict* (CYCON 2012) (pp. 1–19).

Arquilla, J., & Ronfeldt, D. (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. Rand Corporation.

Ashmore, W. C. (2009). *Impact of Alleged Russian Cyber Attacks*.

Assaf O. & Siboni G. (2016), *Guidelines for a National Cyber Strategy*, Memorandum No. 153 (Tel Aviv: Institute for National Security Studies), 18-19.

Assange, J. (2010). *Why the world needs WikiLeaks.* TED. Retrieved from https://www.ted.com/talks/julian_assange_why_the_world_needs_wikileaks

Bajpai P. (2019). *How embargos affect international businesses (XOM, BP)* Retrieved from: https://www.investopedia.com/articles/investing/053115/how-embargoes-affect-international-business.asp

Bannister A. (2018). Cyber Security Trends: State-sponsored espionage and sabotage to shape 15 cybersecurity threats to beware in 2019. Retreived on July 31, 2019 from https://www.ifsecglobal.com/cyber-security/15-cybersecurity-threats-beware-2019/

BBC. (2016). *MH17 Ukraine plane crash: What we know.* BBC News. Retrieved from http://www.bbc.com/news/world-europe-28357880.

Bemelmans-Videc, M.-L., Rist, R. C., & Vedung, E. O. (2011). Carrots, Sticks, and Sermons: *Policy Instruments and Their Evaluation* (Vol. Chapter 1). Transaction Publishers.

Benschop, A. (2017). *CYBEROORLOG*. Retrieved February 24, 2017, from http://www.sociosite.org/cyberoolog.php.

Boothby, W. H. (2015). Deception in the modern, cyber battlespace. In J. D. Ohlin, K. Govern and C. Finkelstein (Eds.), *Cyberwar: Law and ethics for virtual conflicts*. New York: Oxford University Press, 195-214.

Bové, L. (2017). *België krijgt allereerste cybernoodplan.* Retrieved April 30, 2017, from http://www.tijd.be/politiek-economie/belgie-federaal/Belgiekrijgt-allereerste-cybernoodplan/9888045.

Brangetto P. and Veenedaal M.A (2016), *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations* (Tallinn: NATO Cooperative Cyber Defence Centre for Excellence, 8th International Conference on Cyber Conflict, 2016): 117, 121–122, 124.

Broad, William J.; Sanger, David E. (2010). "*Worm in Iran Can Wreck Nuclear Centrifuges"*. The New York Times.

Broderick, R. (2019). "Here's Everything the Mueller Report Says About How Russian Trolls Used Social Media". *BuzzFeed News*. Retrieved August 27, 2019.

Bronner E. & Broad W.J. (2010). "In a Computer Worm, a Possible Biblical Clue". NY Times. Software smart bomb fired at Iranian nuclear plant: Experts". Economictimes.indiatimes.com. 2

Bellis M. (2018). *ARPANET: the world's first internet.* Retrieved July 30, 2019, from https://www.thoughtco.com/arpanet-the-worlds-first-internet-4072558

Bender, J. (2016). *These are the 6 countries on board with Russia's illegal annexation of Crimea* Available at: https://www.businessinsider.my/six-countries-okay-with-russias-annexation-of-crimea-2016-5/#3M6jV8IRi7e5P5vd.97

Berg, Eiki and Saima Oras (2003) 'Kümme aastat Eesti-Vene piiriläbirääkimisi' [Ten Years of Estonian-Russian Border Negotiations], pp. 45-75 in Andres Kasekamp (ed.), Estonian Foreign Policy Yearbook 2003, Tallinn: Estonian Foreign Policy Institute

Bortknik S. (2013). *Five interesting facts about the Morris worm for its 25th anniversary*. Retrieved 25th August 2019 from: https://www.welivesecurity.com/2013/11/06/five-interesting-facts-about-the-morris-worm-for-its-25th-anniversary/

Breene, K. (2016). *Who are the cyberwar superpowers?* Retrieved April 25, 2019, from https://www.weforum.org/agenda/2016/05/who-are-thecyberwar-superpowers/.

Breuninger, K. (2019). *MUELLER PROBE IS OVER: Special counsel submits Russia report to Attorney General William Barr.* www.cnbc.com. Retrieved March 22, 2019.

Broadhurst, R. (2006). *Developments in the global law enforcement of cyber‐crime. Policing: An International Journal of Police Strategies & Management,* 29(3), 408–433. https://doi.org/10.1108/13639510610684674.

Bumgarner J. (2010). *Computers as Weapons of War (PDF).* IO Journal. Archived from the original (PDF) on 19 December 2011. Retrieved 30 May 2019.

Bumgarner J. and Borg S. (2009) *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008.* U.S. Cyber Consequence Special Unit

Business Insider (2013)."The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought". 20 November 2013.

CACI International. (2008). *Dealing with today's asymmetric threat to US and global security*. CACI International. 12.

Cairney, P. (2013). *Policy Concepts in 1000 W ords.* Retrieved April 16, 2017, from https://paulcairney.wordpress.com/2013/11/11/policy-concepts-in1000-words-the-policy-cycle-and-its-stages/.

Carr, J. (2009). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media, Inc.

Carr, J. (2012). *The myth of the CIA and the Trans-Siberian pipeline explosion.* Available at: http://jeffreycarr.blogspot.com/2012/06/myth-of-cia-and-trans-siberian-pipeline.html

Caso, J. S. (2014, June). *The rules of engagement for cyber-warfare and the Tallinn Manual: A case study.* Paper Presented at the IEEE 4th Annual International Conference, Hong Kong, China.

Christoper W. (2011). *"Israeli security chief celebrates Stuxnet cyber-attack"*. The Telegraph. London.

Chumburidze, D. (2010). *The history of Georgia: Georgia under the Soviet Union.* Retrieved from: https://sites.google.com/site/historyofgeorgia/home/georgiaunderthesovietunion

Clark K.W. & Levin P.L. (2009), *"Securing the Information Highway: How to Enhance the United States' Electronic Defenses,"* Foreign Affairs, Vol. 88, No. 6, pp. 2–10.

Clarke, R. A., & Knake, R. (2011). *Cyber War: The Next Threat to National Security and What to Do About It* (Reprint edition). New York: Ecco.

Clausewitz, C. von. (1989). *On War*. Princeton University Press.

CNN. (1999). *Serb supporters sock it to NATO, U.S.* Retrieved April 8, 2017, from http://edition.cnn.com/TECH/computing/9904/06/serbnato.idg/index.html.

Coolsaet, R. (2016*). "All radicalization is local": the genesis and drawbacks of an elusive concept.*

Corbin K. (2009) *Lessons from the Russia-Georgia Cyberwar. Internetnews.com*. Real time IT news.

Cordesman, A. (July 2006). Iran's Support of the Hezbollah in Lebanon, *Center for Strategic and International Studies*, 15.

Craig Forcese (2016). "Hacked" US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards? JUST SECURITY Retrieved from: https://www.justsecurity.org/35652/hacked-election-international-law-silentfaced-clatter-cyrillic-keyboards/.

Crilley, K. (2001). *Information warfare: new battle fields Terrorists, propaganda and the Internet.* Aslib Proceedings, 53(7), 250–264. https://doi.org/10.1108/EUM0000000007059.

Cyrus Farivar (2009). *A brief examination of media coverage of cyberattacks {2007 – present)*

Czosseck, C., Ottis, R. and Talihärm, A.M., (2013). *Estonia after the 2007 cyber-attacks: Legal, strategic and organisational changes in cyber security*. Case Studies in Information Warfare and Security: For Researchers, Teachers and Students.

Danielle Kurtzleben (2016). Contrary to Trump's Tweet, Russian Hacking Came Up Before Election (A Lot), NATIONAL PUBLIC RADIO Retrieved from: http://www.npr.org/2016/12/12/505261053/13-times-russian-hacking-cameup-in-the-presidential-campaign.

David Sanger (2016). U.S. Officials Defend Integrity of Vote, Despite Hacking Fears, N.Y. TIMES Retrieved from: http://www.nytimes.com/2016/11/25/us/politics/hacking-russia-election-fears-barack-obama-donaldtrump.html.

Deb Riechmann and Russ Byoum (2017). Report: Russian Hackers Attacked Election Software Supplier, Time Retrieved from: http://time.com/4806709/russia-hack-election-donald-trump-nsa-reality-winner/.

De Bruycker, M. (2010). *Cyber Defense.*

De Redactie. (2015). *Premier Michel stelt nieuw centrum voor cybersecurity voor.* Retrieved April 30, 2017, from http://deredactie.be/cm/vrtnieuws/binnenland/1.2479531.

De Wolf, L. (2017). *Hacker houdt woord: Tien afleveringen "Orange is the new black"* online. Retrieved May 6, 2017, from http://deredactie.be/cm/vrtnieuws/cultuur%2Ben%2Bmedia/media/1. 2966250.

Denning, D. E. (2001). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Networks and Net wars. The Future of Terror, Crime and Militancy,* 239–288.

Dipert, R. R. (2010). *The Ethics of Cyberwarfare*. Journal of Military Ethics, 9(4), 384–410. https://doi.org/10.1080/15027570.2010.536404.

Dinniss, H. (2012). *Cyber Warfare and the Laws of War*. New York: Cambridge University Press, 265.

E-estonia, 2017: *How Estonia became a global heavyweight in cyber security.* Available on: https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

Ellen Nakashima (2012). "Stuxnet was work of U.S. and Israeli experts, officials say". *The Washington Post*.

Eric Lipton, David E. Sanger and Scott Shane (2016). The Perfect Weapon: How Russian Cyberpower Invaded the U.S., N.Y. TIMES Retrieved from: http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

European Commission (2010). "The EU Internal Security Strategy in Action: Five steps toward a more secure Europe," November 22, 2010, available at: http://tinyurl.com/2cfnqg5 (ec. europa.eu/commission_2010-2014/malmstrom/ archive/internal_security_strategy_in_action_en.pdf).

Euronews. (2016). *Crimean Tartar event hit by cyber-attack in Lithuania.* Retrieved April 8, 2017, from http://www.euronews.com/2016/04/11/crimean-tartar-event-hit-bycyber-attack-in-lithuania.

Europe Institute. (2008). *Cyber War I: Estonia attacked from Russia*. Retrieved May 5, 2017, from http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.

Evron, G. (2017). *The First Internet War in Estonia: The postmortem I wrote, 10 years later*. Retrieved May 5, 2017, from https://hackernoon.com/thefirst-internet-war-in-estonia-the-postmortem-i-wrote-10-years-later72040f53620e.

Farah, T., Shojol, M., Hassan, M., & Alam, D. (2016). *Assessment of vulnerabilities of web applications of Bangladesh: A case study of XSS CSRF. In 2016 Sixth International Conference on Digital Information and Communication Technology and its Applications* (DICTAP) (pp. 74–78). Retrieved from: https://doi.org/10.1109/DICTAP.2016.7544004.

Featherly K. (2016) *Internet History Timeline: ARPANET to the world wide web.* Retrieved from: https://www.britannica.com/topic/ARPANET

Fernandez J.D. and Fernandez A.E. (2005) *SCADA systems: vulnerabilities and remediation.* Journal of Computing Sciences in Colleges.

Finkle, J. (2016). Shamoon virus returns in new Gulf cyber-attacks after four-year hiatus. Reuters. Retrieved from http://www.reuters.com/article/uscyber-saudi-shamoon-idUSKBN13Q38B.

France-Presse, A. (2019). Main points of Mueller report. Archived from the original on August 20, 2019. Retrieved April 20, 2019.

Fruhlinger J. (2018). Top Cybersecurity facts, figures and statistics for 2018. Retrieved on 25th of August, 2019 from: https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html

Fung, B. (2014). *"Cyber Command's exploding budget"* The Washington Post, January 15, 2014

Furnell, S. M., & Warren, M. J. (1999*). Computer hacking and cyber terrorism:*

Garamone, J. (2011). "Lynn: NATO Must Get Ahead of Cyber Threat," American Forces Press Service, January 25, 2011, available at: http://www.defense.gov//news/newsarticle.aspx?id=62572.

Geers, K. (2014). *Kosovo, Cyber Security, and Conflict Resolution.* Retrieved March 27, 2017, from http://www.2501research.com/newblog/2014/11/25/kosovo-conflict-resolution.

GCHQ (2019). www.gchq.gov.uk. Retrieved 10 May 2019.

Globalsecuritynewswire.org. (2010). *"Iranian Nuclear Program Plagued by Technical Difficulties"*.

Grabosky, P. N. (2001). *Virtual Criminality: Old Wine in New Bottles? Social & Legal Studies*, 10(2), 243–249. https://doi.org/10.1177/a017405

Graff G. (2017). *How a Dorm Room Minecraft Scam brought down the internet.* Retrieved on 25th of August, 2019 from: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

Graham R. (2017). *MalwareTech's arrest sheds light on the complex culture of the hacking world* Retrieved on 25th August, 2019 from: https://theconversation.com/malwaretechs-arrest-sheds-light-on-the-complex-culture-of-the-hacking-world-82136

Green, J. (2015). *Cyber Warfare: A Multidisciplinary Analysis* (Vol. Chapter 3: Attribution of cyber warfare). Routledge.

Gross, Michael Joseph (April 2011). "A Declaration of Cyber-War". *Vanity Fair*. Condé Nast.

Gürcan, M. (2012). Savaşın Evrimi ve Teorik Yaklaşımlar, A. Sandıklı(Ed.), *Teoriler ışığında Güvenlik, savaş, barış ve Çatışma Çözümleri*, İstanbul, Bilgesam Yayınlar, 71-133

Guri M., Mirsky Y., Elovici Y. (2017) *Attackers can make it impossible to dial 911* Retrieved from: https://theconversation.com/attackers-can-make-it-impossible-to-dial-911-67980

Gutman Y. (2018). *The Rise of Cyber Espionage and Sabotage via the Internet of Things* Retreived on July 31, 2019 from https://www.iotcentral.io/blog/the-rise-of-cyber-espionage-and-sabotage-via-the-internet-of-thin

Herr, T. (2013). *PrEP: A Framework for Malware & Cyber Weapons* (SSRN Scholarly Paper No. ID 2343798). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2343798.

Hammes, T.X. (2004). *The Sling and the Stone: On War in the 21st Century,* St. Paul: MN Zenith Press, 321.

Hansen, L., & Nissenbaum, H. (2009*). Digital Disaster, Cyber Security and the Copenhagen School* (SSRN Scholarly Paper No. ID 2567410). Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2567410.

Hughes, R. B. (2008). "NATO and Cyber Defence: Mission Accomplished?" Netherlands Atlantic Association, Amsterdam, Atlantisch Perspectief 8 (2008): 1, available at: http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf

Hayward, J. (2015). *Cyber-War Is Too Easy, Effective, and Deniable to be Stopped*. Retrieved May 2, 2017, from http://www.breitbart.com/biggovernment/2015/10/01/cyber-war-easy-effective-deniable-stopped/.

Hill C. (2003) *The Changing Politics of Foreign Policy*, Basingstoke: Palgrave Macmillan.

Ibid. (2010). "A Digital Agenda for Europe," May 19, 2010, 17–18, available at: http://tinyurl.com/2dyjfvn (ec.europa.eu/information_society/digital-agenda/ documents/digital-agenda-communication-en.pdf).

InfoSec Institute. (2016). *Cyber Warfare: From Attribution to Deterrence.* Retrieved April 23, 2017, from http://resources.infosecinstitute.com/cyber-warfare-from-attribution-todeterrence/.

Institute for Defense Studies and Analyses. (2016). *Defense, Deterrence, and Diplomacy*. Retrieved from https://www.youtube.com/watch?v=Df_XQ4JRN_g.

Institute for Science and International Security (2010). "IAEA Report on Iran" (PDF).

Institute for Science and International Security (2011)."Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report."

International Code of Conduct for information security (2011). Annex to letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/66/359, 14 September 2011.

International Strategy for Cyberspace (2011). *Prosperity, Security and Openness in a Networked World.* The White House, Washington, May 2011, pg 4 and 11

Investopedia (2019). *The world's top oil producers of 2017*. Retrieved from: https://www.investopedia.com/investing/worlds-top-oil-producers/

Irving Lachow and Courtney Richardson. (2006). *Terrorist use of the internet: the real story*

Jahanian F. and Mcpherson D. (2005) *The Zombie Roundabout: Understanding, Detecting and Disrupting Botnets* SRUTI (Steps to Reducing Unwanted Traffic on the Internet Workshop) 39 – 44

Kaplan, F. (2016). *Dark Territory: The Secret History of Cyber War. Simon and Schuster.*

Karatzogianni, A. (2008*). Cyber-Conflict and Global Politics*. Routledge.

Kelsey, J. T. G. (2008). *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.*

Kazemzadeh, M. (2007). Ahmedinejad's Foreign Policy, *Comparative Studies of South Asia, Africa and the Middle East, 27*(2), 446.

Keohane, R.O and Nye, J.S. (1987) "Power and Interdependence Revisited," International Organization 41:4 (Autumn 1987): 727–733, 737–740.

Kepes, B. (2016). *Cyberattacks are on the rise*. Retrieved April 25, 2017, from http://www.networkworld.com/article/3094363/security/cyberattacks-are-on-the-rise.html.

Keloe B. (1992). *Zen and the art of the internet.* Retrieved on 25th August, 2019 from http://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html

Kiely, E. and Robertson, L. (2019). "Kushner Distorts Scope of Russia Interference". Factcheck.org. Retrieved August 27, 2019.

Kim Zetter (2010). "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target".

K.M. Van Nispen, F. (2008). Public Policy Instruments. Retrieved April 16, 2017, from https://www.akademika.no/public-policy-instruments/franskmvan-nispen/guy-b-peters/9781858987446.

Kozlowski A. (2014). *Comparative analysis of cyber-attacks on Estonia, Georgia and Kyrgyzstan* http://eujournal.org/index.php/esj/article/v

Krebs Brain (2013) Report: *Russian Hacker Fueled Georgian Cyber Attacks*

Kumar, K., Murphy, D., & Hisgen, A. (2004). *Controlled takeover of services by remaining nodes of clustered computing system.*

Kushner, David (2014) "The Real Story of Stuxnet". *ieee.org*. IEEE Spectrum.

Lee T. (2013). *How a grad student trying to build the first botnet brought the internet to its knees.* Retrieved on 25th August, 2019 from: https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/

Lema, K., & Gopalakrishnan, R. (2017). *Bangladesh Bank heist was "state-sponsored*." Reuters. Retrieved from http://www.reuters.com/article/uscyber-heist-philippines-idUSKBN1700TI.

Levi, M., & Wall, D. S. (2004*). Technologies, Security, and Privacy in the Post-9/11 European Information Society*. Journal of Law and Society, 31(2), 194–220. https://doi.org/10.1111/j.1467-6478.2004.00287.x.

Lewis (2009). "The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict," Center for Strategic and International Studies, Washington, October 2009, 3 (n3), available at: http://tinyurl.com/yjzvlge (csis.org/files/publication/ 091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict. pdf).

Libicki, M. (2009). *Cyber deterrence and Cyberwar.* RAND Corporation. ISBN 978-0833047342.

Libicki, M. (2011). *Cyberwar as a confidence game.* Strategic Studies Quarterly, 1, 132 – 146.

Liff, A. P. (2012). *Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War*. Journal of Strategic Studies, 35(3), 401–428. https://doi.org/10.1080/01402390.2012.663252.

Lin, H. S. (2010). *Offensive Cyber Operations and the Use of Force. Retrieved* April 9, 2017, from http://jnslp.com/2010/08/13/offensive-cyber-operationsand-the-use-of-force/.

Lind, W.S., Nightengale, K., K. Schmitt J. F. and Sutton J. W. (Ekim 1989). The Changing Face of War: Into the Fourth Generation, *Marine Corps Gazette*, 22-26.

Lindstrom, N. (2019). "Why Pittsburgh is mentioned in the Mueller report". *Pittsburgh Tribune-Review*. Retrieved August 27, 2019.

Ilves, Toomas-Hendrik (1998) VIII Estonian Parliament's 7th session, 12.02.1998, http://www.riigikogu.ee/, November 2005

Lukas, Tõnis (2005) X Estonian Parliament's 5th session, 26.01.2005, http://www.riigikogu.ee/, November 2005

Luvaas, J. (2001). *Napoleon On the Art of War* (New York: The Free Press), 99-120.

Magee, T. (2017). *Does the World Need a Geneva Convention for Cyber Warfare?* Retrieved April 1, 2017, from http://www.techworld.com/security/doesworld-need-geneva-convention-for-cyber-warfare-3656996/.

Makarychev, Andrey (2004) 'Marginality or Provinciality? Pskov and Ivangorod at the Intersection of Russia's Trans-border Relations', DIIS Working Paper No. 18, Copenhagen: Danish Institute of International Studies

Mansfield-Devine, S. (2012). Estonia: what doesn't kill you makes you stronger. *Network security,7*, 12-20.

Marjz, F. (2006). *A multifaceted approach to understanding the botnet phenomenon*. Retrieved from /paper/A-multifaceted-approach-to-understanding-the-Rajab

Markoff, J. (2010). "*A Silent Attack, but Not a Subtle One"*. New York Times. Retrieved 27 May 2019.

Maurer T. (2011), *"The Case for Cyberwarfare,"* Retrieved July 30, 2019, from,

http://www.foreignpolicy.com/articles/2011/10/19/the_case_for_cyberwar.

Milosevic, N. (2015). *Case of the cyber war: Kosovo conflict*. Retrieved May 5, 2017, from https://www.linkedin.com/pulse/case-cyber-war-kosovoconflict-nikola-milo%C5%A1evi%C4%87.

Mirkovic J. and Reiher P. (2004) *a Taxonomy of DDoS Attack and DDoS Defense Mechanisms* ACM SIGCOMM Computer Communication Review 34, no.2, 39 - 53

Morin J. F and Paquin J, (2018). *Foreign Policy Analysis: A Toolbox*, Palgrave.

Morozov E. (2010) *Army of Ones and Zeros: How I became a Soldier in the Georgia-Russia Cyberwar*

Mostofa, H. (2017). *Urge to ratify the convention on cybercrime*. Retrieved April 8, 2017, from http://www.thedailystar.net:80/law-our-rights/lawvision/urge-ratify-the-convention-cybercrime-1382548.

NATO, parliamentary assembly. (1999*). Science and Technology Committee. Information Warfare and international Security.* Retrieved February 5 2017, from http://nato-pa.int/archivedpub/comrep/1999/as285stce.asp.

NATO. (2010). "Strategic Concept for the Defence and Security of the North Atlantic Treaty Organization," North Atlantic Treaty Organization (NATO), November 19, 2010, available at: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.

NATO. (2017). *Cyber defense*. Retrieved April 25, 2017, from http://www.nato.int/cps/en/natohq/topics_78170.htm.

Negroponte, N. (1995*). Being digital*. New York: Alfred A. Knopf.

Newman, L.H. (2016), *The Real Hacker Threat to Election Day? Data Deception and Denial, Wired* Available: https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial/.

New York Times (2017). Full Transcript and Video: James Comey's Testimony on Capitol Hill, Retrieved from: https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html?_r=0.

Nikiforova, Elena and Jevgenia Viktorova (2001) 'Shifting Borders within the Contested Borderland', in Eiki Berg (ed.) Negotiating Borders of Multiple Meanings, Tartu: Tartu University Press

Nozario J. (2010) *Georgia DDOS Attacks: A Quick Summary of Observations* Arbor SERT (Security Engineering and Response Team)

O'Day, A. (2004). *Cyberterrorism*. Ash gate.

Office of the National Counterintelligence Executive. (2011). Foreign Spies Stealing U.S. Economic Secrets in Cyberspace. Retrieved from http://www.cfr.org/cybersecurity/office-national-counterintelligenceexecutive-foreign-spies-stealing-us-economic-secretscyberspace/p31052.

O'neill, P. (2016). *Web War I: The cyberattack that changed the world.* Retrieved May 5, 2017, from https://www.dailydot.com/layer8/web-warcyberattack-russia-estonia/.

Ottis, R. (2016). Estonia 2007: Case study on cyber conflict

Pager, T. (2016). *Trump to look at recognizing Crimea as Russian territory, lifting sanctions.* Available at: http://www.politico.eu/article/donald-trump-to-look-at-recognizing-crimea-as-russian-territory-lifting-sanctions-putin/

Paletta, D., Yadron, D. And Valentino-Devries, J. (October 2015). Cyberwar ignites a new arms race: Dozens of countries amass cyberweapons, reconfigure militaries to meet threat. *The Wall Street Journal*. Retrieved from: http://www.wsj.com/articles/cyberwarignites-a-new-arms-race-1444611128. 21.02.2012

Panorama. (2012). Cyberwar. Retrieved March 10, 2017, from http://deredactie.be/cm/vrtnieuws/videozone/programmas/2.27106/2. 27142?video=1.1315987.

Parker, E. (2017*). Hack Job. Foreign Affairs,* (May/June 2017). Retrieved from https://www.foreignaffairs.com/reviews/review-essay/2017-04- 17/hack-job.

Paasi Anssi (1999) 'Boundaries as Social Processes: Territoriality in the World of Flows', pp. 69-89 in David Newman (ed.), Boundaries, Territory and Postmodernity, London: Frank Cass

Paul Woodward (2010). *"Iran confirms Stuxnet found at Bushehr nuclear power plant"*. Warincontext.org.

Polityuk, P. (2016). *Ukraine investigates suspected cyber-attack on Kiev power grid.* Reuters. Retrieved from http://www.reuters.com/article/usukraine-crisis-cyber-attacks-idUSKBN1491ZF.

Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom.* University of Illinois Press.

Presidential Policy Decision (2014). *U.S. Cyber Operations Policy.* Text of document available at www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-fulltext

Prohov, J. (2019). "Fake Tennessee GOP Twitter account cited as example in Mueller report". *WBIR*. Retrieved August 27, 2019.

Propaganda. (2017). Retrieved May 20, 2019, from https://www.merriam-webster.com/dictionary/propaganda

Radio Liberty (2012). *Clinton calls Eurasian Integration an effort to 'Re-Sovietize.*' Available at: https://www.rferl.org/a/clinton-calls-eurasian-integration-effort-to-resovietize/24791921.html

Raitasalo, J. (2005). The western war picture after the Cold War, in Jyri Raitasalo and Joonas Sipilä (eds), *Variable war*. National Defence University: Helsinki, 101–125.

Rajagopalan, M. (2014). *"China suggests U.S. may have fabricated evidence of cyber-attacks"* Reuters, May 29, 2014 (www.reuters.com/article/2014/05/29 us-china-usa-diplomacy)

Ralph Langner (2011). "Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon"

Renard, T. (2014). *The rise of cyber diplomacy: the EU, its strategic partners and cyber security.* Retrieved April 9, 2017, from http://www.egmontinstitute.be/publication_article/the-rise-of-cyberdiplomacy-the-eu-its-strategic-partners-and-cyber-security/.

Richard A. Clark and Robert Knake. (2010). *Cyber war: the next level threat to national security and what to do about it*

Rid Thomas (2012), *"Cyber War Will Not Take Place,"* Journal of Strategic Studies, Vol. 35, No. 1 pp. 5–32.

Rid, Thomas (2013). *Cyber War Will Not Take Place*. London: Hurst.

Rid, T., & McBurney, P. (2012). *Cyber-Weapons.* The RUSI Journal, 157(1), 6–13. https://doi.org/10.1080/03071847.2012.664354.

Roscini, M., & Trust, L. (2014). *Cyber Operations and the Use of Force in International Law*. OUP Oxford.

International Institute for Strategic Studies, Military Balance (2010). London: Routledge, 2010, 28–52, 119–173, 222.

Rondeli (2019). *The Cyber Dimension of the 2008 Russia-Georgia war.* August 8, 2019. Available at: https://www.gfsis.org/blog/view/970

Royal Higher Institute for Defence. (2017). What strategy to address hybrid threats? Conference 16 February 2017. Retrieved from http://www.rhid.be/website/index.php/88-english/conf2017-en/1308- conf-2017-02-16.

Rudner, M. (2017). *"Electronic Jihad": The Internet as Al Qaeda's Catalyst for Global Terror. Studies in Conflict & Terrorism*, 40(1), 10–23. https://doi.org/10.1080/1057610X.2016.1157403.

Ruus K. (2008), "Cyber War I: Estonia Attacked from Russia," European Affairs 9:1 (Winter/Spring 2008): Columbia International Affairs Online.

SAGE. (2017). *Information War: The War for the "Truthful" High Ground* | SAGE International Australia. Retrieved April 8, 2017, from https://www.sageinternational.org.au/general-discussion/information-war-the-war-for-the-truthful-high-ground-2/

Sanger, D. E., & Shane, S. (2016, December 9). *Russian Hackers Acted to Aid Trump in Election, U.S. Says*. The New York Times. Retrieved from https://www.nytimes.com/2016/12/09/us/obama-russia-electionhack.html.

Schell, B., & Martin, C. (2006*). Webster's New World Hacker Dictionary.* John Wiley & Sons.

Schwartz, M. (2017). *Bank Account Hackers Used SS7 to Intercept Security Codes.* Retrieved May 12, 2017, from http://www.bankinfosecurity.com/bankaccount-hackers-used-ss7-to-intercept-security-codes-a-9893.

Seth, S. (2019). *A guide to Iran nuclear deal.* Retrieved from:

https://www.investopedia.com/articles/investing/072715/dummies-guide-iran-nuclear-deal.asp

Shackelford S. & Bradner S. (2018) *Have you updated your toaster? Traumatic Approaches to Governing the Internet of Everything* Retrieved on 25th August, 2019 from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3208018

S. Karnouskos (2011). "Stuxnet Worm Impact on Industrial Cyber-Physical System Security". In: "37th Annual Conference of the IEEE Industrial Electronics Society Melbourne, Australia", 7–10 November 2011.

Sieber, U. and Brunst, P.W. (2007). Cyberterrorism—the use of the Internet for terrorist purposes (Strasbourg: Council of Europe Publishing, 2007), 161–166. Following the attacks, Estonia became one of the first countries in the world to develop a comprehensive national cyber-security strategy. See: "Cyber Security Strategy," Estonian Ministry of Defense, 2008, available at: http://tinyurl.com/5ruln4o (www.mod.gov.ee/files/kmin/img/files/ Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf).

Singer, P. and Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* New York: Oxford University Press, 160-165.

Sinisalu, A. (2008). *Propaganda, Information War and the Estonian-Russian Treaty Relations: Some Aspects of International Law*. Juridica Int'l, 15, 154.

Smith S., Hadley A., and Dunne T. (2008) *Foreign Policy: Theories, Actors, Cases*, 1st ed., Oxford: Oxford University Press.

Stark, Holger (2011). "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War".

Stent, A. (2008). "An Energy Superpower? Russia and Europe," in Kurt M. Campbell and Jonathon Price (eds.), The Global Politics of Energy (Washington: Aspen Institute, 2008), 78.

Steven Cherry & Ralph Langner (2010). "How Stuxnet Is Rewriting the Cyberterrorism Playbook". *IEEE Spectrum.*

Symantec (2010), Retrieved from www.symantec.com/security_response/ writeup.jsp?docid=2010-071400-3123-99. 18.02.2017.

Symantec (2014). "Exploring Stuxnet's PLC Infection Process".

Smith, B. (2017). *The need for a Digital Geneva Convention*. Retrieved April 30, 2017, from https://blogs.microsoft.com/on-theissues/2017/02/14/need-digital-geneva-convention/.

Sytas, A. (2016). *Lithuania said they found Russian spyware on its government computers.* Reuters. Retrieved from http://www.reuters.com/article/uslithuania-cyber-idUSKBN14B1PC.

Tabasky L. (2015). *The current state of cyber warfare.* Retrieved from: https://www.cybersecurity-review.com/articles/the-current-state-of-cyber-warfare/

Terlikowski, M. (2007). "Cyber-attacks on Estonia. Implications for International and Polish Security," Polish Quarterly of International Affairs 16:3 (2007): 75.

The Economist. (2017). The investigation into the Bangladesh Bank heist continues. Retrieved April 14, 2017, from http://www.economist.com/news/finance-and-economics/21719492- much-remains-unknown-sophistication-crime-clear

Thomas T. (2009) *The Bear went through the mountain: Russia appraises its five-day war in* Ossetia. Journal of Slavic Military studies 31 – 67

Thomsen, J. (2019). *"Mueller: Russia sought to help Trump win but did not collude with campaign"*. *The Hill*. Retrieved August 27, 2019.

Tiezzy, S. (2018). *US slaps cyberespionage charges on two Chinese intelligence officers.* December 21, 2018. Available at: https://thediplomat.com/2018/12/us-slaps-cyberespionage-charges-on-2-chinese-intelligence-officers/

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations*, p. 130. Tallinn: CCD COE Publications.

Trend Micro (2012). "STUXNET Malware Targets SCADA Systems".

Tsagourias, N., & Buchan, R. (2015*). Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing.

Tsyganok A. (2008) *Informational Warfare: a geopolitical reality.* Strategic Culture Foundation online magazine.

Turcan, M.& Ozpinar, N. (2009). "Who let the dogs out?": A critique of the security for hire option in weak states. *Dynamics of Asymmetric Conflict*, *2*(3), 143-171.

Tüür, Karmo (2005) 'Kommentaar: Miks Venemaa ja Eesti ei mõista teineteist' [Commentary: Why Russia and Estonia do not Understand Each Other], Pärnu Postimees, 14.10.2005, http://www.parnupostimees.ee/141005/esileht/valismaa/10059427.php

Ullricha J.B. and Lamb J. (2008) *Defacing websites via SQL Injection.* Network Security, vol. 2008, issue 1

United Nations. (1945). *Chapter VII*. Retrieved April 9, 2017, from http://www.un.org/en/sections/un-charter/chapter-vii/index.html.

United Nations. (2015). *Resolution 70/237*. Retrieved from http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/237.

UN General Assembly resolution (2012). *Developments in the field of information and telecommunications in the context of international security.* A/RES/67/27, 11 December 2012

UN General Assembly resolution (2013). *"Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security"* A/68/98, 24 June 2013.

UN General Assembly resolution (2014). *"Developments in the field of information and telecommunications in the context of international security"* A/RES/68/243, 9 January 2014

UN Institute for Disarmament Research, (2013). *The Cyber Index: International Security Trends and Realities*. Accessible at www.unidir.org pp1-2

UNODC. (2010). *Salvador Declaration.* Retrieved April 12, 2017, from http://www.un.org/en/conf/crimecongress2010/.

Valo, J. (2014). *Cyber Attacks and the Use of Force in International Law*. Master Thesis, University of Helsinki, Faculty of Law, Helsinki, 12.

Van der Meer, S. (2015). *Cyber Warfare and Nuclear Weapons: Game-changing Consequences?* Retrieved May 17, 2017, from https://www.researchgate.net/publication/311582858_Cyber_Warfare_and_Nuclear_Weapons_Game-changing_Consequences.

Vanity Fair (2011) "A Declaration of Cyber-War"

Walt S.M. (2010), *"Is the Cyber Threat Overblown?"* Foreign Policy, retrieved on July 30, 2019, from http:// walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown.

Walter Coenraets (2017). Cybercrime: threats and (Belgian) law enforcement.

Washington Post (2015). *Donald Trump's immigration plan would wreak havoc on US society*. Available at: https://www.washingtonpost.com/opinions/donald-trumps-immigration-plan-ould-wreck-havoc-on-us-society/2015/08/17/19703368-451d-11e5-8ab4-c73967a143d3_story.html

Washington Post (2016). In Japan and South Korea, bewilderment at Trump's suggestion they build nukes. Available at: https://www.washingtonpost.com/world/asia_pacific/in-japan-and-south-korea-bewilderment-at-trumps-suggestion-they-build-nukes/2016/03/28/03eb2ace-f50e-11e5-958d-d038dac6e718_story.html

Wayback Machine (2009). Archived on 30 August 2009. Retrieved on 2nd of August, 2019.

Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2013). *Effective detection of sophisticated online banking fraud on extremely imbalanced data*. World Wide Web, 16(4), 449–475. https://doi.org/10.1007/s11280-012-0178-0.

WikiLeaks (2010). "Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation".

Wilkie, R. (2009). *Hybrid warfare: something old, not something new*. Air & Space Power Journal, 23(4), 13–18.

Winer S. (2019) '*Dutch mole' planted Stuxnet virus in Iran nuclear site on behalf of CIA, Mossad* Retrieved from: https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site-report/

Wolf N. (2016). *DDoS attack that disrupted the internet was the largest of its kind in history*. Retrieved on 25th August, 2019 from: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Yar, M. (2013). *Cybercrime and Society.* SAGE.

Yossi Melman (2010). *"'Computer virus in Iran actually targeted larger nuclear facility'"*.

ZDNet (2010) "Stuxnet attackers used 4 Windows zero-day exploits".

Zenko, M. (March-April 2011). The Future of War, *Foreign Policy,* 56-71.

Zetter K. (2011). *Cyberwar Issues Likely to Be Addressed Only After a Catastrophe*. Wired. Retrieved 18 May, 2019.

Zmjewski E. (2010) *Gerogia clings to the Net. Reneysis: the internet Intelligence Authority*