FACULTEIT POLITIEKE EN SOCIALE WETENSCHAPPEN

COULD CYBER-WARFARE BE CONSIDERED A NEW TOOL OF FOREIGN POLICY?

Wetenschappelijke verhandeling
Aantal woorden: 19772

Nanouk Lemmerling
Stamnummer: 01308152

Promotor: Prof. dr. Jeroen Joly
Copromotor: Prof. dr. Wouter Lips

Masterproef voorgelegd voor het behalen van de graad master in de richting Politieke Wetenschappen afstudeerrichting Internationale Politiek

Academiejaar: 2016 - 2017

UNIVERSITEIT GENT

I. Acknowledgments

Throughout this exhausting, but meaningful and interesting research work I struggled to find individuals and institutions willing to discuss with me the topic in question. Therefore, I would firstly like to thank all the people who took the time to discuss the topic and allowed me to interview them. Without their input my thesis would not have produced such an interesting conclusion.

Given the fact it was the first time I wrote a paper of such length in English I was advised to have native speakers read over it. For this, I extend my sincere gratitude to my lovely Erasmus friends, Kerrie O' Flynn and Miranda Wadham, who took time to proof read this master thesis. Hereby I would like to give an extra thankyou to my dear Erasmus friend Gemma Moynihan who has proof read this thesis several times. Sincere thanks also to Faisal Al Suhail, for proof reading this thesis.

Special thanks however, must be given to my supervisor; Professor Jeroen Joly. Without your excellent guidance, advice and assistance I would not have been able to write my thesis at all. For this, I thank you.

II. Abstract

Doorheen de jaren is het onderwerp van cyber en alles wat hierrond leeft in toenemende mate op de voorgrond gekomen. Deze master thesis ontfermt zich over de onderzoeksvraag of cyber oorlogvoering een nieuw onderdeel van buitenlandse beleidsvoering is geworden. Als onderzoeksmethode kozen we voor het afnemen van interviews. Daarbovenop hebben we een uitgebreide literatuurstudie verricht. Uit onze resultaten hebben we kunnen concluderen dat cyber oorlogvoering een beduidend onderdeel is geworden van buitenlandse beleidsvoering en dat het belang hiervan enkel nog zal toenemen.

Nadat we tot bovenstaande vaststelling zijn gekomen, ondervonden we daarnaast dat er een drievoudige denkstroom bestaat met betrekking tot cyber oorlogvoering. Ten eerste bestaat er een denkstroom die niet gelooft in het bestaan van cyber oorlogvoering als toekomstbeeld. Ten tweede is er een stroming, die zich in de meerderheid begeeft, die gelooft dat cyber oorlogvoering enkel mogelijk is als complement van conventionele oorlogvoering. De derde stroming gelooft dat de toekomst cyber oorlogvoering *an sich* zal worden. Hierbij zal dan ook de conventionele oorlogvoering op de achtergrond komen, sterker nog: deze zal op termijn verdwijnen. Desondanks het feit dat de derde stroming een minderheid vormt hebben wij geconcludeerd dat er een grote kans bestaat dat dit wel degelijk onze toekomstige oorlogvoering zal worden. Niettegenstaande dat we ons momenteel nog steeds bevinden in een wereld waar cyber oorlogvoering slechts een aanvulling is op de klassieke oorlogvoering. De eerste stroming is voor ons reeds voorbijgestreefd en achterhaald.

III. Table of contents

1. Introduction

We are currently living in the age of technology, and this age is advancing in an extremely rapid way. Within this age of technology there has been a rise of new threats. These threats emerge in the cyber-world and can lead to a cyber-warfare. All aspects of cyber are increasingly becoming important and set to become a central factor in international relations. Throughout the last century cyber-politics was considered to be non-existent. However, with the rise of the Internet, cyber-warfare has slowly begun to be recognized as an aspect – albeit a modest one – of foreign politics. This topic has received much attention in the past decade and is being increasingly noted as a pivotal aspect of global society. The next decade is predicted to witness a considerable rise in the use of instruments, politics and interests concerning cyber-warfare. One major weakness with the field of cyber is that the characteristics of it are not well understood and thus this topic has yet to be dealt with in an in-depth manner. Despite the rise of literature surrounding cyber-warfare rapidly growing in recent years, this issue has still yet to be fully established in political sciences. Moreover there is still substantial controversy surrounding this subject. Uncertainty remains on how states are dealing with and preparing themselves against these upcoming cyber-threats.

The greatest interpreter of modern war, Carl von Clausewitz, defined war as followed: *a social activity that involves mobilization and organization of individual men, almost never women, for the purpose of inflicting physical violence. It entails the regulation of certain types of social relationships and has its own particular logic* (Clausewitz, 1989, p. 202). Today this definition is outdated, especially in the study of the cyber-domain. The concept of cyber as a fifth domain in war is becoming increasingly popular. Despite the fact that a war fought in this domain might at this moment be unthinkable, it is of utmost importance to consider it because it sheds new light on the future of international relations. This new form of warfare includes new dimensions, contains borderless transnational thinking and carries consequences to a profound extent.

This paper aims to call into question the idea that cyber is becoming a new tool of foreign policy, and if so, what is the likelihood of this leading to cyber-warfare. An exploration will be made about the viability of cyber as an instrument in foreign policy. The form this new instrument would assume will also be assessed. Many countries are making considerable progress in embedding cyber-security in their foreign policy. This is done by being increasing awareness of the risks associated with the cyber-domain, thus investing in technology to protect security of vital cyber infrastructure[1]. Some states and non-state actors are even investing in offensive cyber-warfare capabilities. This is important in this study as if states or non-state actors invest in offensive cyber-warfare capabilities as an instrument of their foreign policy, this could contribute towards a cyber-war (Institute for Defence Studies and Analyses, 2016).

On the 12th of May 2017 there was a worldwide cyber-attack. Seventy-four countries were harassed by a ransomware attack (see infra). Not only were the Russian interior Ministry and the Spanish telecommunication company Telefonica attacked, the National Health Service in the United Kingdom (UK) was attacked too. Six hospitals in the UK were confronted with major IT disruptions in this cyber-attack. It caused massive delays and a variety of problems; several patients were evacuated, ambulances were diverted to hospitals nearby and operations were canceled. Patients were advised to only visit the hospital for extreme emergencies and were told to not contact their general practitioner for unnecessary reasons. American intelligence services and other cyber-experts claim the attack comes from North-Korean hackers. However, there has not been a decisive conclusion on this case. The British opposition party Labour argued that the attack on the hospitals highlighted the urgent need for cyber-security to be placed at the heart of government policy. It also displays the extent of consequences a cyber-attack can bring and how important this subject is becoming in the daily life of people and the thinking of policy makers (Al Jazeera, 2017; CNN, 2017; Debruyne, 2017; edm, 2017).

[1] Vital infrastructure, or often referred to as critical infrastructure, is infrastructure that is essential for the functioning of a society. For example hospitals are infrastructures that are critical for the public health.

So far, there has been some disagreement in regards to what cyber in the future can bring. With this criterion in mind as we undertook this study, asserting that we have found three streams in the discourse surrounding the role of cyber-warfare in foreign policy. Firstly, there is the group of academics that believe cyber-warfare will never become a new form of warfare. Secondly, there is a majority stream of thinkers who believe cyber-warfare will complement conventional warfare. Here we can speak of the emergence of hybrid warfare. Hybrid warfare captures the mixture of coercive and subversive activity, conventional and unconventional methods. This can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare (Royal Higher Institute For Defence, 2017). Thirdly, there is a group of thinkers that believe cyber-warfare will replace conventional warfare.

This paper is divided in multiple sections and sub-sections. We begin by explaining the chosen research method, which is a semi-structured interview. This is followed by a brief explanation on the history of the Internet and why it carries such high importance. In the third sub-section we give an overview of the terminology used in this field. Given the fact that the cyber-world is complex, abstract and not fully understood we deem it necessary to give an extensive clarification of all the different terms relevant to the cyber-world. The fourth sub-section starts with an analysis of the possibility of implementing cyber as a policy instrument. This sub-section begins with examining the evolution in policy instrument studies. Sub-section seven demonstrates how a real example of a cyber-attack can potentially lead to cyber-warfare, namely the cyber-attack conducted by the Stuxnet-virus. This example has influenced the thinking in cyber-warfare, thus carries high importance for our research. We then continue with a comprehensive interpretation on why actors would choose for cyber-warfare instead of conventional warfare. This chapter also examines all the complexities and problems cyber-warfare carries with it. We continue with a comparison between conventional warfare and cyber-warfare, follower by the

sub-section that explores whether cyber can change the international power balance. Our last sub-section describes the three streams in cyber-warfare thinking, as mentioned before. Our conclusions are drawn in the final section.

2. Research method

In order to understand, investigate and analyze the topic of this master thesis the research method chosen is interviews. It was decided that this was the best method for this research because it is one of the most practical and feasible methods to gain the most relevant information. Above that, the topic of this master thesis is not widely understood and often perceived as a controversial subject. Lastly, though there might be a growing body of literature concerning this topic; it remains a new and constantly evolving one. Therefore, interviews were concluded to be the most suitable way to gain the most recent and reliable information.

We have interviewed several people and institutions on the matter. These interview sources were reliable and on recommendations of cyber experts, whom we also interviewed. All the interviews were carried out semi-structured. Mortelmans (2007) describes different types of interviews in his text. The interview technique we conducted falls between a structured interview and an open interview. It's a prepared form of interview with a topic list and a question protocol. All topics and questions were carefully well thought out and considered. It's a semi-structured interview because although all the questions were written out, the continuation of the interviews happened informal and in the mostly natural way. There were no obligations to strictly follow every question on the list. Once again, we have chosen this method to gain as much information as possible and sometimes this could only be achieved by letting go of a strict protocol.

All the interviews (seven in total) were performed live in a face-to-face form. This was done in order to create a direct interaction between the people we interviewed. As Mortelmans has described, to gain the most informative answers an online chat-session or a telephone conversation would not achieve the same

results. Some institutions asked to send the question protocol in advance. Although this was asked, this didn't create a formal atmosphere during the interviews. All interviews, except for one, were recorded with consent. This gave us more freedom and leverage to have a fluent and interactive conversation.

The opening questions were mostly structured and dealt with factual, contextual and technical information. This was followed by transition questions on what experiences and specific knowledge these institutions or persons have concerning the topic. Finally, we finished with key questions. These were based on opinions, observations and perceptions. These questions were posed for additional information but also out of personal interest.

At the beginning of the study we encountered some problems finding people and institutions that were willing to participate. The desired sources are described by Mortelmans as elite-interviews. These sources are very difficult to reach and the first contact happens via a second person that controls the agenda of the first person. They often occupy an important position and are valuable for our research. Once we got a first contact person we noticed a snowball effect. After every interview we gradually got referred to another relevant source, and this continued throughout the whole study. Only after being able to contact one person we finally got indirectly in contact with other sources. This reveals an elusive side to our topic. However, we never noticed a trend in dodging, avoiding or refusing answering questions.

Initially these interviews were going to complement the literature study, but because the overall responses to the questions were unexpectedly informative and helpful they became a great addition to this master thesis. We were able to conduct cross-references by asking the same questions in every interview. We noticed matching answers that helped creating trustworthy conclusions.

3. The Internet

3.1. The importance of the Internet

In assessing the history of crime, a strong pattern of continuity can be seen in the motivations and objectives behind them. What has changed however, is the nature of the attacks. This includes the tools, the methods and the results. As Grabosky has called it "*old wine in new bottles*" (Grabosky, 2001, p. 243). The Internet has given a new life to the nature of crimes, as they cannot be felt physically and currently are carried out in an environment which has yet to formulate an extensive cyber-law system. One individual has the power to reach, interact with, and affect a million of other individuals at the same time. This makes computer-mediated communication a force-multiplier (Yar, 2013).

Modern technology has facilitated attacks that can have extremely destructive outcomes. This evolution in modern technology has led us into a new society, known as the information age. The Internet has created a cyber-space where opportunities for crimes and threats are seemingly limitless. It gives significant power in the hands of one person. With this power and with few resources these individuals can enable attacks with potentially colossal negative outcomes. These outcomes can vary in their adverse effects, stretching from stolen credit card data to implanting viruses in nuclear devices (see infra) (Schell & Martin, 2006; Yar, 2013).

The Internet as a postmodern medium is the most powerful tool for political organization. There are several reasons why the Internet can be seen as the most powerful tool used for political difference, conflict and group gathering. This also explains why the act of cyber-crimes has become so popular (Karatzogianni, 2008).

First of all the Internet is cheap. This gives the opportunity to several key players all around the world to buy basic facilities and influence other people, groups and institutions worldwide. Secondly, the Internet is largely uncensored. Or at

least not sufficiently censored. Spreading (extremist) thoughts, hate, X-rated material has become very easy. Any information and propaganda can reach would-be-sympathisers, quicker than any rally or pamphlet distribution could ever do (Crilley, 2001). We notice a tendency of the Internet to capsize or hedge barriers created by government censors. This is especially important in non-democratic countries because it gives citizens the opportunity to bypass the traditional censorship existing within the state borders. Although we can speak of a decrease in government censorship, the Internet can most probably never be free of censorship (Arquilla & Ronfeldt, 2001). Thirdly, the audience of the Internet has become worldwide. People can reach each other from all over the globe in the widest sense possible, making it a globalized phenomenon. The Internet does not require face-to-face contact, and this enables easy communication with no restrictions, nor social boundaries. The online communities can frequently offer a new dimension to a personal identity. This occurs even faster when a person suffers from low self-esteem, feels left out or alienated in its own society or environment (Karatzogianni, 2008). The Internet offers several avenues for dialogue, giving the opportunity for any person to pitch their ideas or plans. Finding someone who affiliates to or justifies those ideas and plans is not a difficult task. As a fourth reason we note that the Internet bypasses national laws. The Internet is not fully governed or owned by one person, thus making it a very difficult place to police. Every country has its own national laws making certain actions illegal but with the Internet these measurements are easy to bypass (Crilley, 2001). Above that the Internet has, in most places, an unlimited access. The Internet has the potential for an infinite expansion. This makes the cyber environment a very dangerous place because it gives different socio-political or extremist groups a platform to permanently stay in contact. Additionally this only facilitates the influence on members or followers worldwide and enables groups to promote their own version of the truth (Karatzogianni, 2008). As Negroponte has illustrated *"the agent of change will be the Internet (…). The Internet is interesting not only as a massive and pervasive global network, but also as an example of something that has evolved with no apparent designer in charge (…)"* (Negroponte, 1995, p. 181).

The above-mentioned reasons are all advantages of using the Internet; of course using the Internet can have disadvantages as well, which could discourage cyber criminals to conduct cyber-crimes.

The first disadvantage applies to groups that emerged from the Internet. These groups can only exist because of their communication through the Internet. Their line of communication can be cut and this would mean an immediate death to their existence. Secondly, every idea, (upcoming) project, discussion or other can most likely be seen by everyone, and consequently be intercepted. The Internet cannot always guarantee the 'underground' aspect of people gathering in complete seclusion and secret. Thirdly, the accuracy, validations and correctitude of information attained through the Internet is more difficult to validate. Groups, institutions or individuals who rely on the Internet for news, facts or their daily work have to be attentive at all times for possible fake, misleading, inaccurate or biased information (Crilley, 2001).

Given the gap between the advantages and the disadvantages of the Internet, it can be concluded that the Internet is a very persuasive tool for enabling political actions or perform cyber-crimes. The Internet as a source for political change should, therefore, never be underestimated.

3.2. A swift evolution of the Internet and the cyber-world

As reported previously, technology is evolving in an extremely rapid way. It's important to compose a short history of the Internet first before going deep into our research work. We will show the emergence of cyber-crime, cyber-security and eventually cyber-defence in order to completely understand how brisk this technological evolution has been and probably will continue to be.

All roots from our current Internet can be found in the 1960's ARPANET. This was an operational computer network sponsored by the US military. It was originally created to build up a resilient and secure network for military

activities. The ARPANET was seen as a highly important network to sustain communication during the Cold War era where nuclear confrontations formed a permanent threat. The network of the ARPANET consisted out of a packet switching mechanism. This allowed communications to be broken up into 'packet's that could then be sent via several ways to their destination. Once these packets arrived to their destination they could be reassembled to their original form (Yar, 2013).

During these first years of increasing information freedom and technology advances several world players shared a contradictory view on the development. On the one hand, information should be freely shared, and shared to all. But on the other hand information access should be limited and restricted. This was concluded because states tried to protect themselves against possible misuse (Powers & Jablonski, 2015).

From that moment on the innovations and changes occurred quickly. Beginning in 1970, it was made possible to send electronic mail. Apart from the ARPANET, other networks started to emerge. Later on these networks got connected with each other, creating one 'internet'. This single network was known as a structure made up of many linked networks, collectively they were known as the Internet's backbone (Kelsey, 2008). At this point there was no sign of cybercrimes or cyber-security.

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

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

Several attempts have been made to find the starting point of a cyber-warfare era. Although there is no official starting point from where we can speak of the first cyber-attack or a first cyber-crime, a considerable amount of authors (Geers, 2014; Kelsey, 2008; Milosevic, 2015; et. al.) have agreed upon the Kosovo war in 1999 as the first Internet war. This war started in March as an armed conflict between the Federal Republic of Yugoslavia and the Kosovo Liberation Army. The latter received air support from the North Atlantic Treaty Organization (NATO). A pro-Serbian hacker group, named Black Hand, performed several DoS-attacks (see infra) against NATO, the US and the UK. They took down several websites owned by the Kosovo Liberation Army that published propaganda and they took the official website of NATO offline. Several Yugoslavian hackers were helped by Russian hackers to take down US military and navy websites. After NATO attacked the Chinese Embassy in Belgrade, Chinese hackers joined the group of Yugoslavian and Russian hackers. Although the conflict ended officially in June of that year, several attacks continued in cyber-space (CNN, 1999; Geers, 2014).

Cyber-security has only come to prominence after big events. We can notice an exponential change in cyber-security after the events of 9/11. Substantial soft and hard measurement have been taken to enable surveillance and control of suspected cyber-dangers to the society. In 2003 former president George Bush signed the order known as the National Security Directive 16. This order was created to develop guidelines for offensive cyber-warfare (Levi & Wall, 2004).

Apart from the Kosovo war in 1999, many authors (Europe Institute, 2008; Evron, 2017; O'neill, 2016; et. al.) maintain the start of a cyber-warfare era can

be found back in the cyber-attacks conducted against the Estonian government in 2007. This cyber-war is often referred to as 'Cyber-war I'. On April 27th 2007 the Bronze Soldier of Tallinn was swiftly removed and relocated to a military cemetery. The riots that had been going on as a response to the Russian-Estonian quarrels of that year were only enforced when the Estonian government moved the statue. A revolution broke out in both countries. Russian activist groups besieged the Estonian embassy in Moscow for days. Once the protests and riots started to lower, the cyber-attacks emerged. For days, Russian-language web forums had lambasted Estonia for relocating the statue. Russian hackers conducted several DDoS attacks, defacements of websites (of several political websites such as the website of the Estonian Reform Party) and called for vengeance. The Russian websites advocated a strategy for destroying the e-systems that had become important in the government and business in Estonia. This cyber-war was deemed significant because it was performed in a highly sophisticated and intense way. At their peak, the botnets were bombarding Estonia's computer systems with one thousand times their normal rate of incoming e-mail traffic. The messages were coming from everywhere in the world, including China, Peru, the US and Egypt. This cyber-attack underlined the extent of the potential chaos and devastation that could happen when there is a failure to anticipate and prepare for cyber-attacks. This event launched a rise in awareness in several countries, delivering a wake-up call to individual governments and international organizations about the vulnerabilities of their vital infrastructure (Europe Institute, 2008).

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

meant for the enhancement of their cyber-defence capabilities as well as to counter disinformation. NATO recently even claimed cyber-defence is part of its core task of collective defence (NATO, 2017).

At this moment The US, China, Israel, Iran, North Korea, The UK and Russia are states in possession of cyber-defence capabilities (Breene, 2016; NATO, 2017; Royal Higher Institute For Defence, 2017). Surprisingly, when we look at a table published in 2015 on the website of the World Economic Forum we notice that the ten best prepared states against cyber-attacks are, except for the United States of America, none of the above mentioned states who possess cyber-defence capabilities. This shows again that there is an uncertainty existing around knowledge of cyber-security.

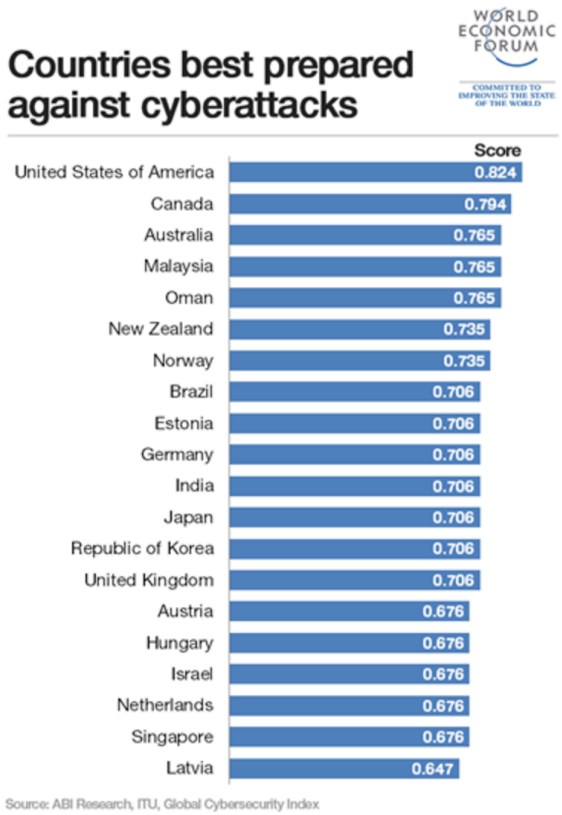

Table 1: countries best prepared against cyber-attacks (World Economic Forum, 2015)

It is clear that the number of cyber-attacks in the world is increasing over the

years (Kepes, 2016). However, it is very difficult to determine the exact number of attacks, the strength of the security and the impact of the defense capabilities. This is because most attacks are never reported and security and capability measurements are not openly shared. Recent studies and personal interviews have shown every state nowadays gets attacked repeatedly on a daily basis. Individuals or organizations often remain unaware that they have been attacked since the purpose of many cyber-attacks is precisely to hack unnoticeably into computers or systems. There is an increase in cyber threats because of the further and on-going digitalization of the worldwide societies and this also happens in vital sectors. The growth in existing devices and their mutual interconnection makes the world even more dependent on cyber technology. Consequently, society is more vulnerable against cyber threats. However we can also fortunately witness a worldwide increase of awareness that there is a need for investment in cyber-security and protection against these cyber threats.

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

4. The (spider) web of definitions

Given the complexity and the relatively new character of the cyber-world we deem it necessary to first explain some definitions concerning this topic.

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

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

What exactly can be described as a cyber-crime? A Cyber-crime can be described as a criminal activity, often very similar to traditional crimes such as identity theft. These crimes involve the use of networks or information systems, executed to vast number of potential victims in order to gain unauthorised access, damage and interfere in computer systems and obtain financial or other advantages ("Advisory Council on International Affairs," 2011; Broadhurst, 2006).

Before we go deeper into the definition of cybercrimes we firstly discuss *who* can conduct a cyber-crime. Political scientist Joseph Nye (2011) makes a rough estimation of who can be an actor in cyber-space. He divides the actors in cyber-

space into three categories: governments, organizations with highly structured networks, individuals and lightly structured networks. Thus, cyber-crimes can be conducted by practically anyone. We mostly refer to someone who has conducted a cyber-crime as a hacker. Cyber hacktivism is a form of activism where certain targets are attacked through hacking techniques. Hackers are persons who deliberately gain unauthorized access to computer systems. Cyber hacktivism is, in contrast to activism, a crime. Cyber hacktivism occurs in order to disrupt normal operations but is not meant to cause serious damage or harm. A hacker can work individually or in group. The most famous hacking group is Anonymous. This hackingroup, known for their Guy Fawkes masks used in the movie V for Vendetta, hacks every website or device that is a property of someone or something they don't agree with (Denning, 2001; Furnell & Warren, 1999; "Panorama," 2012).

The underlying reason of hacking is very often delivering a political message. Following example can clarify the political motive behind a hack. In the wake of the American election in 2017 former president of the US, Barack Obama, opened an investigation by US intelligence agencies to look into a possible influence campaign coming from the president of Russia, Vladimir Putin. According to these agencies Russia has hacked several websites from democratic parties and has given secret document to Wikileaks. This in order to influence the Russian and American public opinion and deform the general preference in favour of presidential candidate Donald Trump (SAGE, 2017; Sanger & Shane, 2016). This example shows how an actor conducts a cyber-crime in order to deliver a political message, or at least in order to influence a political choice.

Cybercrimes can exist in all forms and sizes. The scope of attacks can vary, stretching from hacking into a Facebook account of an ex boyfriend to conducting an intrusion of a nuclear device. In order to fully understand and imagine what the range of cyber-attacks consists of we will explain all the different types on the basis of a conceptual model made by strategic analyst at the Belgian Federal Police; Mrs. Delplace.

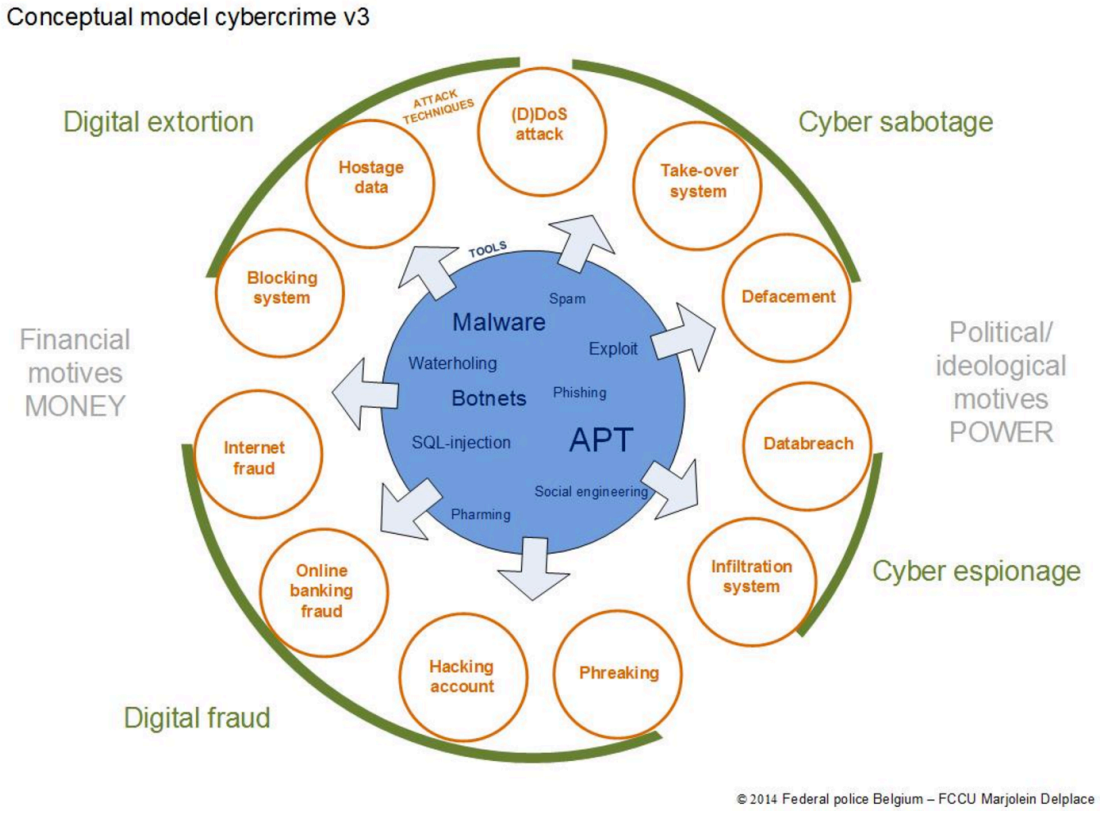

Figure 1: cyber-crimes (Delplace, 2014)

There are three different circles, namely the blue, brown and green one. The inner blue circle represents the tools, followed by the brown circle representing the techniques, ending with the green circle representing the goals. On both sides of the circle there are two motives to be found in light grey. All the following cyber-attacks can be conducted against anyone, this means individuals, companies, governments and critical infrastructure.

4.1. The tools

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

Malware, or malicious software, is the most known tool. The appearance of malware can be in form of viruses or worms. Another tool is APT, which stands for Advanced Persistent Threats. These types of threats are made to conduct a very deep intrusion. They stay as long as possible under the radar in a certain system, in order to collect data and information. Advanced forms of APTs can even adapt themselves to the cyber-environment, meaning that they can remain unnoticed for a longer period. Botnets are a collection of infected systems that work together to attack a certain device. They are distributed computer platforms that can function like computer robots. They use several types of malicious software programs, such as email viruses, and infect other devices with this infected software.

4.2. The goals and motives

The above-mentioned tools are the most important ones. With these tools you can proceed to organize an attack. These attacks are all conducted with a certain goal. We distinguish four goals: digital fraud, digital extortion, cyber-sabotage and cyber-espionage. Reaching one of the stated goals is stimulated by certain motives. We differentiate two different motives. The first motive is a financial motive, where the attackers' main motivation is money. Attacks driven by the first motive can have enormous outcomes. This can be proven by a recent cyber-attack, referred to as the Bangladesh Bank heist, during which about 100 million dollars was stolen by hackers through a sophisticated cyber-attack from the national bank of Bangladesh in 2016. Hackers breached the system of the bank and used the Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging network[2] to order the transfer from the bank account with the New York Federal Reserve. Until today the case has not been cracked. However, many are suspicious that help was given by North Korea. Although the main plotters of this heist have not been caught yet and neither is there any evidence found of money reaching North Korea, it remains an interesting case. This shows a potential shift to state-sponsored cyber-attacks with a financial motive. The fact that this cyber-attack could have been state-sponsored actually

[2] A messaging network for cross border payments (SWIFT Homepage).

makes the motive unclear. The underlying motive could be more politically-tinted. This brings us to the second motive (Farah, Shojol, Hassan, & Alam, 2016; Lema & Gopalakrishnan, 2017; "The investigation into the Bangladesh Bank heist continues," 2017).

The second motive for a cyber-attack is a political or ideological motive; here attackers' main motivation is to gain power. At the end of 2016 the capital of Ukraine's power grid was hit by a cyber-attack. This left the northern part of Kiev temporarily without electricity. Ukraine started an investigation to find the perpetrator of this attack. After tracking down the attack, the Ukrainian government found out it was linked to the Russian intelligence agencies, although it has never been completely confirmed. The investigation of the Ukrainian government unfolded two possible motives behind the attack. One was that Russia has conducted this attack to show off their power in order to prove to the people of Ukraine that the Ukrainian government is not able to fully protect them. The second possible motive was that there was something else happening at the same time and that Russia was in need of a cover-up to assist another operation to succeed (Polityuk, 2016) However, both motives are politically steered and not for the sake of earning money.
These motives behind cyber-attacks can be achieved by several attack techniques (middle brown circle). In the next section we will discuss these techniques. For reasons of space and relevance we will only address the majority of techniques and not all of them.

4.3. The Attack techniques

We start at the top left corner with digital extortion. The example explained will be hostage data or also called ransomware. Ransomware is computer software which uses a method of blackmailing. Certain viruses are installed on a computer; they block computer programs and take the computer as hostage. One can only free its computer by paying money (Benschop, 2017; De Bruycker, 2010; Marjz, 2006; "Ransomware," 2012). In most cases the user of a device

receives a message on his screen saying it has no access to its data any longer unless it pays a certain amount of money. Once the money is paid the device will be freed. Sometimes downloading an anti-virus programme on a USB stick followed by plugging this stick in the infected device can tackle this problem. But more recent and advances forms of malware, such as cryptoware, have the ability to encrypting all the files on a device. This means that all the files are locked and can't be used or touched anymore. Without a decryption key there is no possibility to unblock the system. The act of decrypting a virus is such a complicated and sophisticated act it can take up multiple years of work. For this reason even ICT experts can't solve the problem. Thus if a user hasn't backed up their files, they lose everything they have unless they pay money to the hackers. Asking ransom for files is an upcoming trend; only recently a hacker named The Dark Overlord stole the newest season of the popular Netflix-series Orange Is The New Black. This hacker uploaded the first episode of the season to an illegal file-sharing website. The normal release date was set out on the 9th of June 2017. The hacker demanded Netflix to pay a modest ransom for additional episodes not to be released. Netflix didn't concede and the season was effectively posted online (De Wolf, 2017).

An example of digital fraud is online banking fraud. Online banking fraud can be summarised as fraudulent online banking activities. These fraudulent activities are becoming more and more sophisticated, threatening the cyber-security and trust of online banking business. It has become a serious issue in the management for all banks of financial crime. The danger of these frauds is that it could affect customers worldwide, as well as other high profile websites and it can lead to massive losses (Wei, Li, Cao, Ou, & Chen, 2013). Only recently German hackers have exploited a vulnerability in a global telecom network called Signal System 7 (SS7). Several cyber-attackers exploit the Signal System 7 to steal funds from bank accounts. This system helps mobile networks across the world route calls and texts. This could be done by for example keeping calls connected as users drive on highroads, switching from signal tower to signal tower. It can also be used by hackers to redirect data and they have now found a way to intercept

the two-stage authentication codes sent out by banks. These codes are used to verify the identity of customers attempting to log into their accounts or to place online transactions. They are usually sent in the form of SMS messages and by intercepting these codes through the SS7 service, criminals can empty funds from bank accounts (Schwartz, 2017).

Given the focus of my research we will spend more time discussing the two next goals, which are cyber-sabotage and cyber-espionage. Cyber-espionage can be defined as the clandestine stealing of secret information on networks or information systems by governments or enterprises. This happens for own diplomatic, military or economic interests. Here we are confronted with a thin line between the definition of cyber-crime and cyber-espionage, and caution must be taken while using these concepts. The main difference in definition is that the goal of cyber-espionage is mostly not trying to disturb a computer system or network from the user's point of view. The best form of cyber-espionage is obviously the one a user never notices (Lin, 2010). An example of cyber-espionage is databreach. Databreach stands for breaking into a device and searching for data, followed by copying this data and leaking the gained information. A very famous example of data breach is the website WikiLeaks, created by Julian Assange. Mister Assange leaked several secret and classified documents from the Pentagon and the C.I.A. During a TED conference in 2010 Assange claimed the incentive for doing these controversial actions was trying to "show the world the real truth on several matters that were happening" (Assange, 2010).

The last goal to be found in the upper right corner is cyber-sabotage. The techniques used for cyber-sabotage come in various forms. On the one hand this can be a rather innocent attack such as defacement, which changes the main page, message or the title of a certain website in order to replace it by a personal (political) message. On the other hand this can be a risky attack, like the manipulation of a production process achieved by a take-over system. A take-over system means that hackers could take over an entire system by simply

sending an email or message to a device running the default malware protection software. The person receiving this email or message doesn't even have to open the email or any links because the damage is already done at that point. From that moment on the hacker can take over a system and manipulate it, by for example changing a certain process existing in that system (Kumar, Murphy, & Hisgen, 2004). So a hacker could get into the system of a train control and take it over, here hackers could change tracks of trains and create a collision.

We notice gaps in the outer circle of the model. On every border of these gaps there are techniques. These techniques are located between two goals because they can belong to either one of them, e.g. Internet Fraud can be conducted for digital fraud or digital extortion. Another example is (D)DoS-attack, standing in the middle of digital extortion and cyber-sabotage. Denial of Service attacks (DoS-attacks) is an attack that tries to disturb the normal operation of computer systems or networks. These kinds of attacks are quickly visible; so responding to them often happens very swiftly. Apart from the normal DoS-attacks, there are also distributed DoS-attacks (DDoS-attacks). With these attacks one device can infect multiple devices with an exponential speed. For these kinds of attacks hackers (or in this case botmasters) commonly use botnets. This form of attack is located in the middle of cyber-sabotage and digital extortion because on the one hand it can be done to paralyze a certain website, making it an outcome for cyber-sabotage. On the other hand, an attacker can also paralyze a website while asking money to let the website function again, and that makes it an outcome of digital extortion.

An important form of cyber-crime is not included in the conceptual model, namely cyber-terrorism. Cyber-terrorism is the convergence of cyber-space and terrorism. This is an act of terrorism carried out through the use of a computer. It is the attempt using cyber capabilities, the execution of unlawful attacks or threats in order to intimidate, coerce or seriously disrupt (parts of) society or a government in furtherance of political or social objectives. Cyber terrorists conduct acts with the aim of radicalising and recruiting new members but also

use this platform for financing purposes or sowing fear with videos, pictures or statements shared on the web ("Advisory Council on International Affairs," 2011; Coolsaet, 2016; O'Day, 2004). It is clear the motive of this cyber-crime can be placed under the political and ideological side. Cyber-terrorism has the gaining of power as a motive. This power means gaining influence, expanding groups and radicalising worldwide through the web. Within the conceptual model there is no distinctive form of goal yet for this type of cyber-crime. However, the increasing gathering and influencing of jihadi fighters through the web since the start of the war in Syria shows the growing importance of this type of cyber-crime (Rudner, 2017).

In case of being attacked by one of these crimes, the normal reflex as a state, institution or individual is protecting yourself against it. The protection against these attacks is called cyber-security. Cyber-security is a relatively new phenomenon that has rapidly become an important part in the daily life of politicians, policymakers, academics and the media. It used to be a reference to insecurities concerning networked computers in the 90's. Cyber-security came to the surface during the post-Cold War era. This is a response to the changing technologies and communication during that period. People started speaking of "The Electronic Pearl Harbor" and "weapons of mass disruption". States and politicians realised that protection or security of their technology, communication and everything that belonged to the cyber-world was deemed necessary to remain safe within their borders ("Advisory Council on International Affairs," 2011; De Bruycker, 2010; Hansen & Nissenbaum, 2009).

The thinking behind cyber-security has changed over the years. Technologies developing right now mostly focus on creating more and more possibilities, rather than investing in more security. The design of products is never secured, nor safe by design. Products are designed to be effective, efficient and appealing. Technology is dependent on open sources, connectivity and interdependence, enabling the possibility of exploitation. If a company brings out a new version of their device and wants to promote it to their customers, they will never use the

argument that they invested an astronomical amount of money in their new device for the sake of securing it one hundred percent. Rather, they want to invest an astronomical amount of money in making the new design more attractive, the battery longer and the operating system more accessible. The general argument in cyber-security used to be that airgapping3 is the best way of securing cyber and that this method was sufficient. However, this no longer applies to modern technology. The evolution in thinking went from 'the best security is a meter of thin air' to 'an air gapped system is just a delaying factor'. This evolution will continue and it shows that even the most secured and stand-alone systems can't be fully secured (personal interview, 2017).

Lastly we explain the concept of cyber-warfare. Cyber-warfare is literally a form of warfare occurring in cyber-space. It can be perceived as inter-state cyber-attacks. Kelsey (2008) described cyber-warfare as a phenomenon that can emerge in different grades, such as military operations that are meant to disrupt, mislead, modify or destroy an opponent's computer systems or networks by means of cyber capabilities to state-conducted attacks on critical infrastructure in an opponent's country. Key criteria in this definition are the presence of a military operation aimed at achieving a political or military advantage, the causing of damage to the opponent's cyber infrastructure and the use of cyber-capabilities. But this definition doesn't cover the complete contemporary form of cyber-warfare. A military operation is not necessary and not a given ("Advisory Council on International Affairs," 2011; Kelsey, 2008; Tsagourias & Buchan, 2015). Cyber-warfare can be amalgamated with hybrid warfare and information warfare, but technically they can be described separately. In 1999 NATO released a report that defined the term of information warfare: information warfare could be defined as defensive and offensive operations, conducted by individuals or structured organisations with specific political and strategic goals, for the exploitation, disruption or destruction of data contained in computers or transmitted over the Internet and other networked information systems (NATO,

[3] Airgap is a network security measure. This measure disconnects a network from any other network. It can only get in contact with extern devices, such as an USB-stick.

1999). Hybrid warfare is described as a mix of regular and irregular warfare, a mix of conventional and unconventional warfare. Cyber-space can lend itself perfectly to hybrid warfare because it is not always clear if cyber actions can be perceived as deeds of war (Wilkie, 2009). It is clear that the lines are blurred between these three forms of warfare.

After this comprehensive explanation of all the concepts in the cyber field we will now continue to the second part of this paper. We start by discussing how cyber fits as an instrument of foreign policy.

5. Cyber-warfare as an instrument of foreign policy

5.1. The study of policy instruments

In the Seventies the study of policy instruments emerged. A policy instrument knows different definitions, showing the complexity of this study. It mostly comes down to means of government intervention in markets or society in order to accomplish certain goals or to solve certain problems. Or as author Vedung (2011, p. 21) describes: *policy instruments are a set of techniques by which governmental authorities wield their power in attempting to ensure support and effect or prevent social change (…). For policymakers it is crucial to have a good overview of the generic form of these instruments, because the issue of choosing the appropriate combination is one of the most intricate and important in strategic political planning*. Policy instruments on the one hand affect both agenda setting and policy formulation processes. On the other hand they function as subject of decision-making policy implementation.

The work of Van Nispen (2008) pointed out three approaches that developed throughout the history of studies of policy instruments. First there was the classical instrumental approach. This approach was used from 1970 until 1985. This approach was mainly discredited because of its top-down and mechanical view of the world. This approach claimed the selection and the application of instruments are done on the basis of the characteristics of a specific instrument and its effects in terms of goal-attainment. This approach suffered from a pitfall: there is no connection between the characteristics of instruments and the effects an instrument can bring to reach a goal. This approach also didn't take the characteristics of the political context into account.

Learning from their flaws, the Instrumentalist School of Thought developed its second approach (1985 – 1995). As the name of the approach, namely the instrument-context approach already suggests, this approach does focuses on the context. Apart from that, this approach focused on developing a theory of policy instruments that would enable policy makers to select the appropriate policy instrument for the problem at hand. This selection was done on the basis

of the 'logic of consequence', and on the 'logic of appropriateness'.

Later on, a third approached advanced: refined instrumentalism. Instruments are now considered one of the many variables in the contextual approach that takes policy implementation as a starting point. Hereby merges the study of policy instruments with the study of implementation.

5.2. Preferences in policy instruments

A government's decision on what policy instruments they will use in their (foreign) policy is going to be based on facts but also inevitably on values and beliefs. These values and beliefs will influence the ways in which governments will gather and interpret information. Consequently it will influence the way a policy looks like and what instruments are used to give to indicate and prioritize certain aspects of a policy. Therefore it is impossible to create a complete and consistent list of policymaker preferences. Above that is its impossible to gather all relevant information about a policy problem or anticipate the effects of a solution. Often decisions on what policy instruments will be implemented or invested in are based on a long-term goal. Analyzing if the effect of this decision came with a positive outcome can only be done after an amount of time passed by. And in case of negative outcome governments often seek ways to gather a sufficient amount of information to justify their decisions (Cairney, 2013).

5.3. The policy cycle applied to Belgium

We will now follow the figure by Cairney (2013) which represents a policy cycle. This cycle shows how decisions on policy instruments of policymakers are influenced by own preferences and how this mostly follows a range of stages. During our research work we conducted several interviews. These interviews were performed in Belgium with Belgian individuals and Belgian institutions. To clarify Cairney's policy cycle we will thus use Belgium as a case example.

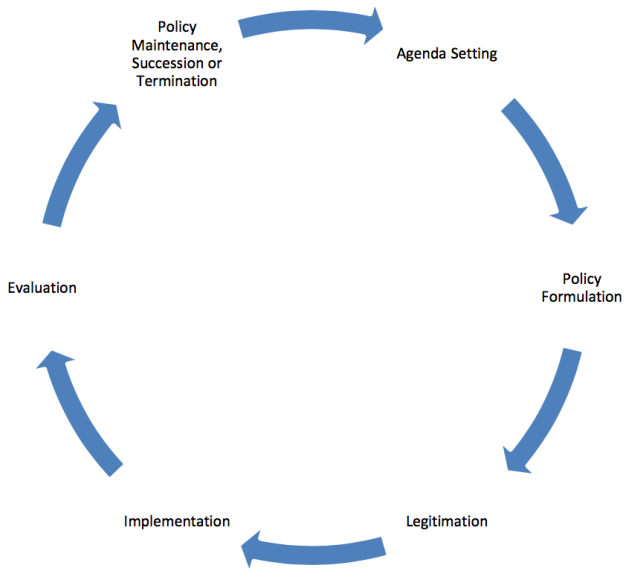

Figure 2: the policy cycle (Cairney, 2013)

First, we start at agenda setting. This stands for identifying problems that require attention from a government. In this phase governments decide what issues deserve most of the attention and they also define what the exact problem is. Here preferences already come to the surface. Out of multiple interviews we performed, we discovered cyber-security is something standing high on the political agenda and that it is a subject of much discussion. It is an important goal of Belgium to keep up with all the other European countries and invest extensively in cyber.

Second is the policy formulation. This means setting objectives, identifying the cost and estimating the effect of solutions, choosing from a list of solutions and selecting policy instruments. Since the latest national government (The Michel government 2014) Belgium has intensively invested in cyber-security. Apart from the already existing Federal Computer Crime Unit and other regional Computer Crime Units, Belgium has since 2015 a Cyber-security Centre and since 2017 a cyber emergency plan. These organizations work together with the government and from this cooperation they set out different objectives, solutions and other instruments (Bové, 2017; De Redactie, 2015).

Thirdly: the legitimations. Here the governments need to make sure the chosen

policy instruments carry support. It can involve one or a combination of: legislative approval, executive approval, seeking consent through consultation with interest groups, and referenda.

The cycle is followed by the fourth step, namely implementation. Here an organization is established or employed for taking up responsibility for implementation. The government ensures that the organization has the resources to bring this job to a proper end and making sure that policy decisions are carried out as planned. As mentioned before, the Belgian government works together with several state and non-state actors to implement and control cyber-security measurement. This all applies to internal affairs. When it comes to foreign affairs the Cabinet of Defence has implemented cyber-space as a fourth defence domain for the Belgian military (apart from land, sea and air) and hired twenty-five people in 2015 to strengthen this new domain (Lemmens, 2015; Paelinck, 2015). Above that the Belgian government also focused on investing in cyber diplomacy. Currently there is one Belgian ambassador appointed for cyber diplomacy. Belgium works together with European institutions such as the European commission and international organizations such as NATO. These organizations set out rules or create measurements that should be implemented by the Belgian government (personal interview, 2017).

Fifth: evaluation. After implementation there has to be an execution of an analyse to which extent the policy was successful or the policy decision was the correct one. Lastly there is the policy maintenance, succession or termination. This stands for the consideration whether the policy should be continued, modified or discontinued. It is clear Belgium is making considerable efforts in intensifying their cyber policy. Weekly the government can receive interpellation from members of the parliament concerning this topic. Because this government is still running until 2018 a final evaluation of the established cyber policy cannot be done yet.

Given the constant evolution of the Internet and the exponential intertwined network of devices worldwide there is an increased input in cyber as an

instrument of foreign policy. Countries receive cyber threats on a daily basis so there is an increasing awareness of cyber threats and recent studies showed this is generally considered as an important, and still increasing risk in international security.

Even though there is an increase in awareness of the risks existing, it remains an unknown and abstract policy to normal society. When policies are processed out of the public spotlight it means high attention to this matter is not desired (Cairney, 2017). This gives the opportunity to conduct a policy only accessible for a privileged world of experts. If we consider the imperviousness of this we can assume cyber policies carry important, dangerous or controversial outcomes. This could also explain why there is few open communication and a vast amount of controversy surrounding cyber policies (especially when it comes down to cyber defense policies) of state and non-state actors.

6. Case study: the Stuxnet-virus

Fears existing around cyber-warfare can be clarified with concerns over potential attacks on digital industrial control systems, or as mentioned before: critical infrastructure. These systems run electric power grids, power plants, water plants and several other physical facilities. When one of these critical infrastructures is attacked by cyber-attackers, the possibility of physical harm is real.

Caution must be taken when making this analysis because conducting such an attack is far from easy, nor self-evident. These attacks carry a high cost and the creation of it is more sophisticated than at first glance. As Slayton (2017) argues, not only does planning an attack of this size take a lot of skill, it also requires knowledge of the physical processes and systems that are targeted. The latter stands in need of information not readily available in computers. Additional to the information technology needed for these attacks, process and automation talent is necessary as well. The attacker will most likely not be able to deploy the cyber-weapon immediately before wanting to use it; triggering it at a specific time requires persistence of communications. Exploiting physical damage through cyber operations is more difficult and costly than simply gathering, distorting or denying access to information. However, there is still considerable amount of disagreement for this analyze. Although attention should be given to arguments in this analyze, the following example will clarify the shortcomings.

In 2010 a sophisticated type of malware, named Stuxnet, emerged and infected several systems. The most controversial attack conducted by this worm was the infiltration of the Iranian nuclear facility in Natanz. This computer programme was created to penetrate several crucial systems and gain control over them. The Stuxnet worm used zero-days vulnerabilities. Zero days vulnerabilities stand for vulnerabilities that were previously unknown. This makes them easy targets because there is no time (literally zero days) to develop and distribute patches. The functioning of this virus happened three-ways.

First, it analysed and targeted Windows networks and computer systems. Once infiltrated in these machines, it continuously replicated itself. Second, the machine infiltrated in the Windows-based Siemens Step7 software[4]. Lastly, by compromising the Step7 software, the worm gained access to the industrial program logic controllers. This final step gave the worm's creators access to crucial industrial information. Additionally it gave them the ability to operate in several devices located in the individual industrial sites. The Stuxnet-virus targeted systems that were airgapped. Meaning these systems were not connected to the public Internet. The only way this virus could penetrate a system was with the help of an intermediary device, such as an USB stick. And, simple as it sounds, this eventually happened in the nuclear devices in Iran. Over fifteen facilities were attacked and penetrated by the Stuxnet worm. In 2012 former president of the US, Barack Obama, admitted working together with Israel on the development of cyber-weapons. The given explanation by the American government for their attack was that they collaborated to retarding the Iran's nuclear programme (Farwell & Rohozinski, 2011; Gibney, 2016; Holloway, 2015; Sanger, 2012).

The importance of this example lays in the evolution of computer warfare. Despite the swiftly and effective disarmament of the virus and the physical harm of the attack that was limited to covertly disabling Iranian centrifuges, this cyber-attacked revealed several fundamental questions. The attack had the capability of starting a war and can be perceived as possible cyber-warfare. There was no on-going armed conflict, which means the US executed an attack in peacetime. The Iranian infrastructures could have been physically damaged. The consequences could even go further than this. When we anticipate on a cyber counter attack, the outcomes are endless. Iran could attack United States' installations and troops in surrounding countries such as Iraq. It could have disrupted the flow of oil out of the Gulf region, with escalating oil prices as aftereffect. The international community could have gotten involved,

[4] The Siemens Software system is prevalent in industrial computing networks. They manage industrial plants.

accelerating and sophisticating this conflict. This event has definitely given incentives to countries to arm themselves more against these attacks and invest in cyber capabilities, whether offensive or defensive. Later, in 2012, a virus called Shamoon struck Saudi Aramco[5]. Around 30 000 computers functioning in this company were infected by the virus. This Saudi company is the largest oil company and stands responsible for ten percent of the global supply. An attack on this company is therefore a significant intrusion. There are many speculations this attack was conducted by Iran in retaliation of the Stuxnet attack they were confronted with two years earlier (Finkle, 2016). This backlash confirms the possibility of a back and forth conflict with potential disastrous outcomes. This back and forth conflict that started via a cyber-manner could evolve into a conventional war. The disastrous outcomes go from destroyed infrastructures and economic losses to physical victims.

[5] Saudi Aramco is a Saudi Arabian oil company. The company produces national petroleum. Apart from that it manufactures, markets and refines crude oil, natural gas, and petroleum products.

7. Why choose cyber-warfare over conventional warfare?

If we pose the question of whether cyber is becoming a new instrument in foreign policy and a potential precedent to a cyber-warfare, we firstly have to ask ourselves why an actor would prefer a cyber-war fare over a conventional warfare. Using the Internet as a medium for solving conflicts is a considerable fact given the advantages it brings: it does not effectively provide legal rules or law, it is marked by an absence of policing or a specific protocol, it can bypass national laws and many more reasons. We will now go into the different reasons why cyber-warfare is preferred over conventional warfare.

7.1. The success of small countries

Using cyber-weapons gives an opportunity for smaller countries to attack bigger ones. Big powers are even more dependent on their critical infrastructure, so attacking infrastructure from such a power can be done by small powers. For example, for the US the stakes are high, as the country's technological sophistication makes it uniquely vulnerable to attack (Parker, 2017). This can be perceived as an asymmetric vulnerability to such warfare (Clarke & Knake, 2011). Here, the classic superiority characterizing conventional warfare is not applicable in cyber-warfare (we will go deeper into this infra 'can cyber change the international power balance?'). There is also a possibility, not an allowance, to attack during peacetime. For all these reasons smaller countries can be more attracted to cyber-warfare. This argument can be countered with the fact that super powers can invest more in cyber capabilities, thus protecting themselves better against attacks and conducting greater attacks (Infosec Institute, 2016).

7.2. The question of legality

Laws governing material on the Internet are not clear and often very complicated defined. It is important for governments to guarantee their citizens a form of freedom when it comes to the usage of the Internet and at the same time guarantee protection of national security and the individual (Crilley, 2001).

Cyber-warfare is a form of warfare that is not explicitly addressed by existing international law. Because there is a lack in rules and law for cybercrimes and cyber-warfare in general, this makes the cyber-domain a very difficult domain to control.

The first attempt of regulating cybercrimes happened in 2003 during the Budapest Convention. This is the first, and at this moment the only, international treaty that tries to address cybercrime. The goal was harmonizing a spider web of national laws and policies on cybercrime across several nations. Its main objective was pursuing a common criminal policy aimed at the protection of society against cybercrime. With around 50 signatories it is the biggest and only legally binding instrument concerning cyber-crime. It has proven significant but can't be perceived as a global instrument (Renard, 2014). At this moment, the treaty has still not been ratified by every party.

As a response to the Russian Georgia War that occurred in 2008, the NATO Cooperative Cyber Defence Centre of Excellence published a paper that discusses the possible application of the Law of Arms Conflict to cyber-attacks.

In 2009 there was a second effort to create some regulation on cybercrime. A cyber-security expert group created the Tallinn Manual, a non-binding study on how international law could be applied to cyber-warfare. Even though this manual included 95 rules of international law, states were slow to take a stand. This was presumably out of concern that doing so might limit their freedom of action in cyber-space (Magee, 2017; mostofa, 2017; Roscini & Trust, 2014; 2015).

In April 2010 a UN Crime Congress was held in Salvador, Brazil. The conference was completed by the Salvador Declaration. The draft of this Declaration included a call for negotiation of a new United Nations treaty on cybercrime. The discussing parties agreed upon the necessity of setting up an Open-ended Intergovernmental Expert Group to conduct research on this new treaty

(UNODC, 2010) This congress was followed by a UN Crime Congress in Doha, Qatar in 2015. This congress was meant to bring governments, policy-makers and experts together for an exchange of their experiences in crime and intensify international cooperation in tackling the threat of transnational organized crime, including cybercrime. Although the expectation for this convention would be discussing new international instruments to combat cybercrime, reluctance for this already came to the surface during the preparations for this convention. The Cybercrime Convention Committee (T-CY) of the Council of Europe discouraged all the signatories of the Budapest convention to develop new international instruments for the fight against cyber-crime, both conventions as new forms of soft law. According to the T-CY this convention should be held to discuss the possibility of capacity building, rather than investing in new instruments. Reaching international consensus on this topic is too complicated and, according to the T-CY, would only result in more division. Therefore the Council of Europe discouraged all the signatories of the Budapest convention to develop new international instruments and they perceived this solution as the best option. The General Assembly also recommends the Budapest Convention as the benchmark concerning cyber-crime. Lastly, a new treaty would cost more than the profit it would grant (personal interview, 2017).

In 2015 the General Assembly adopted the resolution 70/237 (UN, 2015) which encourages multilateral agreements on possible threats coming from the field of information security. In the cyber defence part of the NATO-website the organisation has affirmed that international law applies in cyber-space. However this remains a vague and unexplained part of their policy (NATO, 2017). These two last efforts were the last movements in the creation of international law concerning cybercrimes.

It is clear that although bringing this topic to the surface is a slowly rising trend, most parties or institutions fail in addressing this issue properly. Magee (2017) correctly proposes the question of creating a Geneva Convention for cyber-warfare. The president and chief legal officer of Microsoft, Brad Smith, took a leading role in the creation of such a Convention. On February 14th 2017 mister

Smith did the proposal on the Microsoft website for the creation of a Digital Geneva Convention. Although this has not been elaborated yet, it remains an interesting initiative (Smith, 2017). Fundamental questions rise while considering this Convention. Firstly: are we in need of this Convention and secondly: does it carry any added value to the Geneva Convention? Creating new rules, specifically applicable in cyber-space, might collide with the existing rules in the Geneva Convention and this creates a dangerous imbalance. Imagine the new rules of the Digital Geneva Convention enable the legality of certain criminalities that are not legal in the normal world. This could become a bypass to undermine rules already existing in the normal world. The Geneva Convention says it is not allowed to target civilians; this includes targeting critical infrastructure because it indirectly hurts civilians. But what if the new rules incorporated in the Digital Geneva Convention do not explicitly describe them in the same way, they can have different outcomes. Consequently critical infrastructure might be targeted with the rules of the Digital Geneva Convention in mind. It is also important to bear in mind that states might consider putting their cyber-weapons down, but there is not one state that wants to go first at doing this. When talking about an international convention or regime, no one is confident that this couldn't be twisted against them (Hayward, 2015). However, this remains a topic for open debate.

Given the limitation and shortcoming in jurisdiction concerning cybercrimes and cyber-warfare, this naturally carries an appealing effect to committing crimes in this field. Because a cyber-criminal could perform a cyber-attack without having fear of being caught and being prosecuted for their criminal deed.

7.3. The question of cyber-weapons

The problems emerging when proposing the question if a cyber-weapon can be equated to a conventional weapon can be outlined with a brief analyse of the United Nations Charter. Article 2.4. of the United Nations Charter ("Chapter I | United Nations," 1945) 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". Later in the charter the United Nations clarifies in article 41 and 46 the meaning of an armed force. "*The Security Council may decide what measurement not involving the use of armed force are to be employed to give effect to its decisions (…). These may include 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. Plans for the application of armed force shall be made by the Security Council with the assistance of the Military Staff Committee"*. Furthermore article 51 of the Charter confirms that member states have the right of collective or individual self-defence if they find themselves victim of an armed attack ("Chapter VII | United Nations," 1945).

On the one hand this gives the formal solution that cyber-weapons are not literally included in the Charter. The vagueness and width of these articles, on the other hand, give no reason to exclude the suggestion that a digital attack on a system could not count as an armed attack. Above that, there is no certainty to exclude certain weapons from international law.

The definition of a weapon given by Rid and McBurney (2012), namely: *a tool that is used, or designed to be used, with the aims of threatening or causing physical, functional, or mental harm to structures, systems or living things*, confirms the assumption that cyber-weapons can be equated to conventional weapons. However, this conclusion should be read with caution because the nature of cyber is clearly still open for debate.

The creation of cyber-weapons can occur very quickly, but the deployment of these weapons is a long, expensive and intensive process. This also requires a massive amount of skill how to decently use them in a sustainable way. Cyber-weapons know considerably more variety than conventional munitions, since there are many ways computers and networks can be disabled. This means that acquiring cyber-weapons and knowing their use is considerably harder than

acquiring other kinds of weapons and knowing their use. However, the balance between advantages and disadvantages of cyber and conventional weapons are not an even keel; cyber-weapons remain more attractive then conventional weapons (Herr, 2013).

Overall, the development and deployment carries a lower cost than development and deployment in a conventional war. The visibility of the development of cyber-weapons and cyber mobilization is barely present. One can be occupied by developing a cyber-weapon for years in the most invisible or unnoticeable way. Preparing and transporting army troops and arms for a certain conflict carries higher costs and visibility.

7.4. The question of a cyber counter attack

Kelsey (2008) argues that violations of the distinction[6] and the neutrality principles[7] of International Humanitarian Law are more likely to occur in cyber-warfare than in conventional warfare. During cyber-warfare there is often no physical harm brought to civilians, nor damage of civilian objects. This makes it appealing for states to invest in cyber-weapons in case of a cyber-warfare so they would have weapons to conduct a cyber counter attack. If we look at the spectrum of possible cyber-attacks under International Humanitarian Law, the principle of distinction would on the one side of the spectrum give a state the permission to attack a purely military target. Because a distinction between civilians or civilian objects and military targets has been made. On the other side of the spectrum the principle of distinction wouldn't allow a cyber-attack affecting civilians or civilian objects. Thus it is very difficult to draw a line between a legal cyber-attack and an illegal one. It is important to bear in mind

[6] The principle of distinction is a basic principle in International Humanitarian Law. This principle governs the use of force in an armed conflict where belligerents have the duty to make a distinction between combatants and civilians. This principle grants the minimum loss of civilians and damage to civilians during armed conflicts or military operations (Kasher, 2007).

[7] The principle of distinction is a basic principle in International Humanitarian Law. This principle ensures respect for neutral space. Armed forces involved in the conflict do not enter neutral space and that neutral States are not affected by the collateral effects of hostilities (ICRC, 2010).

that although an attack conducted without the harming of civilians or civilian objects, does not mean an attack couldn't do this in the future. Outcomes of cyber-attacks can sometimes only by felt on a longer-term. The fact that flight networks, agriculture crops, nuclear devices, emergency networks, and so on, can be attacked, creates possible harms for civilians or civilian objects, whether visible in the short or the long-term. Because states can attack other states through cyber-warfare without incurring the political cost that comes with civilian casualties, they are more likely to use cyber-warfare as a method rather than using conventional methods.

When we look at the neutrality principle we once again find an absence of clear International Law. When interfering in cyber-warfare a belligerent uses the international structure of the Internet. Which is a free and hardly controlled network. When a cyber-attack occurs, cyber-weapons are transmitted through the territory of a neutral state. The Hague Convention has forbidden the movement of weapons, even weapons the size of an electron, across the territory of a neutral State. So this makes cyber-warfare an illegal practice. But because of the lack of accountability an atmosphere of impunity is created, it gives states the incentive to engage in prohibited cyber-attacks. Thus, we can conclude that implementing cyber-attacks and starting a cyber-war allows states to inflict damage without carrying the burden associated with conventional warfare and, above that, guaranteeing states a rapidly achieving victory (Kelsey, 2008).

In the analysis of ethics of warfare Dipert (2010) calls this the "ontological" problem of cyber-warfare. Even though physical entities aren't killed or harmed, the quantity of intentional harm may nevertheless fall within consequentialist or other thresholds for acts of war that morally permit counterattack. More than that, it can in some cases even justify a conventional counterattack.

7.5. The question of attribution

One of the most appealing reasons to initiate a cyber-war instead of a conventional war is the problem of attribution. As mentioned before, cyber-warfare is a difficult form of warfare because of its uncontrollable character. If

one plans a cyber-attack on another country they can locate themselves on a device, anywhere in the world. This also declares why it is never possible to give a state, institution or individual full responsibility for a certain cyber-attack. Finding a perpetrator in these wars are only possible by means of probability. This carries the danger of never enabling a settlement to a conflict.

The explanation of Rowe (Green, 2015) explains why the attribution of cyber-warfare is well-founded and helpful. Cyber-weapons are not geographically restricted. The attacker can be miles away from the victim, making it even more appealing to commit an attack because there is less mental reluctance to hurt someone. Cyber-attacks are granted with the absence of persistent traces. Evidence like fingerprints is not applicable in these cases. Above that, it is easy to conceal cyber-weapons because they can't be physically seen. Getting access to cyber-weapons is also a convenient action. Cyber-weapons can be implemented with delayed effects after installing them. Therefore an attacker can practically choose when and how it will act. The link between cause and effect of a cyber-weapon is therefore rather blurry.

The problem of attribution can be can be demonstrated by a recent example: the cyber-attack executed on the Lithuania's parliamentary website in 2016. This website was taken offline just as a discussion panel was set up to discuss the human rights situations in Crimea. The police forces claimed the attack came from abroad. This happened because the Lithuanian parliament passed a law outlawing the use of Soviet and communist symbols. More than 300 websites were attacked. Some websites were completely brought offline while other websites were spammed with the Soviet hammer and sickle. On the one hand there was proof of Russian spyware found in the Lithuanian government computers, but on the other hand there is no conclusive evidence that the Russian government executed the attacks. Therefore this case was never given fully responsibility to any party (Ashmore, 2009; Euronews, 2016; Sytas, 2016).

Apart from the fact that attribution is an exponential problem in cyber-warfare, that doesn't mean this problem does not occur in conventional warfare. When in 2014 the passenger flight MH17 going from the Netherlands to Malaysia crashed while traveling over conflict-hit Ukraine, the problem of attribution immediately appeared. Even though the main assumptions go to Russia as perpetrator of the shooting down, this can never be said with one hundred percent certainty (BBC, 2016).

8. The comparison between a conventional war and a cyber-war

Can a conventional war be compared to a cyber-war? This is a crucial question in warfare studies. There is an overlap existing between both wars when we analyse the fundamental elements that construct a war: conflicting actors, weapons and victims. There are also motives and goals involved. Of course there are differences as well (see supra 'why prefer cyber-warfare over conventional warfare). In the literature there exists a regularly made comparison between the Cold War era and a potential cyber-war era now. This is because of the many similarities emerging when comparing a nuclear war and a cyber-war.

Firstly there is the atmosphere of conflicting actors building up cyber capacities in order to being able to conduct a cyber counter attack, once being attacked. This phenomenon was also visible during the Cold War; only during that war countries build up nuclear capacities. Secondly there exists an uncertainty and vagueness around the capabilities one country has, how much they invest in it and what outcomes they can create. Thirdly, we notice a similar power balance between countries who are known for having cyber capabilities now and those who had nuclear weapons during the Cold War. Thus the power balance hasn't changed. Lastly, there are discussions on the possibility of a non-proliferation for cyber-weapons (Arimatsu, 2012; Liff, 2012). This clearly shows a similarity to the Non-Proliferation Treaty of 1968 that was made up during the Cold War. However, there are some disagreements existing with this comparison. Cyber-weapons carry fundamental characteristic differences to nuclear weapons. The Mutual Assured Destruction during the Cold War only happened because there was parity existing under the weapons one country had. It's not a difficulty to count the amount of missiles a state had. But how do you measure the amount of cyber-weapons a state has? How do you measure existing cyber capacities? Above that there is an important difference in the expiration date of a nuclear weapon and a cyber-weapon. When using a nuclear weapon, it's immediately perished, but a cyber-weapon knows an infinite existence. More over, cyber-weapons can be created again. If an attacked state reveals that its infrastructure was victim of a virus attack, then that state, by the time of its announcement,

most probably has the knowledge and expertise to eliminate, copy and reverse the engineering of the virus. Consequently this allows the attacked state to re-use it again themselves. When discussing a nuclear war there exists a moral hazard. This dimension barely exists in a cyber-war because of the attribution problem. Additionally, There is the complication of availability. During the Cold War there was no excessive availability of nuclear weapons. The price and effort needed for the development and maintenance of these weapons is prohibitively high. Buying a cyber-weapon is already possible for twenty-five euros on the Internet. The cyber-era is much more obscure than the era of the Cold War. It's difficult to trace attackers quickly and reliably, increasing the chances that the targeted country will make an error. Lastly, The public understands cyber threats far less well than it does the threat of nuclear weapons. This is because much of the information is classified and inhibiting public discussion (Kaplan, 2016; Van der Meer, 2015).

Therefore, a more plausible comparison would be between a biological weapon and a cyber-weapon. Biological weapons and cyber-weapons share the difficulty of attribution, a higher availability, the lower moral hazard and the (almost) infinite existence (personal interview, 2017).

9. Can cyber change the international power balance?

Because there are problems existing in cyber-space, such as the problem of attribution, smaller countries could perceive this space as a place where they could increase and enforce their power in international relations. On the other hand, bigger countries still have more sources to invest in cyber capabilities and will have a lower level of reluctance for conducting a counter attack. So even though there might be reasons why a small state would prefer engaging in a cyber-war over a conventional war, the existing power balance between smaller and bigger states is still present in cyber-space.

When the Sony movie The Interview was about to premiere in 2014, a cyber hack attacked Sony Pictures Entertainment. Private information of employees and the company itself, such as salaries, were spread over the web. Every speculation attributed the perpetrator of this hack to North Korea. The content of the above-mentioned movie mainly involved criticism on the North Korean regime. A North Korean foreign ministry spokesman even called the movie an act of terrorism. As a reaction multiple cinemas cancelled the movie, the official release date was postponed and Sony lost about 15 million euros to this hack. The US government decided to impose heavy sanctions on North Korea by barring already limited further commercial engagements and further economic sanctions (Haggard & Lindsay, 2015; Roberts, 2015). This conflict shows that even in cyber-space attacks are conducted with political motives, between known rivalry states and is answered with significant sanctions. The classic hostilities existing in international relations thus apply in cyber-space as well.

Throughout this research and during the conducted interviews we discovered this power balance doesn't only apply to the division of small and big countries but also to the division between 'the Free' and the 'non Free World'. Before embarking upon this topic, we feel the need to firstly describe this controversial division, because what exactly is the Free World? Cambridge dictionary describes the Free World as follows: *those countries whose governments have been chosen in fair elections and whose people have full human rights, usually used*

to refer to the Western world, in contrast to other countries, for example countries that have a communist government (Cambridge English Dictionary). The concept of 'Free World' developed during the Cold War. The term was firstly used by the US to enlighten the freedoms existing in their country, in comparison to the lack of freedom existing in communist countries. Because freedom was such an important concept during the Cold War, it became a widely used concept. Present day, the Free World often refers to the non-communist countries, as formerly opposed to the Soviet Bloc. The Free world often stands for the democratic West. And the non Free World stands for the communist East (Fousek, 2000; Wills, 1999). It is clear that the concept of a Free World and a non Free World is an out-dated concept. Although it was often used as reference during the conducted interviews we prefer to refer to Eastern and Western countries.

This distinction between the West and the East also appears in the cyber-world. The West lives in a free cyber-space without cyber boundaries; there are no restrictions on the freedom to access the Internet. In comparison to countries where there exists a severe restriction on the freedom of the Internet and where there is a censorship of things appearing on the Internet. The most known example of this is The Great Firewall of China. This wall was part of China's censorship and surveillance project, called the Golden Shield Project. In 2017 president Xi Jinping fortified The Great Firewall by capsizing the use of VPN connection[8] (Pham, 2017).

There are fundamental differences in the thinking between world powers from the West, such as the US and France, and world powers from the East, such as Russia and China. This is reflected in cyber areas as well. When country XXX gets attacked in cyber-space there will be a different counter attack conducted,

[8] A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. This network enables sending data between two computers across a shared or public internetwork (Microsoft, 2001).

depending on whether the attacked country is one located in the East or one located in the West. If country XXX is located in the East there is a more likelihood of that country conducting a counter attack in any given form and as swiftly as possible. Whereas, Western countries are more likely to negotiate or invest in diplomatic solutions, rather than preparing an immediate counter attack (personal interview, 2017).

The only, and a rather far-fetched, way of stopping a potential cyber-war is limiting the free open Internet, where everyone can be anonymous and express their selves or do anything they want. This infringes upon a cornerstone of democracy; where freedom of speech is granted. Limiting the use of cyber in the West is not an obvious given and will bump into huge waves of protest. This also applies when we look at the difference in efforts for cyber regulations. Countries of the East are more occupied by regulating the Open Internet, while the regulation of cyber in the West is an extremely difficult, controversial and sophisticated action. It all depends upon how a country reacts to another country. And this reaction is stimulated by political standpoints and based on a state's own principles. Information is something the West perceives as a strength, in comparison to the East where Information is seen as a danger and exploited as weapon for manipulation (personal interview, 2017).

As an example for this we look at the US - Chinese relationship. This relationship constitutes a country from the West (The US) and one from the East (China). This relationship suffers from fundamental disagreements. US policymakers believe it's acceptable to spy for political, commercial and military purposes. This is fundamentally different in comparison to the believes of China, where theft of intellectual property crosses that line. On the other hand, The United States might spy on companies and trade negotiators, but it does so to protect its national interests, not to benefit specific US companies. Here again we find a difference with the believes of Chinese because they don't see this distinction (Parker, 2017). China doesn't see a difference between public and private actors. Chinese firms are part of an effort to modernize the country and build comprehensive power, no matter whether they are private or state owned. They

believe stealing for their benefit is for the benefit of the nation (Segal, 2016). China also takes a different approach than the US when it comes to privacy and communication rights. Throughout the Chinese development of China's cyber policy these privacy and communication rights have not played a dominant role. China emphasizes the importance of cyber sovereignty. President Xi keeps advocating for China's continued ability to limit its citizens' access to the Internet, and consequently reduce the role of the U.S. in Internet operations and rule setting in China's Internet operations (Diplomat, 2017).

In 2015 Russia and the US tried to sign an agreement on measurements of trust in cyber-space. After the Ukraine crisis in 2015 the relationship between Russia and the US reached a low point. This bilateral agreement was never concluded. Meanwhile Russia and China have signed an agreement where they agreed not to launch any cyber-attack against each other. Furthermore they agreed to share cyber-warfare and cyber-defence technology. It is clear this creates an Asian axis of power. China and The US made a bilateral agreement as well on cyber-security but because of their fundamental differences in conceptualising cyber-issues, this agreement was critically received. On the Western side of the geopolitical spectrum the American National Security Agency (NSA) and British Government Communications Headquarters (GCHQ) share signals intelligence. The classic split between the West and the East, with Europe in between, is rendered transparent (Diplomat, 2017; Gewirtz, 2015; Worldcrunch, 2014).

We can conclude the power balance existing between the more democratic West and the more authoritarian East also applies in cyber-space. How this will further develop remains open for debate (personal interview, 2017).

10. Three schools of thought concerning cyber-warfare

10.1. The impossibility of cyber-warfare

The first stream of thought concerning cyber-warfare believes that cyber-warfare will not take place; therefore it is not a phenomenon we would have to fear. Some critical scholars signify that the cyber threat is merely a phantasm. This because of the overestimation of what danger cyber can bring along. Additionally, they believe that the related technology involved in cyber-warfare does not alter the character or means of war. Cyber-space will become more sophisticated, unattainable and secured and this will impede further major attacks. The assumption of a rising trend in attacks such as the example of Stuxnet is exaggerated. A conquest of the global network is not as big a threat as some believe or some assume because of the incredible difficulty of taking control over information systems owned by others, corrupting their data, and in the most extreme cases shutting those systems down. (Libicki, 2007).

The most famous article on how cyber-warfare will not take place is most definitely the article by Thomas Rid, published in 2012. The title of this article is self-evident: cyber-warfare will not take place. Rid concludes his article with three main observations. The first one is the assertion that not high-tech but low-tech has been a leader in the past of violence escalation, instability, and in the end war. Overall what he means in this conclusion is that although the Internet might play a great role in social and political events within niche groups, but this role is only temporarily or applicable over an extended time. Even if the Internet could play a significant role in the working of niche groups, this is not always in a violent manner. He believes political offences created by these groups are not repetitive technologically highly sophisticated forms of sabotage. In short, Rid claims niche groups are small, temporarily and meaningless groups who might conduct uncomplicated attacks that might lead to instability and violence, but they will never come to a significant extent.

The second observation Rid makes is criticising the main analysis in cyber articles. This general analysis argues that cyber-attacks are easier, cheaper and

more effective than conventional attacks. He emphasizes the exaggeration existing in literature on this matter. Rid underscores that quality matters more than quantity, according to him the number of actors that are able to launch an offensive and complex attack is likely to be smaller than commonly assumed. The evolution in technology, cyber protection and security leads to a better protective and defensive setup of complex systems. Consequently, this leads to more need of resources, skills and organization required from the attacker. Having this amount of skill is only attainable to very few sophisticated strategic actors.

The third observation made by Rid draws the attention on the openness needed of defence capabilities of states. The only secure method a state can pursue to protect itself sufficiently from cyber-attacks or even cyber-war is to build defence capabilities. The world's most sophisticated cyber forces have an interest in openness if they want to retain their edge, especially on defensive matters. Only openness and oversight can expose and reduce weaknesses in organization, priorities, technology, and vision. Rid does not believe the increase in technology, cyber-espionage or sabotage will lead to a stand-alone war (Rid, 2012).

In our view Rid's statements are out-dated. His claims seem to be somewhat superficial and doubtful. Although niche groups can have a temporary and small existence, that does not mean the outcomes of their deeds can be summarised into insignificance. When we look at the example of the Sony hack (see supra) we can conclude considerable measurements can be taken as a response to a cyber-attack conducted by a small hacker group. These measurement could eventually lead to a cyber-war. Rid's attempt to exclude the possibility of a cyber-war by emphasizing the difficulty and sophistication of a cyber-attack leaves us unsatisfied. Merely because an attack is complex and can only be created by few experts, does not mean it is an impossible reality. The Stuxnet-virus was created over a ten-year timespan, but that did not stop the attack from happening. Even his last argument forms a source of concern. His claim on how the openness of

defence capabilities is the only way of exposing and reducing weaknesses remains doubtful and vague.

Apart from Rid's research, few academics deny or exclude the possibility of a cyber-war. The shortcomings of this stream brought us to the conclusion this school of thought remains in minority and their analysis seems to be rather out-dated.

10.2. Cyber-warfare as a complement to conventional warfare

In the second stream of thinking academics claim cyber-warfare as a stand-alone concept won't happen, however, it will become a crucial concept in the thinking of warfare. Namely, cyber-warfare will complement conventional warfare. British General Sir Nicholas Houghton recognized in 2015 that most acts of physical war today incorporate an online aspect. Here social networks are exploited to manipulate opinion and perception (The Royal Insitute of International Affairs, 2015) But why could it not become a warfare an sich? There are several arguments for that.

First of all, a clean war in cyber-space alone will never take place because a country that has been attacked will defend itself by conducting a counterattack using all existing tools. Imagine a scenario wherein one actor has been cyber-attacked. The affected party will attack the server of the perpetrator, if they have the opportunity to do so. If the affected actor can ensure more attacks will not be conducted again, by for example assassinating experts who are behind a cyber-attack, they will do this too. It is not a given that one actor who has been cyber-attacked, will respond with the same form of attack (i.e. a cyber counter attack). Affected actors won't limit themselves to an attack in kind. They will use every tool available to them in their retaliation (personal interview, 2017).

Secondly, there have not been artificial intelligence attacks so far. There have been no instances of automated attacks and automated counterattacks. This leads to the conclusion that behind every attack there is a human reason why it

has been conducted. It remains a political decision to carry out a certain attack and this attack will be created and conducted by people from country X and against people from country Y. Cyber-space is a human institution. As long as artificial intelligence does not take over, everything surrounding cyber will be controlled and monitored by people (personal interview, 2017). The later brings us to our third argument.

Motive is a fundamental condition for war to be initiated. This is as true for conventional warfare as it is for cyber-warfare. This motive emerges after a conflict of interest occurs between two actors in a non cyber-space. Once a conflict takes place, there emerges a motive. Without a motive developing initially in one of the four existing military domains (land, sea, air and space), it is unlikely there would start a cyber-warfare (personal interview, 2017). Thus, before being able to start a cyber-war there has to be a motive developed in the other four military domains. Segal (2016) underlines that launching a conventional military operation in retaliation to a cyber-attack is unlikely. However, this destructive counterattack would only be possible if conflicting actors are already engaged in military conflict or perceive core interests as being threatened. A cyber-war emerging out of nowhere; without a motive, on going military conflict or interference of interests, seem rather unlikely.

Although there are several arguments on why cyber-warfare will not become a stand-alone phenomenon, it still can become a complement to conventional warfare. Currently cyber threats are one of the greatest threats to international peace and security. Protecting oneself against it and securing this cyber-space is of vital importance. Ideally, the cooperation of all states would be the best way to eliminate the cyber threat. But as mentioned before the balance of power that exists in international relations also applies to cyber-space. Thus, global cooperation might, not yet, be a reality. However, states do realize there is a need for protection and they achieve this protection by investing and focusing on cyber-security and defence capabilities. We notice a trend in increasing investment in everything surrounding cyber, making it a new domain in defence

policies. States are investing in cyber emergency plans, cyber diplomacy, cyber-security centres. This makes cyber a part of their foreign policy and their strategy thinking. World powers have made efforts, not only in investing in offensive capabilities, but also in defensive capabilities. If there was no possibility of the cyber-dimension becoming an important part in warfare there would not exist such efforts to try and secure cyber-space.

10.3. Cyber-warfare as a stand-alone concept

As John Hayward (2015) has said: *cyber-war is too easy, effective, and deniable to be stopped.*

It may appear as far-fetched and exaggerated to think that cyber-war could be a phenomenon independent to that of war, yet it is one that has been explored. In this case traditional thought and taxonomies that are applicable to conventional warfare do not apply to cyber-warfare. Cyber-warfare is the new warfare. Together with the first stream, this third stream is also a minority. With the on going, unstoppable and swift changes in technology we deem it of utmost interest to reflect on this part with an open mind; it is important to think the unthinkable. One decade ago, no one would have ever imagined attacks like the Stuxnet-attack would have been possible, but that does not mean new forms of attacks or warfare can be developed.

In "Cyberwar is coming!" by Arquilla and Ronfeldt (1992) suggestions and speculations are made around the plausibility of an upcoming era of cyber-warfare. They believe the basis of cyber-warfare is increasing the importance of information. Technology experts, governments and the military around the world are preparing themselves for cyber-warfare. The post-modern battlefield stands to be fundamentally modified by the information technology revolution, at both the strategic and the tactical level. The possibility of a cyber-warfare era is becoming more and more plausible because of the increasing breadth and depth of this battlefield and the ever-improving accuracy and destructiveness of this field. Cyber-war is warfare to fear because it is characterized by the effort to

turn knowledge into capability. Arquilla and Rondfeldt argue that cyber-war might be in need of advanced technologies, but it is not reliant upon advanced technologies per se. Cyber-warfare has the great advantage of having organizational and psychological dimensions as well. Additionally, according to Arquilla and Rondfeldt these dimensions may be as important as the technical dimension. Cyber-war may actually be waged with low technology under some circumstances. Although this analysis seems to fit into this last stream of cyber thinking, the authors do mention that cyber-war characterizes a constant but often halting and contentious interplay between operational and organizational levels. Cyber-war implies a new man-machine interface that strengthens man's capabilities, not a separation of man and machine. The latter might imply they see cyber-warfare as a possibility but never as a separated concept to conventional war. We believe it is highly interesting to read an article dating from 1992 that is already speculating on how cyber-warfare might take place.

During our interviews we noticed vast amount of interviewed actors warned us for The 'Internet of Things (IoT)'. What can we understand under The IoT and why is it something to worry about? The IoT contains several technologies and research disciplines that enable the Internet to reach out into the real world of physical objects. Technologies like short-range wireless communications, real-time localization, and sensor networks are becoming increasingly pervasive and this empowers the existence of the IoT. Human understanding and the usage of, and interaction with advancing technology and the systems they form have not developed at the same pace. This creates a gap in knowledge and different actors are exploring this domain of technology. This makes it a quite new and under-explored subject (Feki, Kawsar, Boussard, & Trappeniers, 2013). By connecting billions of everyday devices, the IoT merges the physical and online worlds, opening up a host of new opportunities and challenges for companies, governments, and consumers. In general it will only increase the ubiquity of the Internet. The securing of devices will become more important and cyber criminals have even more opportunity to conduct attacks. In general it makes the possibilities in the cyber-world even more varied and widespread. The

acceleration of smart adaptive devices, which make their own smart decisions, as well as pass data to other devices, is a new concept. The proliferation of those devices poses serious security challenges for several organizations and institutions. IoT deployments can lead to hackers waging cyber-war on businesses and launching DDoS attacks on enterprise infrastructure (Waldorf, 2016). Perhaps before entering in the world of stand-alone cyber-warfare, the IoT is the first next step in the cyber-world. The IoT will, according, to our analysis make the feasibility of a cyber-warfare only greater. And even though IoT is a rather upcoming and unknown subject, the importance of it will only enlarge.

It's clear that the literature on this last stream is under-developed, but that does not mean it should be considered as an after thought. When looking at the swift evolution in technology and cyber developments we strongly believe this last option, cyber-warfare as a stand-alone war, should be considered seriously.

11. Conclusion

We started this research with the main question investigating if cyber-warfare was becoming a new tool in foreign policy. After reading an extensive amount of books, articles, blogs; listening to different lectures; and conducting interviews, a conclusion can be made.

In (2015) Van Der Meer asserted that in the next decade cyber-security will be a key topic in international politics. We believe this will not be the case in ten years, because it is already happening right now. The main feature of cyber-space is its swift development. The digitalization of the world and the cyber threats and aggression that result from this quick development will only make cyber increasingly important in our world. We have observed the efforts made by state actors for the investment and building up of cyber capacities. These efforts go from security, to defense and deterrence. Our interviews have shown governments are putting cyber higher and higher on the political agenda, creating cyber-security and emergency plans, cyber institutions and even training cyber diplomats. Throughout our research we have given diverse reasons why one would prefer engaging in a cyber-war instead of a conventional war. This once again showed the ease, benefits and accessibility of engaging in the cyber-domain. Therefore, we can answer our research question positively: yes, cyber is becoming a new tool of foreign policy. States are making cyber a fifth domain in defense policies and this expansion in cyber investment will not be reversed. The focal point of cyber in foreign policies is only occurring in a greater extent and will most probably become a core aspect in foreign policies. Cyber and politics are creating an intertwined relationship that is only becoming stronger.

In addition to the above finding as the answer to our research question we have also found a different way in thinking about cyber (warfare). Although the first stream in thinking, which believes cyber-warfare will never take place, is in our opinion outdated and obsolete, there is still a lot of contradistinction existing between the second and the last stream of thought. We believe the second

stream of thinking, which believes cyber-warfare will only complement conventional warfare, can be perceived as the contemporary stream of thinking. A couple of decades ago the majority of people probably thought of cyber-warfare as an impossible phenomenon or let alone a cyber-attack could paralyze vital infrastructure inducing real victims. Look how quick this thinking has changed in only a couple of decades. And even though many academics still believe cyber-warfare will never become a stand-alone concept, we are convinced there is a big possibility this will become our future warfare. The investments continue, the threats become bigger and the developments are unstoppable. So would it not be naïve to exclude the possibility of cyber-warfare as a stand-alone concept? Maybe. The problem, and at the same time the strength, of cyber is the unpredictability of it.

As we look towards the future, a raft of social changes are likely to occur due to this increased usage of technology within daily life. An insufficient regulatory and legal framework provides the global community with great challenges as technological advancement continues to occur at an almost exponential rate. If cyber-warfare can be imagined we might already start thinking of the consequences of such a war. We have seen that the power balance between world powers does also apply in cyber-space. We have also seen that cyber-attacks suffer from the problem of attribution and know unpredictable outcomes. A cyber-war can be fought at any time, in any place. So perhaps it is time to think about the possibility of World War III. This time fought in cyber-space.

VI. References

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

Al Jazeera. (2017). *"Major disruption" as UK hospitals hit by cyber attack.* Retrieved May 13, 2017, from http://www.aljazeera.com/news/2017/05/disruption-uk-hospitals-hit-cyber-attack-170512160000368.html.

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

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

Arquilla, J., & Ronfeldt, D. F. (1992). *Cyberwar is Coming!* Rand Corporation.

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

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

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

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

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

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

Breene, K. (2016). *Who are the cyberwar superpowers?* Retrieved April 25, 2017, from https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

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

Cairney. (2017). *Why doesn't evidence win the day in policy and policymaking?* Retrieved April 23, 2017, from https://paulcairney.wordpress.com/2017/02/22/why-doesnt-evidence-win-the-day-in-policy-and-policymaking/.

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

Cambridge English Dictionary. (n.d.). *the free world Definition in the Cambridge* English Dictionary. Retrieved May 1, 2017, from http://dictionary.cambridge.org/us/dictionary/english/the-free-world.

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

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

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

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

CNN, L. S.-S., Milena Veselinovic and Hilary McGann. (2017). *UK prime minister: Ransomware attack is global.* Retrieved May 13, 2017, from http://www.cnn.com/2017/05/12/health/uk-nhs-cyber-attack/index.html.

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

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

De Bruycker, M. (2010). *Cyber Defence. Cyber Defence*, 4.

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

De Wolf, L. (2017). *Hacker houdt woord: Tien afleveringen "Orange is the new black" online.* Retrieved May 6, 2017, from http://deredactie.be/cm/vrtnieuws/cultuur%2Ben%2Bmedia/media/1.2966250.

Debruyne, A. (2017). *Wereldwijde cyberaanval ransomware werk van Noord-Korea*. Retrieved May 16, 2017, from http://www.knack.be/nieuws/wereld/wereldwijde-cyberaanval-ransomware-werk-van-noord-korea/article-normal-853059.html.

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

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

Diplomat, G. B. and C. D. Y., The. (2017). *Evaluating the US-China Cybersecurity* Agreement, Part 2: China's Take on Cyberspace and Cybersecurity. Retrieved May 13, 2017, from http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/.

edm, gjs. (2017). *Ook Russisch ministerie van Binnenlandse Zaken getroffen door cyberaanval.* Retrieved May 13, 2017, from http://www.standaard.be/cnt/dmf20170512_02879069.

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

Europe Institute. (2008). *Cyber War I: Estonia attacked from Russia.* Retrieved May 5, 2017, from

http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.

Evron, G. (2017). *The First Internet War in Estonia: The postmortem I wrote, 10 years later.* Retrieved May 5, 2017, from https://hackernoon.com/the-first-internet-war-in-estonia-the-postmortem-i-wrote-10-years-later-72040f53620e.

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

Farwell, J. P., & Rohozinski, R. (2011). *Stuxnet and the Future of Cyber War.* Survival, 53(1), 23–40. https://doi.org/10.1080/00396338.2011.555586.

Feki, M. A., Kawsar, F., Boussard, M., & Trappeniers, L. (2013). T*he Internet of Things: The Next Technological Revolution.* Computer, 46(2), 24–25. https://doi.org/10.1109/MC.2013.63.

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

Fousek, J. (2000). *To Lead the Free World: American Nationalism and the Cultural Roots of the Cold War*. Univ of North Carolina Press.

Furnell, S. M., & Warren, M. J. (1999). *Computer hacking and cyber terrorism: The real threats in the new millennium?* Computers and Security, *18*(1), 28–34.

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

Gewirtz, D. (2015). *Why the next World War will be a cyberwar first, and a shooting war second.* Retrieved May 13, 2017, from http://www.zdnet.com/article/the-next-world-war-will-be-a-cyberwar-first-and-a-shooting-war-a-distant-second/.

Gibney, A. (2016). *Zero Days*.

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

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

Haggard, S., & Lindsay, J. R. (2015). *North Korea and the Sony hack : exporting instability through cyberspace* (Report). Honolulu, HI : East-West Center. Retrieved from http://scholarspace.manoa.hawaii.edu/handle/10125/36444.

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

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

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

Holloway, M. (2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities.* Retrieved April 13, 2017, from http://large.stanford.edu/courses/2015/ph241/holloway1/

ICRC. (2010). *The law of armed conflict.* Retrieved April 9, 2017, from /eng/resources/documents/misc/5p8ex4.htm.

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

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

Jr, J. S. N. (2011). *The Future of Power*. PublicAffairs.

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

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

Kasher, A. (2007). *The Principle of Distinction.* Journal of Military Ethics, 6(2), 152–167. https://doi.org/10.1080/15027570701436841.

Kelsey, J. T. G. (2008). *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.* Michigan Law Review, *106*(7), 1427–1451.

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

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

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

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

Lemmens, L. (2015). *25 extra personeelsleden voor cyberveiligheid bij ADIV ondanks federale aanwervingsstop.* Retrieved April 30, 2017, from http://www.polinfo.be/newsview.aspx?contentdomains=POLINFO&id=VS300309727&lang=nl.

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

Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.

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

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

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

Marjz, F. (2006). A *multifaceted approach to understanding the botnet phenomenon*. Retrieved from /paper/A-multifaceted-approach-to-understanding-the-Rajab-Zarfoss/3325cdfb66a03aad5a6d0b19840f6bdb713d0e7a.

Microsoft. (2001). *Virtual Private Networking: An Overview*. Retrieved May 1, 2017, from https://technet.microsoft.com/en-us/library/bb742566.aspx.

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

Mortelmans, D. (2007). *Handboek kwalitatieve onderzoeksmethoden*. Acco.

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

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

NATO, parlementary assembly. (1999). *Science and Technology Committee. Information Warfare and international Security.* Retrieved February 5,

2017, from http://nato-pa.int/archivedpub/comrep/1999/as285stc-e.asp.

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

O'Day, A. (2004). *Cyberterrorism*. Ashgate.

Office of the National Counterintelligence Executive. (2011). *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*. Retrieved April 5, 2017, from http://www.cfr.org/cybersecurity/office-national-counterintelligence-executive-foreign-spies-stealing-us-economic-secrets-cyberspace/p31052.

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

Paelinck, G. (2015). Belgisch leger krijgt cybercomponent naast traditionele land-, lucht- en zeemacht. Retrieved April 30, 2017, from http://deredactie.be/cm/vrtnieuws/politiek/1.2296591.

Panorama. (2012). *Cyberwar.* Retrieved March 10, 2017, from http://deredactie.be/cm/vrtnieuws/videozone/programmas/2.27106/2.27142?video=1.1315987.

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

Pham, S. (2017). *China fortifies Great Firewall with crackdown on VPNs.* Retrieved May 1, 2017, from

http://money.cnn.com/2017/01/23/technology/china-vpn-illegal-great-firewall/index.html.

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

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

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

Rid, T. (2012). *Cyber War Will Not Take Place.* Journal of Strategic Studies, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939.

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

Roberts, D. (2015). *Obama imposes new sanctions against North Korea in response to Sony hack.* The Guardian. Retrieved from https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview.

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

Royal Higher Institute For Defence. (2017). *What strategy to address hybrid threats?* Conference 16 February 2017. Retrieved April 25, 2017, from

http://www.rhid.be/website/index.php/88-english/conf2017-en/1308-conf-2017-02-16.

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

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

Sanger, D. E. (2012). *Obama Ordered Wave of Cyberattacks Against Iran.* The New York Time*s*. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

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

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

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

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (1 edition). New York: PublicAffairs.

Slayton, R. (2017). *What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment*. International Security, 41(3), 72–109.

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

SWIFT Homepage. (n.d.). Retrieved April 25, 2017, from https://www.swift.com/node/7746.

Symantec (2012). *Ransomware: A Growing Menace.* Retrieved April 6, 2017, from http://www.symantec.com/connect/blogs/ransomware-growing-menace.

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

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

The Royal Insitute of International Affairs. (2015). Building a British Military Fit for Future Challenges Rather than Past Conflicts. Retrieved May 15, 2017, from https://www.chathamhouse.org//node/18434.

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

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

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

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

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

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

Waldorf, K. (2016, July 22). *The Dangers of the IoT*. Retrieved May 5, 2017, from https://www.wirelessweek.com/article/2016/07/dangers-iot.

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

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

Wills, G. (1999). Bully of the Free World. *Foreign Affairs*, *78*(2), 50–59. https://doi.org/10.2307/20049208.

World Economic Forum. (2015). Top countries best prepared against cyberattacks. Retrieved April 25, 2017, from https://www.weforum.org/agenda/2015/07/top-countries-best-prepared-against-cyberattacks/.

Worldcrunch. (2014, October 30). China and Russia Forge Cybersecurity Partnership Without the U.S. Retrieved May 13, 2017, from http://www.huffingtonpost.com/worldcrunch/why-russia-and-china-see-_b_6071528.html.

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