FORSVARET
Forsvarets høgskole

Deterrence of Cyberattacks

Gudbrand Søfferud

Master thesis

Forsvarets høgskole

Spring 2019

Forord

Denne masteroppgaven er et resultat av ti deler lesing, fire deler kildekontroll, åtte deler skriving, tre deler hastverk, to deler uro og seks deler nysgjerrighet. I tillegg kommer drøyt tredve liter kaffe.

Deadlinespøkelset har besøkt meg titt og ofte gjennom denne seansen. Jeg ønsker å rette en takk til veileder, Magnus Petersson for tålmodighet, gode råd og Zen. En takk også til hjemmelaget mitt; Therese, Anders, Sunniva, Sigurd og Ole.

Temaet for denne oppgaven var noe jeg fattet interesse for under utdanningen, både fordi jeg ser på det som relevant og fordi jeg oppfattet det som et relativt uutforsket område som stadig er under utvikling. Dessverre er temaet er så altfor stort for en enkelt masteroppgave og det krever mer plass og tid enn et masterstudium kan gi. I lønnlig håp om at oppgaven kan gjøre nytte for seg utover det lille miljøet i Norge, er oppgaven skrevet på engelsk.

Sammendrag

Cyberområdet har gitt verden nye muligheter for kommunikasjon, kontroll og produktivitet. Det har effektivisert samfunnet og innvirker på alt fra forsvar, regjering, forskning og finans til helse, industri, energi og forsyning. Selv privatlivet har endret seg og vil fortsette å endres som følge av et inntog av strømmetjenester, IoT , sosiale medier, bloggere og influencere.

Cyberområdet har også bragt med seg noen nisser på lasset. Trojanere gjenoppstår i form av ondsinnede dataprogrammer. Dagens troll sprer sine løgner uinnskrenket gjennom sosiale nettverk og svakheter i datasystemene har gitt angriperne på vestlig demokrati nye innfallsvinkler.

Det er tre hovedtrusler som truer samfunnet gjennom cyberspace; spionasje, sabotasje og undergravende virksomhet. Denne oppgaven forsøker å vise at for å kunne redusere trusselen fra angrep i cyberspace, må dette søkes løst gjennom internasjonale avtaler, nasjonale poitiske veivalg, et integrert cyberforsvar både på nasjonalt og internasjonalt plan og gjennom avskrekking.

Abstract

Cyberspace has given the world unprecedented opportunities for communication, control and productivity. It has transformed and rationalized every public and private sector from government, defense, health and science to finance, industry, transport and production.

Even the private sphere has been influenced as a result of connected appliances, streaming and social media, bloggers and influencers.

Nonetheless, cyberspace has brought out some more sinister phenomena. Trojan horses have resurrected as malware and troll factories now spread their lies unhindered through social media. The enemies of Western democracy have gained a new vector of attack.

There are three main threats to society that have gained new access to society through cyberspace; espionage, sabotage and subversion.

This thesis intends to show that the endeavour to reduce the threat of attacks in cyberspace must be sought through international agreements, national policy, a concerted national and international cybersecurity and deterrence.

Index

1.Introduction

1.1. Background

Cyberspace has revolutionized the way we interact. From a humble start, it has changed the way we control our machines to the way we communicate with each other. Critical infrastructure, ranging from transportation, energy, food and water supply to healthcare, finance, government and military systems have been and are becoming more and more connected, giving unprecedented opportunities for situation awareness and accuracy.

Created within the sphere of Western liberalism, the Internet was made free for all. Unregulated, without any form of censorship or control, it has allowed a boundless sharing of information and opinion. This freedom and the ever- increasing speed of interchange has impacted political life, creating new ways for politicians to reach the electorate, while at the same time giving the electorate a voice in return. In business life, every industry and marketplace have been challenged and changed. It has affected our personal lives, altering the way we receive information, shop our groceries and clothes to the way we consume entertainment and communicate with each other.

Cyberspace has not come without a host of problems. Hacktivism, viruses, Trojans, DDoS, phishing and ransomware have all become household names. Former director of the CIA, Leon Panetta, urged the strengthening of cyber security measures, saying that cyberspace "could also be "the battlefield of the future".(Ravindranath, 2014) Warnings are rife about how attacks in cyberspace can turn a state's weapons impotent, its military command and control systems useless, shatter the civilian social fabric and leave a country's industry and infrastructure in tatters.

There are methods to protect against these attacks, but evidence show that they do not stop them from reappearing in new guises. This effectively constitutes a state of continual weapons race between the attacker and the defender.

The sovereignty and autonomy of a state are under pressure not only from direct cyber-attacks to government bodies. Private companies of vital national value have equally become attainable targets. These companies have to fend for themselves against cyber-attacks, a task they are unequal to perform. They are not capable to withstand hostile campaigns from

Advanced Persistent Threats[1] (APT). Erosion has also been caused by internationalization, where cloud computing and multinational companies slip away from a state's jurisdiction.

In order to understand how a state best can organize its collected efforts to create resilience and safeguard its sovereignty and its way of life, it is not sufficient to look only at the domestic scene. It is also necessary to look beyond the national borders to investigate what legislation, cooperation and vehicles of defense and deterrence that can reduce the hazards of cyberspace and defend a state's sovereignty.

1.2. Scope and research questions

Historically, deterrence has been used to safeguard a nation against hostile attacks, raising the bar for an attacker. Both defensive and offensive measures are tools used to deter an enemy. The essence of deterrence is to induce an aggressor to believe that the cost and the risk of an attack will too high and that the returns will be too low.

In cyberspace, the expenditure and resources necessary to carry out an attack are low, compared to kinetic attacks. The risk of retaliation has so far been negligible cyberspace and the benefits to be gained from of a cyberattack have been potentially large. If the reward of an attack is neither cost, resources or risk can dissuade an attacker, what opportunities are there for deterrence?

So far, there have been no cases where cyberattacks have escalated into war.

The goal of this thesis is to find out to what extent cyberattacks can be deterred. This will be done by examining various offensive and defensive measures and assessing their effectiveness as deterrent vehicles. The thesis will endeavour to answer the following questions:

- What are cyber-attacks and how do they threaten a state?
- How does deterrence of cyberattacks differ from deterrence of armed attacks?
- What vehicles of deterrence are relevant to employ against cyberattacks and what are their inherent strengths and weaknesses?

[1] Advanced Persistant Threat is the designation of hacker organizations that use continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences. APTs are generally seen as government- controlled.(Andress & Winterfeld, 2013)

1.3. Limitations

Volumes have been written about the threats in cyberspace and of deterrence in general.

In the endeavour to write a Master thesis on the deterrence of cyber-attacks, it is impossible to treat all sides of the subject in equal detail. The following limitations have been necessary to focus on the most important aspects of this subject.

The thesis will be limited to studying deterrence in the perspective of state sovereignty, focusing on Western democracies. Although the threats and vulnerabilities will be similar to all states, it is only Western democracies that are sufficiently open to divulge information on cyber-attacks. Another reason for this limitation is that when it comes to offensive measures, it is only the great powers that possess the necessary conventional and nuclear forces to escalate a conflict beyond certain levels. Among the Western democracies, we find the USA, Great Britain and France who all have a nuclear capability. In addition, NATO extends this ability to most of the other democracies. This limitation allows the thesis to explore strategies that are limited to them and unavailable to small or failed states.

The theories on deterrence are to a large degree influenced by the nuclear era. In the face of nuclear weapons, deterrence by denial was futile. As a result, deterrence theory was in general preoccupied with punishment. This left the field of scholarly debate on deterrence by denial relatively sterile. In the thesis, this is reflected by the shortness of the theoretical basis for denial, but denial is discussed in more detail in relation to cyberattacks, where defensive measures may prove less hopeless. International Relations (IR) theories have a bearing on the political side of cyber conflicts. Nevertheless, the scope of the thesis is the deterrence of cyber-attacks. It is not concerned with the reasons to why states resort to launch hostile operations in cyberspace. The thesis will not provide a thorough presentation or of IR theories.

Hostile actors proliferate in cyberspace. Many of them are criminals or political activists, but cybercrime and political activism will not be the scope of this thesis. They may be a threat to civilian life and can be used by Advanced Persistant Threats (APT) to blur the origin of an attack. Although private hackers, activist groups or criminals may aspire to threaten a state, they will not be discussed unless they pose a threat to the sovereignty of a state.

Cyber-attacks come in many guises, but for a state-actor, they can serve as instruments to reduce an adversary state's power and freedom of action. They manifest themselves in three main categories: espionage, sabotage and subversion. Although espionage can seriously reduce a state's edge in technology by stealing vital information[2], espionage cannot be defined as an act of war and it cannot be deterred. It will not be discussed in any detail in this thesis.

1.4. Disposition

The thesis will try to explain why this is the case by examining the nature of cyberattacks, their effects, how they are used and investigate why states have not been induced to declare war. This thesis is structured in the following way:

The research methodology and analytical framework is first presented, followed by an appreciation of the sources used in the thesis.

To set the context of the thesis, a general overview is presented to show how society has grown vulnerable by the incorporation of cyberspace.

This is followed by a description of four well-known cyberattacks. The four examples of attacks are chosen because they represent four main vectors of attacks. Three of these attacks, the Stuxnet, "Operation Orchard", and the Russian attack on the U.S. Presidential election were carried out with the intent and capability of damaging a state or reducing its influence, whilst the fourth shows how vital national interests can be attacked through the private sector.

- The Stuxnet attack on the Natanz nuclear facility. The case illustrates how cyberspace can be used to attack a national strategic capacity. It is also an example of how an attack can be tailored to a target.

- "Operation Orchard". The case of the Israeli attack on Syria in 2007, shows how cyber weapons can be used in war to gain tactical advantage.

- The Russian interference in the U.S. presidential election gives an example of how the fabric of society can be influenced and subverted through cyberspace.

- The "Lockergoga"- attack on Norsk Hydro in March 2019, although its origin is as yet undisclosed, serves as an example of how an attack on an important industry company

[2] In 2014, Su Bin, a Chinese national was arrested in Canada. Extradited to the USA, he was charged with the theft of *"military technical data, including data relating to the C-17 strategic transport aircraft and certain fighter jets produced for the U.S. military."*

can disrupt vital national interests. It also highlights the challenges to national strategy when the attacked company is multinational.

These attacks illustrate what types of threats that exist in cyberspace, how cyber weapons function and the ways they can be employed in international conflicts. They also exemplify how the emergence of cyberspace has created new vulnerabilities to a state and what obstacles may hinder response to such attacks.

Deterrence theory is next presented with a short introduction of the strategies used during the Cold War, which spurred the academic discussion on deterrence.

Outlining the measures that are or can be employed to counter a cyber threat, the fourth part of the thesis will consider the opportunities and constraints of cyber deterrence by discussing the strengths and weaknesses of offensive and defensive deterrent measures. This will include an appreciation of the use of International Law and its relevance to cyberspace.

In conclusion, the thesis will discuss to what extent cyberattacks can be deterred and suggest what measures that are most likely to reduce the threat of hostile behaviour in cyberspace.

1.5. Research methodology

The goal of this thesis is to advance the understanding of how cyberattacks can be deterred. In order to do so, it is necessary to answer the three research questions of the thesis. The first question is what a cyber-attack is and how it threatens a state. This necessitates a reduction of the myriad of different types of malware and attack methods into a few main categories. Four examples of cyberattacks are presented. Each of these attacks illustrates a specific threat, attack vector and target. This will explain how cyberattacks function, what vulnerabilities they exploit and what kind of damage they are capable of doing.

The second research question is posed in order to explore how deterrence of cyberattacks differs from deterrence of armed attacks. To do so, the theory of deterrence must be consulted. Its validity in cyberspace is shown in relation to the examples of cyberattacks presented with research question number one. This question is also explored further under the third research question.

The third research question queries what vehicles of deterrence are relevant to employ against cyberattacks and what their inherent strengths and weaknesses are. To answer this, the vehicles are examined under the headings of offensive and defensive measures. In the conclusion, the thesis argues that the deterrence of cyberattacks is a multifaceted endeavour, where both defensive and offensive measures are vital.

This thesis uses the qualitative method. This method is chosen because the thesis is mainly based on literary studies. The bulk of the literary sources are academic works, which gives validity to the thesis. On the other hand, literary sources raise some challenges as to the reliability of these sources. As pointed to under 1.3 Limitations, incidents in cyberspace do not age well, and that may also be the case of articles connected to them. Incidents that seem serious or important when they occur may turn out to be trivial when looked at from a distance. There is also the bias of interpretation. The analysis of an incident against a backdrop of several similar incidents may give a different interpretation than if the incident is unprecedented. To reduce the bias of interpretation, the case of the Stuxnet attack and the case of the Russian interference in the 2016 election examples have been chosen, both because they exemplify how cyber-attacks can be used against a state, and because they are well documented in several academic sources. That these sources are academic also increases their reliability when they show that there is a general consensus on the specific case.

The two other cases are less well documented.

For the case of “Operation Orchard”, there are few academic sources apart from the book “Cyber war will not take place” (Rid, 2013). This case has been chosen because it is one of very few cases where a cyberattack is documented to have played a part in armed conflict. Since there is very little information available to describe how the attack was carried out, the focus in this case is on what cyber-attacks can achieve in conjunction with physical attacks.

The Hydro case is new. The attack was announced in a press release on March 19th, 2019 (Hydro, 2019a) and investigation and forensic work is still ongoing. No scholarly work has been produced on the incident, and the security companies that cooperate with Hydro are reticent. This case has been included because it illustrates important issues in the deterrence of cyber-attacks. First, it is an example of how a state can be targeted through the private sector. Second, Lockergoga, the malware that was used in the attack is a new breed of ransomware that

Another problem with reliability arise when government documents are consulted. Since defence, security and deterrence are of vital interest to states, there are few unclassified documents that convey anything but general views. There is also a challenge that many of these documents are written for the public. The goal of these documents may serve other purposes than telling the truth. To reduce this bias, the documents have been scrutinized and correlated to theory and other sources.

1.6. Sources

The thesis relies mainly on literary sources, where the goal is to produce a nuanced analysis of the problems that a state faces from cyber-attacks, how these threats can be countered and the strengths and weaknesses of the deterrent measures.

The thesis uses scientific articles and scholarly sources to form the basis on deterrence theory. It must be noted that deterrence theory is a topic that has not been in vogue since the Cold War ended. As a result of this, most of the sources on deterrence antedate the appearance of cyberspace and are in general preoccupied with nuclear deterrence.

Cyberspace is relatively new and is in constant flux. This creates a problem with what cases that should be examined. Not all cyber-attacks are relevant to the discussion of deterrence. Due to the development of cyberspace, new programs and security flaws constantly appear. As a result of this, several cyberattacks that have received much academic attention are dated. The reason for this is that they were generally unsophisticated. Most of them involved no more than the defacing of web pages, spamming mail servers and congesting servers by DDOS- attacks. Although the novelty of these attack made headlines and caught the attention of scholars and laymen alike, they did little harm and little to threaten the sovereignty of a state. This makes the use of early attacks as examples problematic. New attacks may be far more sinister, but pose another problem in that there may not yet exist any scholarly debate or official documents about them. In such cases, newspaper articles, more or less informed, and security firm and government web pages, more or less candid, may be the only sources available. In these cases, caution in relation to reliability is maintained and sought improved by using several different sources.

2.The vulnerability of modern society

Prior to the introduction of cyberspace, sectors of vital national interest like energy, transport, health, finances, defense or government were difficult to manipulate by an adversary. Espionage entailed high personal risk and the control systems within the different sectors could not be manipulated except through physical intrusion and sabotage or by armed attacks. The defense of these systems were taken care of in two main ways: situation awareness and control. To some degree, imminent attacks or sabotage could be predicted by the international situation, through diplomacy and by the intelligence services. The outer perimeter of the state would be safeguarded by the armed services, whereas the police force would be responsible for upholding law and order and sustaining the cohesion of civilian life until higher levels of insecurity would require more resources from the armed forces like the Home Guard. Sabotage would trigger tighter defence of vulnerable, high-value targets vital to the state, giving resilience to society, as it would slowly be turned to a war footing. There was little opportunity for subversive action since the media was edited and run by national news houses or were state-controlled. In this situation, peacetime required little need for constant vigilance in most sectors.

Cyberattacks have changed this. Cyber weapons may be planted or launched in peacetime and have the capacity to disrupt communication, put entire sectors out of operation. Attacks in cyberspace can be performed with unprecedented speed, giving little warning and no time for countermeasures.

The military services were early adopters of digitization, but the efficiency of digital command and control systems has been leveraged across all industries, trade, transportation, government and finance. Cyberspace was built within the sphere of liberalism. It has no national boundaries and open communication, transparency, trust, rule- of-law and fair play have been taken for granted.

Digital products, the Internet and social media platforms were all built without any consideration that these liberties could be threatened. In this environment, national companies have been allowed to evolve unhindered into multinational companies, where little else than taxation is precariously kept under national jurisdiction.

Email and the Internet have been disruptive in the way information can be despatched and shared. This was seen as strengthening democracy and may have turned out to be instrumental in the popular risings in the Middle East.

At the same time, the introduction of E-mail and the Internet boosted the vulnerability of civilian society, as a host of viruses and worms could now be sown through emails and web browsers. The advent of social media platforms has opened up new opportunities for subversive actions, ushering in social engineering and information campaigns.

At the dawn of the Internet of Things (IoT), modern society has become, and continually grows more vulnerable to attacks in cyberspace. Because the diversity of components, systems and services in cyberspace have been modelled and configured to function in a hostile-free environment, it is the inherent lack of integral security of the targeted systems, or the victim's lack of routines and vigilance that is the direct cause of the vulnerabilities in modern society.

It is inevitable that a new low-risk vector for attack has been created when computers and automated processes assisting or replacing manpower, are connected to the Internet.

2.1. Cyber weapons

Basically, all cyber weapons function in the same way.

A target system is scanned for possible entry. If this is found, the system is infiltrated and by exploiting vulnerabilities basically, the payload of the attack is delivered.

Rid and McBurney have submitted a definition to what cyber weapons are. This distinguishes cyber weapons from crime and espionage: *"computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings"(Rid & McBurney, 2012).*

In order to fully grasp the threat of cyberattacks, it is necessary to understand that the toolbox of attackers is large, and that the tools are widely available. Proliferation of these tools is difficult to restrict. The leaked hacking tools from the NSA, auctioned off by "the Shadow Brokers" is an example of how both state-based hackers and private hackers can get hold of state-of-the-art software (Price, 2016). As a result of this, the ability to launch sophisticated attacks is not restricted to state-based hackers.

Once a system is infiltrated, there are three main actions that can be performed: espionage, sabotage or subversion. These actions need not take place at once. A backdoor can be created, giving the attacker the opportunity to control the attack remotely and commence an attack at a favourable moment. Whether the attack is carried out with a computer virus in order to steal information, destroy or interrupt a system through malware or using social media as an instrument to manipulate public opinion, it is the inherent vulnerability of the targeted system, or the victim's lack of vigilance that is the direct reason for the fall. There must be a weak link that can be exploited.

The Norwegian intelligence service issues a yearly report describing the threats to Norway. In the issue for 2019, China and Russia pose the largest threats. Their cyber operations have become more coordinated and effective than before. Targeted objects span from political institutions, military systems to research institutions and private high-tech companies. Russia's cyber operations have been aimed to undermine political processes and increase polarization within Europe and NATO through the use of false news, social media and influencing elections.(Etterretningstjenesten, 2019b)

2.2. Hackers, hacktivists and APTs

Most attacks in cyberspace are motivated by economical gain and are classified and prosecuted as crime. Cyberattacks can also be carried out with a political motive. When they are carried out by private persons or organizations, they are classified as "hactivism". States also use cyberspace as a political tool. State hackers are known as advanced persistant threats (APTs).[3] See Appendix A for a list of known APTs and their origin.

Attacks in cyberspace are common. The vast majority of infiltration attempts come through the mail system. A classic way to gain access is by including a program disguised as an attachment to an email, inducing the recipient to open it. Opening the attachment, the recipient unwittingly launches the program, which manipulates the system leaving it open for infiltration and exploitation. In 2017, F-secure stated in their report "state of cyber security" that 60 % of what they understood to be *"active reconnaissance traffic"* came from Russian IP addresses. Half of this traffic was searching for unprotected http/https ports.

> Attackers probe these ports in an attempt to look for vulnerable software that can be exploited in order to upload malware or otherwise compromise the device" "attackers can compromise a machine (such as by infecting a computer with malware) and then use it to conduct scans looking for additional targets "Worms, bots, and other types of malware programmed to automatically begin scanning for new targets after infecting a particular device are often spread in this fashion (F-Secure, 2017, p. 17).

[3] See appendix A for a list of known APTs with names, origin and known attacks.

Although the characteristics of cybercrime and hacktivism may use the same tools and share many of the characteristics of government-backed attacks, they do not have the same opportunities of insidious turmoil and sabotage. A state can protect its hackers and give them immunity from prosecution. Another difference between them is the economic power. A state far outstrips criminal and activist organizations in its ability to provide its hacker organization with funds, time, organization, manpower and resources. An example of this is can be seen in Appendix B. The appendix lists the known attacks attributed to APT 28 (GRU[4]) between 2015 and 2018. It is indicative of the variety of targets, methods, scope and capacity of a state- governed hacker network. This means that the cyber-attacks launched by a state on another state or its vital sectors are potentially more sinister than anything that a private hacker will be able to produce. This does not imply that private hackers can be dismissed. On There are situations when a private hacker might choose to launch an attack when a state would hesitate to do so.

For a state, the threshold for committing serious digital sabotage in peacetime is high, due to the fact that such operations can be interpreted as acts of war. Nevertheless, the way from capacity to actual use has been shortened (Etterretningstjenesten, 2019a).

[4] GRU is the foreign military intelligence agency of the Russian General Staff.

3.Attacks in Cyberspace

In this chapter, four types of attacks relevant to a state are presented. The examples illustrate how such attacks can be used, how they function, what targets they may strike, and the vulnerabilities they may exploit.

3.1. Stuxnet - attacking the system

Stuxnet is the best- known attack on a computer system and is an example of how an attack can be tailored to strike at a particular target.

In 2010, Iran experienced a rise in the malfunction of the centrifuges at its uranium enrichment plant in Natanz. Normally, it replaced up to 10 percent of its centrifuges a year, which amounted to about 800. Over a course of a few months, this had increased to between 1000 and 2000 centrifuges breaking down.

The Stuxnet worm was discovered, when the Belorussian computer security firm VirusBlokAda became aware of a computer in Iran caught in a reboot loop. The firm found out, that the virus had been launched in June 2009 and that it used a “zero-day” exploit in Windows Explorer to spread through infected USB sticks from one computer to another.

One of the driver files had used a valid signed certificate stole from RealTek Semiconductor, a hardware maker in Taiwan to pass as a trusted program from that company. Another driver file had a stolen certificate from JMicron Technology, which happened to be located in the same business park as RealTek. ESET, a security firm, wrote that such professional operations were rarely seen, testifying that the attackers had significant resources.(Zetter, 2011)

Stuxnet is a piece of malware, which was written expressly for targeting industrial systems, while using personal computers as an attack vector. Industrial systems are operated and controlled by specialized computers called Programmable Logic controllers (PLCs) in a three-tiered Industry Control System (ICS). In this system, the lowest tier consist of field devices, like engines valves etc. These are controlled by the second tier. The second tier consists of PLCs. They in their turn are directed by the third and topmost tier, called the Supervisory Control And Data Acquisition/ Human Machine Interface (SCADA/HMI)(De Falco, 2012).

The SCADA and PLCs at the Natanz enrichment plant, their architecture and programs were all delivered by Siemens.

The Stuxnet computer worm was aimed at the Siemens SCADA –programs. Infiltrating Microsoft Windows, the worm used a root kit to conceal the content of the malware. Next, the worm specifically sought out and compromised the Siemens Step 7 SCADA software, which controlled the PLCs.

Making sure that the Central Processing Unit (CPU) of the PLC were either type 6ES7-315-2 or 6ES7-417, it would check which types of field units that the PLC controlled.(De Falco, 2012)

Symantec has given further evidence to the sophistication of the Stuxnet:

- Stuxnet requires particular frequency converter drives from specific vendors, some of which may not be procurable in certain countries.
- Stuxnet requires the frequency converter drives to be operating at very high speeds, between 807 Hz and 1210 Hz. While frequency converter drives are used in many industrial control applications, these speeds are used only in a limited number of applications.
- Stuxnet changes the output frequencies and thus the speed of the motors for short intervals over periods of months. Interfering with the speed of the motors sabotages the normal operation of the industrial control process.
- Stuxnet's requirement for particular frequency converter drives and operating characteristics focuses the number of possible speculated targets to a limited set of possibilities.

  Relative to the typical uses of frequency converter drives, these frequencies are considered very high-speed and now limit the potential speculated targets of Stuxnet.

  Efficient low-harmonic frequency converter drives that output over 600Hz are regulated for export in the United States by the Nuclear Regulatory Commission as they can be used for uranium enrichment. Operation at those frequencies occurs for a period of time, Stuxnet then hijacks the PLC code and begins modifying the behavior of the frequency converter drives. In addition to other parameters, over a period of months, Stuxnet changes the output frequency for short periods of time to 1410Hz and then to 2Hz and then to 1064Hz. Modification of the output frequency essentially sabotages the automation system from operating properly. (Chien, 2010)

The resetting of the centrifuges' speed resulted in a 20% breakdown of the centrifuges and was a serious impediment to the Iranian nuclear enrichment program, setting the production back with one to two years according to some estimates(Chien, 2010).

The clandestine operation of the computer virus left Iran humiliated and the country did not divulge any information about the attack. Although there are no sources to who the attackers were, widespread speculation among web security sites and newspaper articles point to either Israel, the United States or a cooperation of the two states as the makers of Stuxnet. They stood to gain from the disruption of the Iranian nuclear program. The fact that no proof of origin has been brought to market since 2011, bears witness to the difficulty of attribution.

The Stuxnet attack is significant in that it exemplifies how a target of vital national interest can be sabotaged without an escalation to war. Attribution of a cyber-attack can be extremely difficult and Iran did not respond to the attack.

3.2. Operation Orchard – a coordinated attack

On September 6th. 2007, Israel launched an air strike on a suspected Syrian nuclear facility in Dayr- ez-Zor in. In combination with this air strike, Israel probably launched a cyber-attack on the Syrian radar warning systems while the physical attack was carried out. The assumption is that Unit 8200[5] of the Israeli Defense Force (IDF) used a “kill-switch” embedded in the air-defense system by a subcontractor to render it useless(Rid, 2013, pp. 41,42).

In this attack, the goal of using cyber weapons was not to shut down the radar system. This would have raised suspicion among the Syrian forces. Instead, the cyber weapon was meant to make the radar system behave as normal, while at the same time cloaking the Israeli airplanes during their bomb run. The act of blinding the Syrian air controllers by exploiting weaknesses in the attacked radar system rendered the defensive measures of the Syrian forces useless.

This attack is not well documented. Primary sources for the attack are classified. Besides it being mentioned by Thomas Rid, there are some apocryphal texts concerning the operation, but none that discuss the use cyber weapons. In spite of this, the attack is significant in three ways. First, that it is one of a very few incidents where cyber weapons have been used in a military action. Secondly, it demonstrates how a cyber weapon can gain an advantage against an enemy, when used in conjunction with a physical attack.

Thirdly, this attack along with the Stuxnet attack shows how cyber operations in general are kept secret both by the attacker and by the victim.

This cyberattack was an act of sabotage. In general, sabotage is extremely hard to counter, both because the preparations can be concealed, materiel and men necessary for the action are limited in number and because the carrying out of the infiltration, sabotage and exfiltration often can be carried out without detection.

Sabotage carried out by cyberattacks are far less risky for the attacker than through physical attacks. Operatives need not approach the target, keeping them out of harm’s reach. This increases the opportunities for deniability. For the defender, a sabotage attack through

[5] Unit 8200 is an Israeli Intelligence Corps unit.

cyberspace will pose the same problems as do all sabotage actions; they will be prepared, tailored for the specific target and launched in stealth.

It stands to reason that cyberattacks are likely to be used as instruments in international conflicts, but when they will be employed and how or if they will be answered will be determined by the gravity of their effects.

3.3. Trump vs. Clinton – social media subversion

In the U.S. presidential election of 2016, an influence campaign originating from Russia introduced a new form of cyberattack. The attack was intended to reduce Hillary Clinton's chances of winning. In so doing, the campaign supported Donald Trump (Intelligence Community Assessment, 2017). Although the outcome of the election cannot be proved a direct effect of the Russian campaign, it was seen as a threat to the U.S. national security.

The influence campaign was multifaceted and used both open messaging through Russian media and third parties, stealing information from the Democratic Party and uploading it to WikiLeaks, but more spectacularly the use of social media.

On the 16th of February 2018, the United States Department of Justice indicted eleven members of the Internet Research Agency (IRA), a Russian "troll factory" headquartered in St. Petersburg. In the indictment, the IRA was accused for engaging in operations to interfere with the presidential elections and political processes of the United States(U.S. Department of Justice, 2018).

These activities were carried out from as early as 2014 both by stealing and compromising information from the Democrats in order to discredit them, bought political advertisements, but more significantly by subversive actions through the use of social media.

Here, the hackers joined or started groups on social media sites, particularly on Facebook, Twitter and Instagram, where they created hundreds of accounts through which they sought to influence the public opinion by supporting radical groups.

This way, some of the groups controlled by the IRA had hundreds of thousands of online followers by 2016. Although the operations were mostly carried out from Russia, Virtual Private Networks (VPNs) were set up on servers inside the USA. This allowed the IRA to mask the origin of its operation. In order to spread enmity among the American electorate, the operation targeted both left- and right- leaning ideologies. This even included the staging of political rallies (Boyd et al., 2018).

Following the attack, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) divulged their view of the attack in a joint report:

> We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump.
>
> "Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations (Intelligence Community Assessment, 2017).

In the report, the CIA, FBI and NSA expect that *"Moscow will apply lessons learned from its campaign aimed at the US presidential election to future influence efforts in the United States and worldwide, including against US allies and their election processes"(Ibid.2017).*

They also believed that Russia would *"continue to consider using cyber-enabled disclosure operations because of their belief that these can accomplish Russian goals relatively easily without significant damage to Russian interests"(Ibid 2017).*

3.4. Hydro - Crippling the private sector

At 8:31 on the 19th of March 2019, Norsk Hydro sent out the following news flash:

> Hydro became victim of an extensive cyber-attack in the early hours of Tuesday, March 19, impacting operations in several of the company's business areas. IT-systems in most business areas are impacted and Hydro is switching to manual operations as far as possible. Hydro is working to contain and neutralize the attack, but does not yet know the full extent of the situation (Hydro, 2019a).

Hydro had been attacked by a computer virus called LockerGoga. It is part of a strain of virus called ransomware. Ransomware typically encrypts the contents of a computer or server, offering to decrypt it if a ransom is paid. LockerGoga was first reported on January 25th., 2019 when it attacked the French engineering company Altran Technologies.

In Hydro's case, the attack spread across all of the company's business areas and forced an isolation of all plants, switching to manual operation and procedures at the production facilities. The clean-up of the incident was both complex and large. All PCs and servers companywide had to reviewed, cleaned for any malware and restored.

Good backup procedures form the key defense against ransomware once a system has been attacked, but whereas an attack can be a nuisance for a private person, it can be disruptive for large firms. The attack vector can be through portable media storage, E-mail attachment or through a supply-chain attack[6]

In a press release dated March 26th, Hydro estimated that in the first week following the attack, financial losses mounted to between 300 and 350 million NOK. As of April 5th , 2019, Hydro reported in a press release that production was back to normal, but there were still delays in invoicing, billing and reporting (Hydro, 2019b).

There are no indications that the attack on Hydro was state-sponsored or done with any other than pecuniary motives. This illustrates the difficulty of attributing cyber attacks

The Lockergoga – attack was technologically advanced, easy to implement and extremely rapid, taking down the whole centralised command and control structure of Norsk Hydro within a very short time. The attack shows both how fast a cyber-attack is, the level of damage it is capable of causing and the cost and work necessary to bring the situation back to normal.

Whatever the motive or provenance of this particular attack, it still serves as a good example of how vital, national interests can be threatened or destabilized by targeting and attacking the private sector.

[6] An attack on a company computer system through its suppliers' or partners' access to the same system.

4.Deterrence theory and cyberspace

Finding causes to events and predicting effects is difficult in a world full of chance and variation. To do so, theories highlight certain events while others are given less relevance. A simplification of the world, a theory will generalize in order to explain a subject.

In order to discuss deterrence and its application in cyberspace, it is first necessary to understand how the theory of deterrence has developed. Next, deterrence by punishment and deterrence by denial are presented before the application of these theories in cyberspace is discussed.

4.1. The origins of deterrence theory

Deterrence is a strategy intended to discourage an opponent from hostile action. It has been an integral part of security policy ever since the dawn of human conflict, but it was the advent of the Cold War that made deterrence into the main strategic goal. The development of nuclear weapons caused a "true revolution" in strategy and made deterrence by punishment more important that deterrence by denial (Jervis, Lebow, & Stein, 1985, p. 2).

André Beaufre has given a good explanation of the deterrence strategy with and without nuclear weapons. According to him, the nuclear strategy, due to the lack of an effective defence against destruction, rests upon a negative capability, which is to "avoid the great trial of strength, in other words deterrence" (Beaufre, 1965, pp. 23-33).

The prenuclear strategy, according to Beaufre, rested on a positive capability to win large gains with small losses. The logical defense to this would be to ensure that the cost of the attack far outweighed the benefits. The effect of this strategy was a continual arms race. Kaufmann points this out as the main reason why the United States opted for massive retaliation to supplant the matching of the enemy gun- by- gun, tank- by- tank:

"the recently terminated Korean war, fought to a stalemate at a tremendous sacrifice in American lives and treasure"…"jeopardized the prospects for a balanced budget" "Its embarrassments and risks certainly invited the institution of a policy that would achieve the same deterrent effects without the accompanying economic and political strains."(Kaufmann, 1954)

Introduced by the Eisenhower administration, massive retaliation with nuclear weapons became the answer to both conventional and nuclear attacks.

Nuclear weapons did not deter lower level aggression. To remedy this, a new policy was introduced by the Kennedy administration in 1961. Dubbed “Flexible Response (House, 1961, pp. 6,7)”, it reflected the incapacity of nuclear weapons to deter low-level aggression. Constituting a break with the “New Look”- policy of the Eisenhower administration, the new strategy allowed for a stepped escalation of intensity through the use of conventional offensive and defensive capabilities, rather than a leap directly to massive retaliation.

Eventually, the nuclear arsenal of the superpowers grew into a state that created a stalemate of mutual assured destruction (MAD). The risks involved with a nuclear holocaust made statesmen embrace deterrence, as it seemed to be a viable solution for balancing the precarious situation of two superpowers armed to the teeth. The deterrence of nuclear weapons was maintained through various strategies, ranging from military parades, deployment, multiple re-entry vehicles (MIRVs) hardened launch sites and nuclear tests. It was the ultimate deterrent of the nuclear weapons that spurred the academic study of deterrence.

4.2. Deterrence by punishment

Patrick Morgan describes the essence of deterrence as *“manipulating someone’s behavior by threatening him with harm”(Morgan, 1983, pp. 11-17).* Morgan further argues that the success or failure of deterrence takes place in the mind of a potential attacker. He acknowledges that the cost/benefit calculation is important, but he also underlines that the effectiveness of deterrence is dependent upon the fear that it induces.(Morgan, 1983, p. 23)

On a national scale it is the state that is responsible for deterring enemies, safeguarding *“its military security, the integrity of its political life, and the well-being of its people.”(Kennan, 1985, p. 218)*

In an international context, *“Deterrence theory began and prospered not out of the analysis of particular cases but as an abstract analysis of the behaviour to be expected when two sides are able to threaten each other*”(Jervis et al., 1985, p. 1).

Mearsheimer identifies the objective of deterrence as developing in the mind of the adversary a fear of the consequences of his actions or a *“function of costs and risks” (Mearsheimer, 1985).* This is echoed by Brantly who states that *“the most common form of deterrence known* *as conventional deterrence … focuses on the ex-ante dissuasion of adversaries through the threat of expost costs in response to potential adversary actions (Brantly, 2018, p. 32).*

Whether the scale is on an individual or a national scale, deterrence is linked to the perception of risk and punishment. To be effective, deterrence must be credible and clearly understood by the recipient that is to be deterred.

Williams and Hawkins develop this further, saying that deterrence «… implies a psychological process whereby individuals are deterred from committing criminal acts only if they perceive legal sanctions as certain, swift and/or severe."(Williams & Hawkins, 1986)

The classic formulation as a strategy for conflict management was given by William Kaufmann in his memorandum "Requirements of Deterrence"

> Essentially, deterrence means preventing certain types of contingencies from arising. To achieve this objective it becomes necessary to communicate in some way to a prospective antagonist what is likely to happen to him should he create the situation in question. The expectation is that, confronted with this prospect, he will be deterred from taking the action that is regarded as inimical--at least so long as other less intolerable alternatives are open to him (Kaufmann, 1954).

Kaufmann further stresses that the credibility of a state's commitment is vital. The three necessary criteria for achieving this are capability, cost and intention.

Capability is defined as the defender's ability to inflict harm upon the aggressor. *"The enemy must be persuaded not only that the instrument exists but also that its power is operational.(Kaufmann, 1954)"*

Costs are defined as the cost that the aggressor will risk from launching an attack. These must be *«greater than the advantages to be won from attaining the objective (Kaufmann, 1954).*"

Intention is defined as the policy of the defender and it will be interpreted by the aggressor based on three main factors, popular support, previous behaviour and public statements.

Lebow iterates on Kaufmann's point of popular support, pointing out that domestic problems can *"be so severe as to arouse concern for the frangibility of the state itself"* (Lebow, 1985b, p. 182).

Lebow follows Kaufmann in his main findings and has set forth four conditions for deterrence.

- *Credibility.*
  In order for deterrence to work, the aggressor must be assured of the defender's commitment to defend his interests with force. The aggressor must also be convinced of the defender's ability to fight.
- *Communication.*
  The capability and resolve to fight must be announced both in words as well as in action. This puts a toll on the communication process of the defender, but the reception of the aggressor is no less important. The aggressor will interpret the signals he gets but will not necessarily grasp the meaning of what he receives in the same way as it was intended to be understood.
- *Repeatedly publicised.*
  This must be done in order to keep the defender's policy in the mind of the aggressor, the defender and the public.
- *Clearly defined.*
  The nature of the punishment must be clearly understood by the aggressor. In theory, a rational aggressor will weigh the costs and benefits and will, if the costs are sufficiently higher than the benefits, be deterred (Lebow, 1985a, pp. 204-211).

Another vital point where Lebow, Morgan and Kaufmann are in accord is the importance of the intention, resolve and defiance of the defender and that they must be outspoken, In addition, the aggressor must be convinced that action will follow words.

In spite of this, Lebow maintains that deterrence theory is of little help to predict state behaviour or as a strategy of conflict management. He maintains that deterrence may even provoke the very behaviour it seeks to prevent. In his words, the most fundamental characteristic of deterrence theory is that it is *"a system of abstract logic all of whose postulates have been derived deductively" (Lebow, 1985a, pp. 206-211).*

4.3. Deterrence by denial

Denial is a deterrent measure intended to reduce an adversary's ability to intrude or interfere. It " *deters an attack by convincing an attacker there will be no gains commensurate with the cost of attack*" *(Philbin, 2013).* As is evident from the discussion above, during the cold war, deterrence by punishment left deterrence by denial in the shadows.

The ultimate deterrent of nuclear weapons affected the academic discussion, and the focus was on punishment. Even though denial strategies were carried out or proposed, such as the Strategic Defense Initiative (SDI)[7], hardened missile silos and bomb shelters, denial was seen as too costly or insufficient against nuclear attacks.

4.4. Deterring cyberattacks

Today, the legacy of nuclear weapons as the ultimate deterrent to prevent full-scale war is still with us. The same is the case with conventional forces. They are still kept to deter and contain smaller conflicts. The introduction of cyberspace has created new tools for war and a new arena for international conflict. The fact that private persons have acquired the necessary skills and resources to perform serious attacks in cyberspace clearly shows how inexpensive cyber weapons are in comparison to physical weapon systems.

The relatively low cost of entry into cyberspace is highlighted as an important reason to why cyberspace has turned into a field of conflict. (Sheldon, 2012) If, by using cyber weapons, a state could attain its objectives at a fraction of the cost of a kinetic attack, the cost/benefit ratio would indicate the facility by which a state would turn to using cyber weapons.

Do cyberattacks necessitate other responses than those that have proved to be sufficient in the past? Tolga claims that:

> Deterrence theory in cyberspace differs from the classic nuclear deterrence and conventional deterrence in the aspects of actors and means. Cyber deterrence, at its very core, is a result of states' desire to avoid being attacked in or via cyberspace. Potential targets include their military networks, the networks of state or private firms or any element of the state critical infrastructure (industrial systems, finance, publicity, communication lines, power grid and transportation)(Tolga, 2018, p. 7).

Does the new attack vector through cyberspace supersede traditional deterrent instruments of coercion?

Nye does not seem to be of this opinion. He argues that *"even when punishment is used, deterrent threats need not be limited to cyber responses, and they may address general behavior as well as specific acts"*(Nye Jr, 2017, p. 45).

If the argument of Thomas Rid holds, there will be no cyberwar. Rid links this to Clausewitz' postulate that "war is an act of force to compel the enemy to do our will"

[7] The Strategic Defense Initiative or "Star Wars" was a missile defense program proposed by the Reagan Administration to protect the United States against incoming ballistic nuclear missiles by space- and ground based missile-, particle beam- and laser weapons systems.

If, Rid says, an act is *“not potentially violent, it’s not an act of war and it’s not an armed attack”(Rid, 2013, p. 1).*

He links this to the non- violent nature of cyberattacks. In general, Rid says, cyberattacks are either not lethal, or the lethality is caused not by the cyber weapon, but by some malfunction of the attacked system itself.

Following Rid’s argument, it is difficult to see how non-violent trespasses in cyberspace can escalate to physical war. This may reduce the deterrent value of physical instruments in dealing with cyber-attacks.

4.5. The security dilemma in cyberspace

The security dilemma is a theory of offense and defense. Its argument states that conflict and war is more likely to occur when the offence has the supremacy over defense.

The theory puts technology as the primary cause to the prevailing supremacy of either the defense or the offense at a given time. In cyberspace, the prevalent perception is that the offense has the supremacy at the moment. Jervis puts up the cost of defense versus the cost of defense as one criteria to whether states will seek to create offensive or defensive weapons. If the cost of attack is less or equal to the cost of defense, then offensive weapons will be created.(Art & Jervis, 2009, p. 91)

A multitude of programs, systems, devices and users in cyberspace create innumerable opportunities for attacks[8]. At the same time, the cost of cyber weapons is negligible on a national scale. Even though an attack in cyberspace may cost an attacker millions, it will still be dwarfed by the cost of development, maintenance, training, readiness and deployment of any physical weapons system. Tolga points out that: *“there is less will to deter actions in cyber space, causing weakened deterrence. This allows actors to behave more boldly in cyberspace both in peace or war”(Tolga, 2018, p. 7).*

This may result from the fact that so far, attacks in cyberspace have not caused a level of damage severe enough to seriously threaten a state.

Defending against cyber-attacks not only demands constant vigilance, but continual development of security software and practices. This is very expensive and as these measures are reactive, they leave the initiative in the hands of the attacker.

[8] Components and code are made by different companies. Each product will have its own specific vulnerabilities, which can be exploited.

Sheldon links the supremacy of the offensive both to the severity of an attack and to the problem of attribution. (Sheldon, 2012)

4.6. Attribution

Attribution is no easy task in cyberspace. By the use of proxies or other unobtrusive methods, malware can be introduced in ways that do not arouse suspicion or reveal its origin.

Destruction of evidence is another way to hide the identity of an attacker. The Stuxnet worm was programmed to erase itself, whereas the personnel of the Internet Research Agency *"deleted and destroyed data, including emails, social media accounts, and other evidence of their activities" (Justice, 2018)*. In spite of this, these efforts will not assure the attackers anonymity. F- secure[9] is sanguine in their view on attribution. In their view, investigators will correlate information from metadata such as:

> IP addresses used in attacks, the language and email addresses used in phishing campaigns and other correspondence, social engineering tactics, TTPs used for persistence and lateral movement, or even time correlations between outbound connections from an ISP and subsequent outgoing connections from a VPN exit node are used to paint this picture. As careful as attackers might be, it's going to be almost impossible to prevent authorities from putting the puzzle together (F-Secure, 2017).

This is in part connected to the way tracks can be obscured

Investigation of who is behind an attack is not impossible, but it is rendered difficult by the way the origin of an attack can be obscured by attacking through proxies, such as supply chain attacks, or by manipulation of the signs that investigators use to identify the This may throw the investigators off the scent or convince them that the blame lies elsewhere. Attribution is insecure, as illustrated in appendix B where attribution is stated in the following manner: *"NCSC assess with high confidence that the GRU was almost certainly responsible."* For deterrence, it is not only the identity of the attacker that is important. It is also about getting the information in time. Attribution is time-consuming, reducing the window of opportunity for retaliation.

[9] F-Secure is a Finnish antivirus and cyber security company

4.7. Severity

So far, there have been no instances where an attack in cyberspace has induced a breakout of war between two states. The explanation may be that states have not gone to war, - yet-.

Early cyberattacks were mainly used as an arena for hackers to show their skills and both the malware and types of attacks were mostly unsophisticated.

> Stuxnet was different from all of these. It wasn't an evolution in malware, but a revolution. The idea that someone would create such a sophisticated worm to slither blindly through networks in search of a single target was "leaps and bounds" beyond what the Symantec researchers had expected (Zetter, 2011).

Since then, there has been a development of state- sponsored attacks in cyberspace.

> APTs[10] are long-term, covert malware campaigns run by well-funded teams who are typically backed by the resources of a nation state. The playbook for such attacks is to stay "low and slow" in an organization's infrastructure over a long period of time, allowing the attackers to gather detailed information on the target enterprise. The usual goal of these malware campaigns is ongoing theft of highly confidential data or even disruption of operations. (Ibid. 2011)

The APTs are far more sinister than private hackers. With the funding and resources of a state, they are able to inflict far more damage. The cases of Stuxnet, the Russian campaign against the U.S. presidential election and the Titan Rain attacks[11] testify to this.

There may be several reasons why states have chosen not to go to war after having suffered an attack in cyberspace. If the severity of an attack is low, the defender may choose not to escalate the conflict. This may be the result of several factors.

One factor may be that the effects of the attack are not perceived by the victim state to be severe enough to justify an armed attack. Another factor may be that the cyber weapons have been constructed (tailored) in such a way that the effects of the attack will not invoke an armed response. A third reason may be that an acknowledgement of a cyber-attack would make the struck state lose face. This could compel it to deny that the attack had taken place.

[10] Advanced Persistent Threats

[11] Titan Rain was a series of coordinated attacks on government and private companies. Significant targets were: Lockheed Martin, Sandia National laboratories (involved in national security, nuclear weapons design, defense systems and energy) and Redstone Arsenal (home to NASA Marshall Space Flight Center, U.S. Army Combat Capabilities Development Command Aviation & Missile Center, Missile Defense Agency, DIA / Missile and Space Intelligence Center, U.S. Army Aviation and Missile Command, Program Executive Office Aviation and the U.S. Army Materiel Command.(Hamnes, 2012)

5.How to deter cyber-attacks?

This chapter will first show how cyber-attacks are deterred today through denial, showing how this is organized and the challenges to this approach. Next, deterrence by punishment is presented with an appreciation of the restraints posed by International Law and what results this strategy can incur.

Cyberspace is for all purposes an unrestricted, anarchic area, where national borders are fuzzy and prosecution is restricted to national legislation. In the absence of international laws, it may be that it is rather the fear of retaliation that makes countries refrain from launching attacks in cyberspace. As proven by their track record, revisionist and authoritarian states like Russia, Iran, China and North Korea, there has been little to threaten or dissuade their subversive attacks and espionage.

Although international law eventually could play a more important role in the ordering of cyberspace, this is not yet the case, as NATO testifies in that it:

> will exercise restraint and act in accordance with international law. The Alliance also welcomed efforts undertaken in other international fora to develop norms of responsible state behaviour and confidence-building measures to foster a more transparent and stable cyberspace for the international community"(NATO, 2018)

What course to take in order to deter hostile attacks in cyberspace is not easy. There are proponents for several ways of response. All carry their own specific strengths and weaknesses. Deterrence can be achieved through a combination of defensive and offensive measures. The U.S Department of Defense explains this in its "Cyber Strategy" where in order to deter cyber-attacks it and seek*:*

> "to use all instruments of national power to deter adversaries from conducting malicious cyberspace activity that would threaten U.S. national interests, our allies, or our partners. The Department will prioritize securing sensitive DoD information and deterring malicious cyber activities that constitute a use of force against the United States, our allies, or our partners. Should deterrence fail, the Joint Force stands ready to employ the full range of military capabilities in response (U.S. Department of Defense2018, p. 1).

Further, the U.S. DoD will: *"counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions"(Ibid. 2018, p. 4).*

Cyber weapons differ from nuclear weapons in that they cannot function as a deterrent by their existence alone. Whereas the effectiveness of a nuclear weapon is not diminished, even though its potential is known, a cyber weapon's effectiveness seizes once its potential is revealed. This lies in the fact that it is a logical weapon. Once it is used, its mode of operation will be revealed, and it will no longer have any value. The enemy will recognise it if it is launched a second time and be able to protect himself.

An attack in the real world is expensive to launch both in preparation and in execution. Weapon systems, training, readiness, logistics, maintenance and manoeuvre are costly, difficult to conceal from the enemy and if the enemy is forewarned and given the opportunity to prepare countermeasures, catastrophic losses can ensue.

In themselves, these are important barriers for launching an attack in the physical world. The cost of deterrence in the physical world is equally expensive, but the credibility of a carrier group or a nuclear submarine is undisputable. Their range and latent capacity of destructive power are tangible threats and gives an attacker a clear indication of what could be the response to aggressive action.

Another obstacle for deterrence in cyberspace is the non-lethal character of cyberattacks.

The U.S. National Cyber Strategy argues:

> that an offense-defense strategic framework must be adopted, once again, in order to think about and organize against threats in cyberspace…cyberspace is an environment of offense dominance in which deterrence is easily overwhelmed…Implementing a dedicated deterrence strategy against cyber aggression entails establishing a credible commitment to respond to attacks. The credibility of deterrence depends on the capability to detect attack, determine its source, and inflict appropriate cost in response. Importantly, the political will to carry out the promised retaliation must be signalled clearly in advance of any aggression. Cyberspace raises significant challenges on all of these necessary components for successful deterrence (The White House, 2018, p. 10).

5.1. Deterrence by denial

Denial is a deterrent measure intended to reduce an adversary's ability to intrude or interfere.

It "*deters an attack by convincing an attacker there will be no gains commensurate with the cost of attack*" (Philbin, 2013).

In cyberspace, denial is done through several defensive measures. Vulnerabilities in a system are reduced through good routines and keeping software up-to-date. Control of entry points is carried out through control of passwords and credentials, Systems are layered and access to higher levels is restricted. Security software scans for malignant software to stop intrusion through mail and portable memory storage.

There are several reasons why denial strategies are not at the centre of the deterrence. The first is that denial will not inflict any pain on the aggressor. As discussed earlier, this is not easily achieved through denial alone.

Philbin's argument highlights three of the main problems with halting hostile intrusion in cyberspace. The first is connected with the security problem. Presently, as previously discussed under 4.5, the offense has the superiority over defense (ibid.2013).

The second is that an attack in cyberspace is cost beneficial when compared to a physical attack (ibid.2013). This is a result of the relative cost and effect of a cyber weapon as compared to a physical weapons system.

The third is that in cyberspace, defensive measures can be probed continuously with impunity (ibid.2013). Denial will not inflict any pain on the aggressor.

Given that the offensive has the upper hand in cyberspace, defending against attacks in cyberspace is no simple matter.

5.1.1. National policy: Organization, actors and responsibility in cyberdefense

Following the increased vulnerability of modern society, vital sectors have through their connected command and control systems, become attainable targets. As a consequence, it has become necessary to adopt new defensive measures to safeguard them. This is done partly through technical solutions like firewalls, authentication, passwords, virus scans and encryption to reduce opportunities for ingress. Backup routines and computer emergency readiness teams (CERT) are employed to reduce serious damage caused by security breaches, and surveillance and cross- sectorial cooperation increase the awareness of threats. Social media are for the most part controlled by multinational companies and have until today only to a minimal degree been subjected to national control in respect of their content. This is probably a result of a lack of need until the Russian attack on the U.S.A during the presidential election of 2016.

As the United States is the target of most cyberattacks worldwide, it may be used as an example of how cyberdefense can be organized, although this may be done differently in other countries.

In the USA, it is the Department of Homeland Security and its subsidiary, the US National Cybersecurity and Communications Integration Center (NCCIC) that is tasked with reducing the risk of systemic cybersecurity and communications challenges across public and private sector networks. Other aspects of the country's cybersecurity such as intelligence and investigation are delegated to the CIA, NSA and FBI. It is worth noting that these agencies reach out to the private sector for information exchange and that the agencies are interlinked through many joint task forces and committees.

The US National Cybersecurity and Communications Integration Center (NCCIC) serves as the national hub for cyber and communications information, technical expertise, and operational integration, and operates a round-the-clock situational awareness, analysis, and incident response center Its stakeholders are the federal government, the private sector and some international partners. In addition, come the states, local, tribal, and territorial (SLTT) governments. Through the Einstein program, the NCCIC, collects, correlates, analyzes, and shares security information to protect the federal computer networks. The NCCIC is not responsible for the cybersecurity of the private sector, but supports it through information exchange, education and training, incident response capabilities and malware analysis. In addition, cybersecurity assessments are offered, such as vulnerability-, Red Team-, and Phishing campaign assessments. Through the Industrial Control Systems Joint Working Group (ICSJWG), the NCCIC collaborates with the private sector in order to reduce risk to the nation's industrial control systems. This is done across all critical infrastructure sectors.(US Department of Homeland security)

Intelligence gathering is a necessary part of defense. It provides information about hostile actors. In the United States, this task is carried out by the CIA and NSA.
The CIA's primary mission *is "to collect, analyze, evaluate, and disseminate foreign intelligence to assist the President and senior US government policymakers in making decisions relating to national security"(CIA, 2018).* To support this mission, the newly formed Directorate of Digital Innovation supplies *"cutting-edge digital and cyber tradecraft and IT infrastructure(Ibid.2017).* The CIA is naturally reticent about what it does, since divulging information will inform both the public and the country's adversaries.(Fox-Brewster, 2017)

The NSA's main role in cybersecurity is to help protect and defend national security systems. This is done by carrying out foreign intelligence, surveilling the development and operation of hostile foreign powers' cyberspace capabilities. This information is used to develop solutions to counter threats, implement strategic defensive measures and to publish guidance to cybersecurity professionals.(NSA, 2019)

Investigation and prosecution is an equally important element in reducing the threat in cyberspace. The FBI is the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists. This is done through a cyber division with specially trained cybersquads at the headquarter and at the FBI's field offices. The goal is to finding the hackers' identity and bring them to justice. The FBI is also the lead federal agency responsible for investigating foreign influence operations. In 2017, the Foreign Influence Task Force (FITF) was established to identify and counteract malign foreign influence operations targeting the United States. Through the FITF, the FBI approaches this threat by:

- Investigations and operations:
  The FITF works with FBI field offices across the country to counter the extensive influence operations of our foreign adversaries.

- Information and intelligence sharing:
  The FBI works closely with other intelligence community agencies, as well as with state and local law enforcement partners and election officials, to ensure a common understanding of the threat and a unified strategy to address it.

- Private sector partnerships:
  The FBI considers strategic engagement with U.S. technology companies, including threat indicator sharing, to be important in combating foreign influence actors.(FBI, 2019).

5.1.2. The private sector

Private companies represent one of the vectors of attack that can be and have been used to destabilize [12]a state (Fox-Brewster, 2017). The trouble of protecting these companies against hostile attacks is that the prime motive of private companies is to earn money and that they concentrate on that mission. General economic theory postulates that in order to maximise profits, all unnecessary activities will be reduced to a minimum, streamlining the organization

[12] Privately held companies of different sectors (e.g. military industry, finance, energy, production etc.) can be targeted in order to steal information vital to national security, sabotaged to reduce

for operation in a normal situation, where the risk is known. This is also the case for IT security. Although a private company may be resilient and withstand cyber-attacks, they will not, unless the company is an IT security firm, have the necessary resources or expertise to withstand determined attacks from state-sponsored hackers.

Today, these companies are for the most part left to fend for themselves. As shown above in the case of the NCCIC, they do receive some assistance from their governments either as warnings of cyber activity or as some help in forensics and in the rebuilding of their infrastructure once, they have been attacked. In their daily run however, they are on their own. Given the supremacy of the offensive within cyberspace, private companies will never be able to spend enough money to defend themselves against attacks from advanced state-sponsored hacking.

In a perspective of defense, it would make sense that companies that constitute vital, national interest should be shielded by their state, since only a state has the sufficient resources to shoulder this responsibility. This is evident in the U.S. National Cyber strategy, signed in September 2018, where the United States pledged that it would:

> use all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation «and "prevent the use of digital platforms for malign foreign influence operations while respecting civil rights and liberties(House, 2018).

This may also point towards an evolution to a higher degree of integration and cooperation in and between the sectors. Unfortunately, the development of multinational companies and cloud computing, where vital information is stored or control systems operate outside a state's jurisdiction complicate such efforts.

5.1.3. The media

The media sector is a special case. Here, it is not only the danger of sabotage that threaten the sector, but subversion. A community without internal cohesion can easily fall prey to external pressures.

How can freedom of speech be safeguarded when stopping hostile information campaigns demands censorship? Subversive attacks may destabilize a state by eroding the cohesion of its society. How can "fake news", conspiracy theories and destabilization attempts be stopped when it is spread by a legal news company like Russia Today (RT)(Torvik, 2019) or such information is legally uploaded to social media, outside the jurisdiction of the victim state?

Lack of internal cohesion, like the way that President Trump has downplayed the Russian subversive actions in the Presidential election in 2016, can be seen as an opportunity for further involvement by the Russian trolling campaign.

This was expressed by the CIA, FBI and NSA, who *"assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes"(Assessment, 2017).*

5.1.4. Legal sanctions and prosecution

Taking legal sanctions against state-backed hackers is difficult. The first obstacle is attribution as stated in a declassified report by the CIA, FBI, and National Security Agency:

> The Intelligence Community rarely can publicly reveal the full extent of its knowledge or the precise bases for its assessments, as the release of such information would reveal sensitive sources or methods and imperil the ability to collect critical foreign intelligence in the future (Assessment, 2017).

Jurisdiction is another obstacle. Although the FBI indicted the leaders of the Russian Internet Research Agency in 2018, there can be little hope of bringing any of them to justice. Legal sanctions against foreign nationals living within the nation responsible for the attack can serve no other purpose than showing the public that the attack and how it was accomplished did not go unnoticed. It is unlikely that apart from the humiliation of being called out, legal sanctions against the agents of an attack will not deter that nation from carrying on with its operations.

There is another way to reduce the access and opportunity for foreign subversive interventions through social media platforms. As discussed earlier, private companies' main focus is to make profits. Social media companies have not taken editorial responsibility or willingly introduced checks to malignant content, both because the tradition of the Internet has been free from censorship, but also because this would reduce profits.

When Mark Zuckerberg in March 2019 asked governments around the world to take responsibility for legislation against malware, election security, privacy and data portability, it was to forestall the possibility that Facebook may be held liable for what is posted on its platform.

Presented in a report on disinformation and fake news delivered February 2019 to the House of Commons, this is in fact proposed as a solution to reduce the impact of cyber-attacks by law. Here, national legislation is forwarded as a bulwark against foreign influence campaigns.

The report suggests that the service providers must assume legal liability for the content on their platforms:

- Compulsory Code of Ethics for tech companies overseen by independent regulator
- Regulator given powers to launch legal action against companies breaching code
- Government to reform current electoral communications laws and rules on overseas involvement in UK elections
- Social media companies obliged to take down known sources of harmful content, including proven sources of disinformation(House of Commons, 2019)

It is to be expected that the social media companies will enforce restriction of hostile intervention if they face prosecution and fines for serving as the medium for malign content.

5.1.5. International cooperation

International Law and cooperation have yet to come onto the stage in the fight to control malignant behaviour in cyberspace. In October 2018, the first UN panel discussion was held on whether International Law applies to cyberspace and what other responses states should consider. Although the discussion has started, there is still no general agreement and there is probably a long way to go before it will be legally binding. Liis Vihul of Cyber Law International speculated *“that major cyber powers are unwilling to discuss red lines for offensive cyber activity” (Vihul, UN).* Other international organizations like the EU and NATO have come further and have implemented or prepare action plans to curb attacks in cyberspace.

5.2. Deterrence by punishment

Alcibiades is quoted as having said *“Men do not rest content with parrying a blow of a superior, but often strike the first blow to prevent the attack being made”.(Thucydides, ca. 420 BCE).*

Donald Rumsfeld said of terrorism: *“You can't defend at every place at every time against every technique. You just can't do it, because they just keep changing techniques and time, and you have to go after them. And you have to take it to them, and that means you have to preempt them”(Woodward, 2004, p. 34)*

From the Peloponnesian war to the war on terrorism, deterrence by offensive measures has a long history.

5.2.1. Deterrence by physical force

There is no one way to safeguard against cyber-attacks. Technologically, they will change so rapidly, and the ways of attacking are so manifold, that in spite of constant development of defensive measures and a constant vigil, the walls will not be safe. Could retaliation or pre-emption with physical force function as a way to reduce the flow of serious attacks?

The first question that arises when it comes to retaliation with physical is how it can be done. Retaliation must inflict enough pain on the attacker that he will refrain from committing a hostile action or to stop committing it.

One solution could be to look at the strategy that Israel employs in its dealings with non-state groups. This has been dubbed “mowing the lawn”. It reflects the assumption that Israel is in a continuous conflict and that the sensible way to act is to accept a certain level of risk and launch military actions when the enemy’s capabilities rise above this level. (Inbar & Shamir, 2014)

The “lawn mower” strategy is probably appropriate In Israel’s case, for in this situation the opposing groups are weaker than the state that defends itself. The resources of a non-state group is not comparable to the resources of a state and physical attacks with the resources available to a state will be effective. Nevertheless, they will at best only reduce the severity of the attacks for a limited time.

Another solution could be retaliation with physical attacks that so seriously cripple the attacker that he will not have the ability to attack again.

Neither of these solutions seem to be viable. Coercion or signalling by using offensive physical measures in the fashion of the Israeli strategy cannot make the conflict disappear.

In cases where the attacker is equally capable of threatening the defender with physical weapons, it is difficult to see how retaliation or pre-emption with physical force can be done without risking an escalation to an armed conflict.

5.2.2. Legal aspects

Another important aspect that must be considered is how an armed response to an attack in cyberspace can be done in accordance with Jus ad Bellum and Jus in Bello. Although the international law of armed conflict (LOAC) does not necessarily concern hostile attacks in cyberspace, it is up to the attacked state to define such an attack as a cause for the lawful use of violence. Retaliation to an attack in cyberspace will in the case physical force is used, be bound by the LOAC and must follow the regulations set down for distinction, necessity and proportionality.

The example of the Russian interference in the US presidential election of 2016 exemplifies the problems of an armed response. The interference can be seen as a clear breach of the sovereignty set down in the Westphalian Treaty, where each state was free as Henry Kissinger described it "*to choose its own domestic structure and religious orientation free from intervention" (Kissinger, 2015).*

Article 2 In the U.N. Charter further states that:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations (United Nations, 1945).

In both instances, the interference in a state's internal affairs by another state is seen as unlawful. Article 51 in the U.N. charter leaves every state the right to defend itself if it suffers an armed attack. Would it be possible to interpret this interference in cyberspace as an attack that could lawfully be answered by a physical attack? In such cases, the criteria of distinction, necessity and proportionality must be met.

Distinction is connected to what can be considered as lawful targets in war. Physical weapons can function well as agents of deterrence. They may be used to retaliate and inflict swift, certain and severe punishment to the attacker. Nevertheless, offensive retaliatory measures in the physical world incur a high probability of collateral damage. Retaliation by a physical attack would have to adhere to Jus in Bello, where the St. Petersburg declaration gives the principle of distinction: *"the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy."* This means that civilian targets are unlawful according to the LOAC.

The principle of necessity is contained within the LOAC. This is interpreted as:

> *only that degree and kind of force, not otherwise prohibited by the law of armed conflict, that is required in order to achieve the legitimate purpose of the conflict, namely the complete or partial submission of the enemy at the earliest possible moment with the minimum expenditure of life and resources(Ministy of Defence, 2004).*

Although violent action can be seen as an appropriate response, the principle sets up the limits to what kind of weapons, targets and actions that are permissible in conflicts. An armed response to a cyber-attack will be held to this account, even though the cyber-attack is not.

Proportionality is the third criterion that must be considered in connection with armed attacks. Retaliating to a cyberattack with a conventional or a nuclear attack raises the question of how this can be seen as a proportionate use of force. Sheldon argues that cyber power is not coercive, and although cyber weapons may be used in sync with physical attacks, they generally exploit deficiencies in the defender's own systems(Sheldon, 2012).

Thomas Rid is in agreement with Sheldon as to the non-violence of cyber weapons, stating: "*most cyber-attacks are not violent and cannot sensibly be understood as a form of violent action. And those cyber attacks that actually do have the potential of force, actual or realized, are bound to be violent only indirectly"* (Rid, 2013, p. 12).

It is particularly proportionality as set forth in the LOAC that sets up important barriers for a defender. The LOAC primarily acknowledges violence as a legitimate casus belli, and this may make it difficult to legitimize the use of violence as a reply in kind to cyberattacks, given their non-violent nature. Since the origin of a cyber-attack often is obscure, there is a problem of legally attributing the blame and retaliating with physical force. The severity of a cyberattack reduces the lawful grounds for an armed response. The attacker may also use this factor to reduce the severity of an attack, thereby reducing the opportunity for the defender of lawful retaliation with physical weapons.

5.2.3. Deterrence with cyber weapons

Kaufmann makes an important distinction when it comes to the ability to respond to a threat; "*Potential as against actual capability cannot be regarded as a convincing instrument of deterrence*".(Kaufmann, 1954)

Kaufmann's dictum is undisputed in the case of nuclear weapons. This policy is continued by the USA in the introduction of dissuasion. It is intended to persuade:

> the adversary of the futility of competition with the United States, either on a general basis or in a particular category of military power, which could be nuclear weapons or fighter aircraft or attack submarines or anything else. The goal is to lead the adversary to conclude that it would be pointless to compete in the acquisition of military capabilities (Yost, 2003).

To attain credibility in cyberspace, both the speed of responding to an attack and the manner of the response, i.e. the deterrent measures that are used, are vital. What sets cyber weapons in another category from nuclear or conventional weapons is their characteristics. There can be no parades or test firing as with nuclear weapons. Cyber weapons cannot be stockpiled in order to function as a threat to an enemy. Like the hollow, wooden horse at the gates of Troy, cyber weapons are logical weapons. Once they are put to use, they will be depleted, since the defender will be able to study and counter them.

> Langner has called Stuxnet a one-shot weapon. Once it was discovered, the attackers would never be able to use it or a similar ploy again without Iran growing immediately suspicious of malfunctioning equipment (Zetter, 2011).

Using offensive cyber weapons to retaliate will also procure the aggressor with information of the defender's general capabilities in cyberspace. That information will help to refine his next attack or may make him try to attack in another way or to strike at another target. It would also mean that the aggressor's defense will be strengthened, reducing the opportunity for retaliation at a later date. The development of offensive cyber weapons to deter an enemy without using them is unlikely to have any effect. The use of offensive cyber weapons that harm the opponent is likely to turn into an arms race with a high probability of escalation to an armed conflict.

Unless cyber weapons are used, they are not credible and because of the development in cyberspace, they will soon become obsolete. Once a cyber weapon has been used, its usefulness ceases.

One way to retaliate within cyberspace could be to use offensive weapons that are less sophisticated than the defender is capable of producing. This might be done to show the defender's resolve to defend himself, while concealing his true offensive capacity.

Kaufmann argues against such a strategy, pointing to the risks involved in not responding to an attack:

> If we back down and let the challenge go unheeded, we will suffer losses of prestige, we will decrease our capacity for instituting effective deterrence policies in the future, and we will encourage the opponent to take further actions of a detrimental character (Kaufmann, 1954, p. 7).

Lebow argues that offensive action with reduced force may be counterproductive and may indeed solicit the exact action that the deterrent vehicle is intended to forestall. He gives several examples of this, one of which is the Sino-Indian conflict of Ladakh in 1960. Here, the Chinese withdrawal was intended to show resolve and strength, while still allowing the Indians to save face and back down. Instead, this led to heightened tension, since the Indians interpreted the withdrawal as a Chinese fear of defeat and unresolve. (Lebow, 1985a, pp. 207-209)

Offensive actions in cyberspace has its proponents. Late Sen. John McCain advocated an offensive policy in what he called an "information war with Russia" In his book "The restless wave", he suggested that America should consider cyberattacks to retaliate for Russia's meddling in U.S. elections.(Gould, 2018)

It is also significant that when Emanuel Macron, the French President launched the declaration *"Paris Call for Trust and Security in Cyberspace"(l'Elysée, 2018),* the United States declined to sign(Sanger, 2018). This can be interpreted as a sign that the USA does not wish to relinquish its own opportunities to launch cyberattacks.

Although most such attacks would be clandestine, some attacks could be carried out with a high degree of openness in order to expose the vulnerabilities of the aggressor and to display both to the enemy and the public the capability and resolve of the state that is defending itself.

According to anonymous sources in the U.S administration (Hansen, 2019) U.S. cyber command turned off the electricity of the Russian Internet Research Agency during the midterm elections of 2018. This was done in response for the interference in the presidential election in 2016 and to pre-empt intervention during the 2018 elections.

Another factor that favours attacks with cyber weapons is that they can be designed to reduce collateral damage.

The Stuxnet worm shows how cyber weapons may reduce the risk of breaching the regulation on distinction. Even though the worm spread to other systems besides the Iranian nuclear enrichment centrifuges, there were very few systems and machines damaged outside Iran. The worm was constructed in a way to reduce collateral damage both by how it would only deliver its malware program if it found the PLCs to have the specific settings compliant with the high speed of the nuclear centrifuges. If these settings were not found, the program would try to infect other computers. Another failsafe was the self-destruct mechanism built into the worm, causing it to erase itself in 2012.

Ralph Langner said that the Stuxnet "*could be considered a textbook example of a "just war" approach. It didn't kill anyone"(Singer & Friedman, 2014, p. 120).*

5.2.4. Prosecution

In general, all cyber-attacks will be interpreted as crimes when they are investigated and actors will be prosecuted as criminals if they are caught. In general, this has a deterrent effect on individuals, but the characteristics of cyberspace has made it less formidable. A targeted system can be hacked from another country and there are ways to obscure where the attack originated, although this is becoming more difficult. Prosecution is also harder to accomplish if the attacker is based in a country with no extradition agreement with the attacked state. Attempts have been made to combat foreign state intrusion through prosecution. As shown in the example of the Russian intervention in the U.S presidential election of 2016, the FBI indicted the Internet Research Agency and thirteen of its staff.

The possibility that these defendants will ever be present in an American court of law is highly unlikely. The indictment probably served two other purposes. One was to show Moscow that the USA was capable of reconstructing how the IRA had operated, but also that it had the capability of tapping the internal emails between the members of the IRA. Another motive was probably to show the American public the vigilance of the government and that the attacker were held responsible to the rule of law.

Even though prosecution is a punitive measure, it is not an offensive one. Prosecution is reactive in nature, and as an instrument in international relations, it is unlikely to raise the level of conflict. Through the necessary investigation, the attackers and how they operate will be exposed. Prosecution thus serves as a defensive measure against cyber-attacks, through the punishment of individuals, by embarrassing the attacking state by publicity and a legal ground for international sanctions.

5.2.5. International sanctions

Should a cyber-attack be interpreted as a breach of the peace and thereby come under the jurisdiction of the United Nations, the Security Council may take action to restore international peace and security. Article 41 in the Charter includes *“complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.”*

Dependent upon the economic power of the victim state, economic sanctions can be severe for a country, but it will rarely be coercive. Lebow has argued that although the U.S. oil embargo on Japan in 1941 was meant to curb the country’s aggressive politics, and indeed was severe on the country, the embargo instead proved to be a catalyst to the attack on Pearl Harbor. (Lebow, 1985a, pp. 221,222)

In spite of the sanctions, economic and otherwise, that have been put in motion, neither Russia nor China, have refrained from constantly launching cyber-attacks against the U.S. or the West in general, which supports Lebow’s argument. The economic sanctions imposed on Russia from 2014 and onwards may even have increased Russia’s efforts to disrupt the West through subversive activities in several sectors including cyberspace.

6.Conclusion

The goal of this thesis has been to examine how cyberattacks can be deterred. Based on the foregoing research, the conclusion presents its findings on the three research questions. The thesis points to possible solutions to deter hostile actions in cyberspace and suggests further research.

6.1. Cyberattacks and the threat to states

Cyberattacks share some common characteristics. They attack through computer systems on order to deliver their payload. Their speed gives a defender very little time to mitigate damage once a system has been breached. Following the intrusion, a cyber-attack will in general exploit a vulnerability inherent in the targeted system. Following the exploit, the intruder will gain control to steal, sabotage or subvert.

The four examples that were introduced in chapter 3 represent four main vectors where a state can be attacked. Three of these attacks were launched with the intent of damaging a state or reducing its influence, while all four shared the capability to strike a state’s vital national interests. None of the attacks were violent in themselves, but were able to inflict damage by exploiting vulnerabilities in the systems. To what degree do cyberattacks threaten a state?

A cyber weapon can be used in two separate situation. It can be used in an armed conflict, but due to its non- violent character, it will be used in conjunction with physical attacks. This means that only the threat of massive punishment will be able to stop it. In peace, cyber weapons will threaten a state, but only up to the point where the cyber-attack can give the defending state reason to retaliate with physical force.

The statement, that once a cyber weapon has been used, its usefulness ceases, is not only a description of the usefulness of the weapon. It also denotes the process that will be started by the attacked state to reduce the perceived vulnerability and improve its proficiency. As discussed by Barzashka, the Stuxnet attack at the Natanz nuclear facility, may even have improved the Iranian efforts of enriching uranium, as they were able to enrich it to 3,5% before the attack in 2007 and were able to enrich it to 20% in 2010. *“Uranium-enrichment capacity grew during the time that Stuxnet was said to have been destroying Iranian* *centrifuges" (Barzashka, 2013)*. It is evident that repeated attacks will hone the skills, improve the infrastructure and the organization of the defenders.

6.2. Deterrence of cyber-attacks vs deterrence of physical attacks

Is deterrence of cyberattacks different from deterrence of armed attacks?

Cyber-attacks are difficult to fit into the LOAC. As has been shown, both the severity, non-lethality and difficulty of attributing a cyber-attack are problematic. This restricts lawful response, particularly in peacetime. So far, research shows that cyber-attacks do not replace or reduce the need for deterrence against physical attacks. In war, cyber-attacks will be attempted to be deterred by denial and through deterrence with physical punishment as described above. In peacetime, there is no one solution that will deter cyber-attacks. Deterrence of cyber-attacks must be approached through several measures. This is discussed below.

6.3. Relevant vehicles of deterrence; strengths and weaknesses

There is no silver bullet- solution to deterring cyberattacks. As is shown, cyber-attacks will most likely be kept under the threshold that would give a state a reason to retaliate with physical force. There are several important components that can serve as vehicles of deterrence.

Dissuasion through international agreements is an important segment of deterrence, but it only works if the collective punishment from the world community is more important than the security that can be gained from an attack. Although states may choose to adhere to such agreements, there are many examples where signatory states have acted in violation of the LOAC when vital, national interests are at stake. This was the case for the gas attacks in the Syrian civil war and of the Russian annexation of the Crimea. Both attacks were in violation International Humanitarian Law (IHL) and the LOAC. Although international law may fall short in deterring attacks, international agreements on security cooperation and prosecution may greatly reduce the vulnerabilities of cyberspace.

Cyberdefense is a non-aggressive policy and will not deter an aggressor when an attack is perceived as a favourable course of action for the aggressive state. Nonetheless, reducing the damage that an attacker can hope to inflict is part of the solution to combat cyber-attacks. Defense must be built on a resilient infrastructure, good organization, clear procedures that are followed and awareness of risk. Technical solutions are necessarily a vital part of cyberdefense. They encompass processes such as the control of gateways, firewalls, metadata scanning software and password control.

Cyberdefense will provide information of the vector and origin of an attack through the intelligence services, but also through forensic and surveillance activities. Although this may not deter an attacker, if the cost/benefit ratio can be swung sufficiently in favour of the defender, it will reduce his hopes of success.

Active defense has been suggested as a solution where defensive and offensive measures are exploited in an automated fashion. The solution suggests that *"real-time detection, analysis and mitigation of network breaches are combined with the aggressive use of legal countermeasures beyond network and state territorial borders"(Jasper, 2017, pp. 18-20).*

This can be seen as a search for a technical solution to deter cyber-attacks. Automated processes are able to filter out known threats and stop them. This is already a part of cyberdefense.

> In targeted attacks (a superset of attacks that includes APT) adversaries use specifically mutated forms of malware that allow the same basic exploit code to be written and re-written in hundreds or even thousands of ways. Same basic code every time, but these slight mutations are specifically done to evade detection from classic anti-virus solutions. Once mutated sufficiently, the targeted attack can deliver the payload to the target with high confidence that no signature-based means of detection will pick it up (Rowney, 2011).

Automated processes will be able to stop known threats by scanning for their signature. This means that the problem of intrusion and exploitation still remains. As argued by George and Smoke in their discussion on the Berlin crisis, a determined attacker with the resources of a state, will be able to design around a deterrent threat (George & Smoke, 1974). In cyberspace, this can be achieved by creating new malware and circumvent automated processes to steal, destroy or subvert.

Offensive action is another way to deter cyberattacks.

It has been argued that Russia’s activities in cyberspace is a way to counter the West’s superior physical force and influence on the so-called “colour-revolutions”. (Etterretningstjenesten, 2019a) From a defensive realistic viewpoint, Russia can be interpreted as trying “to maintain its position in the system”, (Waltz, 2010) using cyberspace as a field where it is “free to strike at any point along the whole line of defense, and in full force.”(Clausevitz, 1993, p. 431)

This does not imply that it is only the West that is vulnerable in cyberspace. Pigman points this out, stating that *“Russian political elites view cyberspace as the source of significant threats to Russia’s own national security; against regime security, ... public safety, ... societal norms and cohesion”(Pigman, 2019b).* This is significant in that it shows that the Russian regime sees itself as vulnerable to cyber-attacks. Can offensive action following these vectors prove effective?

Political control of the Western populace is lax. The Russian inroad to influencing the West has been through the exploitation of the freedom of speech and social media. Compared to the situation in Russia or China. Subversive attacks on regimes like Russia or China may indeed prove more effective than such attacks are in the West.

Pre-emptive strikes may produce results in the short run, but it is doubtful they will make an enemy change his policy. Following the Bush doctrine, such attempts have been made in the war on terrorism, and still terrorism has not disappeared. The alleged hacking of the electricity of the St. Petersburg Internet Research Agency in 2018 may have been an attempt to pre-empt Russian attempts to interfere with the midterm elections to the U.S. Congress. Anonymous sources in the U.S. administration acknowledged that it was no more than the sting of a fly, but was valuable in proving that the USA could use the same kinds of attacks (Hansen, 2019)

In themselves, offensive measures of retaliation or pre-emption are either likely to prove too weak to deter future attacks, or too strong, risking an escalation to an armed conflict.

As long as the attacks in cyberspace fall short of providing legal grounds for an armed response, deterrence by offensive measures is unlikely to prove effective on its own.

A deterrent vehicle that may prove potent in deterring cyber-attacks is publicity.

> After two U.S. election cycles dominated by talk of the cyber threat from Russia, many Americans see their democracy as deeply vulnerable to influence operations on social networks, as well as penetration of election infrastructure. With no satisfactory safeguard against foreign interference in place and the 2020 presidential election cycle fast approaching, these concerns are likely to persist”(Pigman, 2019a).

Secrecy is one of the reasons to why attacks in cyberspace can continue to flourish. Awareness of the problem is vital, both in the government and in the private sector. This is especially important when subversive operations are carried out using the freedom of speech as a shield[13].

Raising the general awareness of cyberattacks, can be accomplished through education. This is a long process, but can be effective in curtailing an attacker's chances of success.

Publicity is another important factor to subdue the desirability of attacking, since *"an incipient aggressor may be inhibited by his own conscience, or more likely, by the prospect of losing moral standing, and hence political standing, with uncommited countries" (Snyder, 1961, p. 10).*

The indictment of the thirteen members of the Internet Research Agency and the conviction of Maria Butina (Heggen, 2019) in connection with the American presidential election 2016, the public denunciation of the Russian attempt at hacking into the computer system of the Organisation for the Prohibition of Chemical Weapons in the Hague [14] and the worldwide publicity in the aftermath of the Skripal gas attack in Salisbury, represent ways of how this can be achieved. Considering these targets, Russia can be seen as seeking to bolster its political standing. "*Embarrassed by ... truth, Russia fought back by retaliating against the truth tellers and against the truth itself"(Demers, 2018).*

Publicity and free speech is also the Achilles' heel of authoritative states, sensitive as they are to public opinion. Letting the sun in by means of education, awareness and publicity are vital elements to curb the mass of state-sponsored cyber-attacks and make the trolls burst.

[13] E.g. Russia Today, which transmits in Arab, French, English, German, Spanish and has launched subsidiaries outside Russia, notably in France, where the channel has sided with "les vestes jaunes"(Torvik, 2019).

[14] In 2018, four GRU operatives were caught trying to hack into the computer network of the Organisation for the Prohibition of Chemical Weapons (OPCW). Plans for their next target, a laboratory in Switzerland were found among the agents' possessions. The OPCW and its laboratory were responsible for the investigation and forensic work following the Skripal nerve agent attack (2018) and the gas attacks in Syria. *"... the evince..., the overarching Russian strategic goal: to pursue its interests through illegal influence and disinformation operations aimed at muddying or altering perceptions of the truth."* (Demers, 2018)

6.4. Deterrence - A long haul[15]

Cyberspace resembles the Wild West in the sense that it is a place where vast areas are left without any authority capable of upholding the law. Will the anarchy and lack of legislation continue to remain the situation in cyberspace?

In 1953, President Eisenhower did not see the deterrence of Soviet Russia as a quick-fix. In his eyes *"The USSR will continue to rely heavily on tactics of division and subversion to weaken the free world… exploit differences among members of the free world… to manipulate opinion and control governments wherever possible" (162/1, 1953).*

In order to counter the constant threat from the USSR, the NSC 162/1 prescribed in addition to military forces and readiness, the maintenance of a strong economy, the maintenance of morale and the operation of free institutions, expand scientific training and provide for an appropriate distribution of services in the event of national emergency.

The seesaw competition of offense and defense may be slowly turning direction. As has been shown, legislation is slowly curbing the free- roaming days of social media. International discussions are held on how to curb attacks in cyberspace. States have intensified their efforts to prevent successful attacks by improving their defensive cyber architecture and become more resilient to attacks. On the other hand, we may have seen some attempts that retaliation has been carried out. Should the offense keep the supremacy over defense in cyberspace these attempts can evolve into deterrence by punishment.

In the end, law and order came to the West. Subjected to state jurisdiction, the Wild West ceased to be. With growing international cooperation, setting standards for the safeguarding of network traffic, technical solutions, prosecution and punishment of attackers, each country's cyberdefense can become far more effective. Through publicity and awareness, it will become harder for malefactors to influence the public.

It will probably be the concerted efforts of international cooperation, stricter regulation of social media, improved national security, education and awareness and finally the threat of retaliation that will deter attackers, mitigate the consequences of attacks and safeguard free

[15] The quote signified Dwight D. Eisenhower's vision for defense planning to ensure constant readiness and vigilance

elections, free speech and safe infrastructure. Such processes take time, but there are signs that the days of Wild West of cyberspace are coming to an end.

6.5. Further research

Cyberspace is still in development, which means that there will be new vulnerabilities to exploit and new ways to exploit them. The emergence of the Internet of Things (IoT), cloud computing and the worry among Western democracies of allowing Chinese companies to deliver 5G networks, are all signs that the vulnerabilities and attacks in cyberspace may be with us for years to come.

International cooperation to stop cyberattacks is probably a key to reduce their virulence. There is cooperation between security firms and different government bodies to share information on discovered threats and how they can be neutralized. Nonetheless, we see companies and states can be successfully attacked by the same malware after it has been discovered and the solution to stop it has been divulged. The example of Hydro is a case in point. The same virus attacked Altran on January 24th and Hydro was not hit until the 15th of March. What are the obstacles to rapid publication of new threats and implementation of countermeasures?

Zero- day exploits are among the favourite weaknesses exploited in cyber-attacks. The black market ecosystem of cyberspace is an important part of the threats in cyberspace. It is here that “zero-day”- exploits have been sold off to the highest bidder, and where states are suspected to be potential buyers.(Ablon, Libicki, & Golay, 2014, pp. 25-28) Some companies have offered bounties to persuade hackers sell their information back to them in order to stop the vulnerability and improve their products. This has the potential of turning criminal hackers into legitimate actors. International cooperation may also have an impact through investigation and prosecution. What means are effective to reduce the malignant spreading of zero-day exploits? The black market of cyberspace and how it can be curbed is a field that warrants more research.

In his book, “The soul of Battle”, Victor Davis Hanson writes about how the three generals Epaminondas[16], Sherman[17] and Patton[18] fought against and vanquished tyranny. One of Hanson’s main points in this book is that their armies were democratic, and that it was the democratic spirit that was pivotal to these victories. Their tyrannical enemies had an “Achilles’ heel” in that they suppressed their population[19].(Hanson, 1999)

As has been shown earlier, authoritarian states today have the same disadvantage in that they need to control their own population. This vulnerability is recognised by authoritarian regimes and the West has been accused of manipulating popular sentiment (Pigman, 2019a). This attack vector has not been exploited in any known attacks, but could become a powerful deterrent measure against such adversaries. Influence cyber operations against authoritative states, their effects and their influence on international relations is a topic for further research.

[16] Theban general who defeated the Spartan empire in the fourth century BCE.

[17] American general, who played a major part with his “army of the West” in defeating the Confederacy (1860-1865)

[18] American general. Led the US Seventh Army in the Mediterranean theatre and the U.S. Third Army through France and Germany during WW2.

[19] Sparta suppressed the Helots, The Confederacy was a slave economy and the Third Reich had occupied most of Europe.

7.Appendix A Advanced Persistant Threats

APT	Name	Origin	Targeted sectors
APT1	Unit 61398, Comment Crew	China's People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department	IT, defense, aerospace, science, space, high tech, international organizations
APT3	UPS Team	China	Aerospace, Defense, Constructio, Engineering, High Tech, Telecommunications,Transportation
APT5		unknown	Asia-Based Telecommunications, and Tech Firms, High-Tech Manufacturing, Military Application Technology and satelite communication
APT10	Menupass Team	China	Construction, engineering, aerospace, telecom, United States, European, and Japanese govts.
APT12	Calc Team	China	Journalists, government, defense industrial base
APT16		China	Japanese and Taiwanese high-tech, government services, media and financial services industries
APT17	Tailgator Team, Deputy Dog	China	U.S. government, and international law firms and information technology companies
APT18	Wekby	China	Aerospace, Defense, Construction, Engineering, Education, Health and Biotechnology, High Tech, Telecommunications, Transportation
APT19	Codoso Team	China	Legal and investment
APT28	Fancy Bear/Sofacy/Tsar Team/Pawnstorm/Sednit/CyberCaliphate/Cyber Berkut/Voodoo Bear/Sandworm/BlackEnergy Actors/STRONTIUM	Russia, GRU	USA, Europe, Caucasus, NATO, EU, defense,

APT29	The Dukes/Cozy Bear	Russia, FSB[20]/SVR[21]	Western European governments, foreign policy groups and other similar organizations
APT30		China	Members of the Association of Southeast Asian Nations (ASEAN)
APT32	OceanLotus Group	Vietnam	Foreign companies investing in Vietnam’s manufacturing, consumer products, consulting and hospitality sectors
APT33		Iran	Aerospace, energy
APT34		Iran	financial, government, energy, chemical, and telecommunications
APT37	Reaper	North Korea	South Korea, chemicals, electronics, manufacturing, aerospace, automotive, and healthcare
APT38		North Korea	Financial institutions world-wide

[20] Federal Security Service of the Russian Federation

[21] Foreign Intelligence Service of the Russian Federation

8.Appendix B

Cyberattacks connected to APT 28 (GRU)

Attack	Assessment
Between July and August 2015 multiple email accounts belonging to a small UK-based TV station were accessed and content stolen.	NCSC[22] assess with high confidence that the GRU was almost certainly responsible.
In August 2016, confidential medical files relating to a number of international athletes were released. WADA stated publicly that this data came from a hack of its Anti-Doping Administration and Management system.	NCSC assess with high confidence that the GRU was almost certainly responsible.
In 2016, the Democratic National Committee (DNC) was hacked and documents were subsequently published online.	NCSC assess with high confidence that the GRU was almost certainly responsible.
In October 2017, BadRabbit ransomware encrypted hard drives and rendered IT inoperable. This caused disruption including to the Kyiv metro, Odessa airport, Russia’s central bank and two Russian media outlets.	NCSC assess with high confidence that the GRU was almost certainly responsible.
Attack NCSC Assessment In June 2017 a destructive cyber attack targeted the Ukrainian financial, energy and government sectors but spread further affecting other European and Russian businesses.	The UK Government attributed this attack to the GRU in February 2018. NCSC assess with high confidence that the GRU was almost certainly responsible.
In October 2017, VPNFILTER malware infected thousands of home and small business routers and network devices worldwide. The infection potentially allowed attackers to control infected devices, render them inoperable and intercept or block network traffic.	In April 2018, the NCSC, FBI and Department for Homeland Security issued a joint Technical Alert about this activity by Russian state-sponsored actors.
In March 2018 the GRU attempted to compromise the UK Foreign and Commonwealth Office (FCO) computer systems via a spearphishing attack.	NCSC assess with high confidence that the GRU was almost certainly responsible.
In April 2018 the GRU attempted to use its cyber capabilities to gain access to the UK Defence and Science Technology Laboratory (DSTL) computer systems.	NCSC assess with high confidence that the GRU was almost certainly responsible.

[22] National Cyber Security Centre. The NCSC supports the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public.

In April 2018 the GRU attempted to use its cyber capabilities to gain access to official OPCW[23] computer networks.	NCSC assess with high confidence that the GRU was almost certainly responsible.
In May 2018 GRU hackers sent spearphishing emails which impersonated Swiss federal authorities to directly target OPCW employees, and thus OPCW computer systems. These employees were likely attending a forthcoming conference in Spiez.	NCSC assess with high confidence that the GRU was almost certainly responsible.

(National Cyber Security Centre, 2019)

[23] Organisation for the Prohibition of Chemical Weapons. The OPCW is the implementing body for the Chemical Weapons Convention, and oversees the global endeavour to permanently and verifiably eliminate chemical weapons.

9.Bibliography

162/1, N. (1953). Report to the National Security Council by the Executive Secretary *NSC 162/2*. Retrieved from https://history.state.gov/historicaldocuments/frus1952-54v02p1/d101

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Zero-Day Vulnerabilities in the Black and Gray Markets. In *Markets for Cybercrime Tools and Stolen Data* (pp. 25-28): RAND Corporation.

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners*: Elsevier.

Art, R. J., & Jervis, R. (2009). *International politics: enduring concepts and contemporary issues*.

Assessment, I. C. (2017). *Assessing Russian Activities and Intentions in Recent US Elections*. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Barzashka, I. (2013). Are Cyber-Weapons Effective? *The RUSI Journal, 158*(2), 48-56. doi:10.1080/03071847.2013.787735

Beaufre, A. (1965). *Deterrence and strategy*. London: Faber Faber Ltd., 24 Russel Square, London.

Boyd, R. L., Spangher, A., Fourney, A., Nushi, B., Ranade, G., Pennebaker, J., & Horvitz, E. (2018). Characterizing the Internet Research Agency's Social Media Operations During the 2016 US Presidential Election using Linguistic Analyses.

Brantly, A. F. (2018). *The Cyber Deterrence Problem*. Paper presented at the 2018 10th International Conference on Cyber Conflict. https://ccdcoe.org/uploads/2018/10/Art-02-The-Cyber-Deterrence-Problem.pdf

Centre, N. C. S. (2019). The National Cyber Security Centre. Retrieved from https://www.ncsc.gov.uk/

Chien, E. (2010). Stuxnet: A Breakthrough [Stuxnet investigation]. Internet web page Retrieved from https://www.symantec.com/connect/blogs/stuxnet-breakthrough

CIA. (2017). Digital Innovation. Retrieved from https://www.cia.gov/offices-of-cia/digital-innovation

CIA. (2018). About CIA. Retrieved from https://www.cia.gov/about-cia/todays-cia/what-we-do

Clausevitz. (1993). *On War* (10 ed.): Knopf, Alfred.A.

De Falco, M. (2012). *Stuxnet Facts Report. A technical and Strategic Analysis*. Retrieved from Tallinn: https://ccdcoe.org/library/

Defence, M. o. (2004). Section 2.2 Military necessity. In *The Manual of the Law of Armed Conflict*. Oxford: Oxford University Press.

Defense, U. S. D. o. (2018). *Cyber strategy*. https://www.defense.gov Retrieved from https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Demers, J. C. (2018). Remarks on the Unsealing of an Indictment Against Russian GRU Officers for Various Malicious Cyber Activities. In (October 4. ed.): United States Department of Justice.

Etterretningstjenesten. (2019a).

Etterretningstjenesten. (2019b). *Fokus 2019*. Retrieved from www.forsvaret.no/fokus.

F-Secure. (2017). *State of cybersecurity*. Retrieved from https://fsecurepressglobal.files.wordpress.com/2017/02/cyber-security-report-2017.pdf

FBI. (2019). Counterintelligence. Retrieved from https://www.fbi.gov/investigate/counterintelligence/foreign-influence

Fox-Brewster, T. (2017). NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid'. *Forbes*.

George, A. L., & Smoke, R. (1974). *Deterrence in American foreign policy: Theory and practice*: Columbia University Press.

Gould, J. (2018). McCain book: US should consier cyberattack to punish Putin. *Defense news*. Retrieved from defensenews.com website: https://www.defensenews.com/video/2018/05/04/mccain-book-advocates-cyberwarfare-retaliation-against-russia/

Hamnes, L. (2012, June 3.). 16 spektakulære cyberangrep. *teknisk ukeblad*.

Hansen, K. (2019, 2019, February 27). USAs militærhackere gikk til angrep: Skrudde av internett i russisk trollfabrikk. *Aftenposten*. Retrieved from https://www.aftenposten.no/verden/i/ddVvzJ/USAs-militarhackere-gikk-til-angrep-Skrudde-av-internett-i-russisk-trollfabrikk

Hanson, V. D. (1999). *The soul of battle: From ancient times to the present day, how three great liberators vanquished tyranny*: Simon and Schuster.

Heggen, Ø. (2019). Første russer dømt for å påvirke presidentvalget i USA. Retrieved from https://www.nrk.no/urix/russisk-kvinne-domt-for-a-ha-pavirket-usas-presidentvalg-og-infiltrert-vapenorganisasjon-1.14529551

House of Commons, D., Culture, Media and Sport committee. (2019). *Disinformation and 'fake news': Final Report*. www. parliament.uk/dcmscom: Parliamentary Copyright House of Commons Retrieved from |https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

House, W. (1961). President Kennedy's special message to the congress on urgent national needs. In (May 25., 1961 ed., pp. 24). John F. Kennedy Presidential Library and Museum.

House, W. (2018). *National Cyber Strategy - 2018*. The White House Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Hydro, N. (2019a). Hydro subject to cyber attack [Press release]. Retrieved from https://www.hydro.com/en/media/news/2019/hydro-subject-to-cyber-attack/

Hydro, N. (2019b). Update on cyber attack April 5. In (April 5. , 2019 ed.).

Inbar, E., & Shamir, E. (2014). 'Mowing the Grass': Israel's Strategy for Protracted Intractable Conflict. *Journal of strategic studies, 37*(January 2014), 26. doi:10.1080/01402390.2013.830972

Jasper, S. (2017). *Strategic cyber deterrence: The active cyber defense option*: Rowman & Littlefield.

Jervis, R., Lebow, R. N., & Stein, J. G. (1985). *Psychology and deterrence*. Baltimore and London: JHU Press.

Justice, U. S. D. o. (2018). *Internet Research Agency Indictment*. Retrieved from https://www.justice.gov/file/1035477/download.

Kaufmann, W. W. (1954). *The requirements of deterrence*. In memoranda, Vol. memorandum 7. (pp. 23). Retrieved from http://findit.library.yale.edu/catalog/digcoll:560733

Kennan, G. F. (1985). *Morality and Foreign Policy*: Council on Foreign Relations.

Kissinger, H. (2015). *World order*: Penguin Books.

l'Elysée, P. d. (2018). *Paris call for trust and security in cyberspace*. www. diplomatie.gouv.fr.

Lebow, R. N. (1985a). Conclusions. In *Psychology & Deterrence* (pp. 203-232). Baltimore and London: Johns Hopkins University Press.

Lebow, R. N. (1985b). The Deterrence Deadlock. In *Psychology and Deterrence* (pp. 180 - 202). Bltimore and London: Johns Hopkins University Press.

Mearsheimer, J. J. (1985). *Conventional deterrence*: Cornell University Press.

Morgan, P. M. (1983). *Deterrence: A conceptual analysis* (Vol. 40): Sage Publications.

Nations, U. (1945). U.N Charter. In.

NATO. (2018). Cyber defence. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm

NSA. (2019). Cybersecurity. Retrieved from https://www.nsa.gov/what-we-do/cybersecurity/

Nye Jr, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44-71.

Philbin, M. J. (2013). *Cyber deterrence: An old concept in a new domain*. Retrieved from

Pigman, L. (2019a). Behind Russia’s cyberwarfare lies a serious case of cyber-phobia. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2019/01/17/behind-russias-cyberwarfare-lies-a-serious-case-of-cyber-phobia/?noredirect=on&utm_term=.d55b5e119062

Pigman, L. (2019b). Russia’s vision of cyberspace: a danger to regime security, public safety, and societal norms and cohesion. *Journal of Cyber Policy, 4*(1), 22-34. doi:10.1080/23738871.2018.1546884

Price, R. (2016, August 15, 2016). 'Shadow Brokers' claim to have hacked an NSA-linked elite computer security unit. *Business Insider*. Retrieved from https://www.businessinsider.com/shadow-brokers-claims-to-hack-equation-group-group-linked-to-nsa-2016-8?r=US&IR=T&IR=T

Ravindranath, M. (2014). Panetta: Cyberspace is "battlefield of the future". *The Washington Post*. Retrieved from Panetta: Cyberspace is "battlefield of the future" website:

Rid, T. (2013). *Cyber war will not take place*: Hurst & Company, London, UK.

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

Rowney, K. (2011). What We Talk About When We Talk About APT. Retrieved from https://www.symantec.com/connect/blogs/what-we-talk-about-when-we-talk-about-apt

Sanger, D. E. (2018, November 12 2018). U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks. *The New your Times*. Retrieved from https://www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html?rref=collection%2Ftimestopic%2FStuxnet

security, U. D. o. H. (2019). National Cybersecurity and Communications Integration Center. Retrieved from https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center

Sheldon, J. (2012). Toward a Theory of Cyber Power. *Cyberspace and National Security*, 207-224.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*: Oxford University Press USA.

Snyder, G. H. (1961). *Deterrence and defense* (Vol. 2168): Princeton University Press.

Thucydides. (ca. 420 BCE). the Peloponnesian war. In (pp. 713). New york: Free Press.

Tolga, I. B. (2018). *Principles of Cyber Deterrence and the Challenges in Developing a Credible Cyber Deterrence Posture* Retrieved from https://ccdcoe.org/

Torvik, Y. G. (2019, April 10, 2019). From Russia with love? *Klassekampen*, pp. 20-21.

UN. (October 25th, 2018). The Application of International Law in Cyberspace: State of Play. Retrieved from https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/

Waltz, K. N. (2010). *Theory of International Politics*: Waveland Press.

Williams, K. R., & Hawkins, R. (1986). Perceptual research on general deterrence: A critical review. *Law and Society Review*, 545-572.

Woodward, B. (2004). *Plan of attack*: Simon and Schuster.

Yost, D. S. (2003). Debating security strategies. *NATO review*(Winter 2003), 15 - 19.

Zetter, K. (Producer). (2011). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. [news article] Retrieved from https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/