Cyber Security: Cooperation or Proliferation?

Jasper Smallenbroek
J.J. Slauerhoffplantsoen 10
2548ED, Den Haag
Student number: S2548968
Phone number: (+44) 7480683642 (+31) 707532050
Supervisor: Dr. Benjamin Herborth
DECLARATION BY CANDIDATE

I hereby declare that this thesis, "Cyber Security: Cooperation or Proliferation", is my own work and my own effort and that it has not been accepted anywhere else for the award of any other degree or diploma. Where sources of information have been used, they have been acknowledged.

Name JASPER SMALLENBROEK

Signature

Date 11-08-2015
# Table of Contents

**Introduction** ............................................................................................................. 1

**I - Background** ......................................................................................................... 3
The proliferation problem ............................................................................................... 5
The trade-off .................................................................................................................... 6

**III - US cyber policy** ................................................................................................. 9
Case and source selection .............................................................................................. 9
From the 2003 *National Strategy to Secure Cyberspace* to the 2011 *International Strategy for Cyberspace* ........................................................................................................ 10
NSPD 54 and PPD 20 ..................................................................................................... 13

**II - State of the art** ................................................................................................... 17
Researching the Trade-Off ............................................................................................. 17
The securitisation of cyberspace and computer security ............................................... 19
Cyber deterrence ........................................................................................................... 22
Cyber power .................................................................................................................. 24
Cyberspace as an ecosystem ......................................................................................... 25
The potential for cooperation ......................................................................................... 28
Assumptions and impact on policy recommendations ............................................... 30

**III - What is a cyber weapon?** .................................................................................. 32
The lack of definition ..................................................................................................... 33
Towards a definition ...................................................................................................... 34
The anti-virus virus ....................................................................................................... 39

**IV - What is cyberspace?** ........................................................................................ 40
Origins ............................................................................................................................. 40
Conflicting definitions ................................................................................................. 42
The technical functioning of cyberspace .................................................................... 42
The Dynamics of Cyberspace ..................................................................................... 43

**V - US Policy and Cyberspace** ............................................................................... 45

**VI - Miscalculation?** ................................................................................................ 47
The role of cyber weapons in cyberspace ..................................................................... 48

**VII - The Prospects for Cyber Arms Control** ......................................................... 54

**Conclusion: Proliferation or cooperation?** .............................................................. 59

**Bibliography** ............................................................................................................. 64
Introduction

This thesis will examine to what extent there is a trade-off between the development of cyber weapons and cooperation in cyber security. To what extent are these mutually exclusive? It does so by focusing specifically on the policies of the United States (US), which has been at the forefront of developing cyber capabilities and policy. Through this case study it will become possible to draw out the rationale behind the development of cyber capabilities. Simultaneously, it will also expose a duality present in the policies of the US. On the one hand the Department of Homeland Security (DHS) is working on securing critical infrastructure while on the other the military and intelligence agencies are successfully finding ways to compromise those same systems. Meanwhile, meaningful international cooperation on cyber security has been minimal. Are the policy choices of the US stimulating the proliferation of cyber weapons and thereby reducing the prospects for cooperation?

The after the introduction this thesis will begin by providing the reader with some background on the topic of cyber security. How has cyber security become something states are deeply concerned about? While answering this question it will provide a brief overview of US policy cyber security and its evolution. While doing so it will highlight the most important US policy documents pertaining to cyber security. By examining these documents it will draw out the central principles of US policy cyber policy. This will expose the potentially opposite goals of developing offensive capabilities while simultaneously defending critical infrastructure from attack and maintaining a functioning cyberspace. This discussion will lead into a section, which focuses on explaining why these simultaneous goals of offence and defence are, in a technical sense, at odds with each other.

After providing the reader with this background information the thesis will proceed to provide an overview of the most current literature surrounding cyber
security policy in the state of the art chapter. It will do so by outlining the predominant theoretical perspectives that frame thinking about the use of cyber weapons and the potential for cyber security cooperation. Within the current literature there are several such theories. In doing so it will place the theories into three categories cyber deterrence theory, cyber power theory, and cyber ecosystem theory. By comparing these different theoretical perspectives their underlying assumptions will become clear making it possible to outline why the policy recommendations resulting from each of these perspectives differ.

Chapter II will then deal with the question of what cyber weapons are. Strangely, while there has been much discussion about cyber weapons no international organisations, or states have defined what they are. Here, Rid and McBurney have made one of the only contributions. Their work will be closely examined while holding it up against the Tallinn Manual, which has been published by a North Atlantic Treaty Organisation (NATO) think tank to examine how international law is applicable to cyber warfare. Using a sound definition is of great importance to the argument of this thesis as it allows us to focus specifically on cyber weapons as a distinct form of malware. It is of vital importance that we are able to differentiate cyber weapons from malware that is used for purposes such as theft, sabotage or espionage.

This discussion will be followed by a more conceptual chapter, which explores what cyberspace is. Examining this question closely is important, as it is cyberspace, which provides us the context in which relations occur. The chapter will show that it is possible to compare and contrast the different conceptualisations of cyberspace by analysing their underlying assumptions. By distilling what these assumptions are the strengths and weaknesses of different conceptualisation of cyberspace can be highlighted. Meanwhile this chapter will also focus on how cyberspace works technically. Allowing us to form a picture of what the dynamics of cyberspace are, compared to physical space. These findings will then be related back to the previous discussion of the theoretical perspectives to gain a deeper understanding of their strengths and weaknesses.
After having explored the different theoretical perspectives and defined what cyberspace and cyber weapons are, this thesis shall move on to its analysis chapters. First, it will examine why cyber weapons are being created. To do so, this thesis shall use a categorisation of cyber conflict, which ranges from most to least common type of conflict. This will allow us to explore what utility cyber weapons have. The following chapter will analyse the trade-offs states face when they consider serious cooperation in the field of cyber security. It will do so by comparing the chemical weapons convention to a possible treaty banning cyber weapons. By doing so, it will draw out the obstacles to more substantial cooperation. This will answer the question to what degree there can be said to be trade-off between cooperation and the proliferation of cyber weapons.

I - Background

The growing interest in cyber weapons and cyber warfare can largely be explained by the realisation that today’s events in cyberspace impact society, the economy, and national security (DeNardis 2014:86-88). The invention and development of the internet through the 1960s and 70s, followed by the vast expansion of the world wide web from the mid 1990s onwards means that we have become increasingly dependent on networked communications (Nye 2011:24-25). It is clear that the expansion of cyberspace has presented society with new opportunities and vulnerabilities (Kuehl 2009:18). On the one hand it is estimated that currently the internet has 2 billion users who annually exchange 8 trillion US dollars through e-commerce with the US pocketing 30 per cent of the global internet revenue (Pelissie et al. 2011:1, 4). On the other hand the frequency of politically and criminally motivated cyber attacks has also increased (Renard 2014:8). Most critical infrastructure in the US such as electricity grids, banking and transportation systems now rely on cyberspace to function. This makes them vulnerable to attack from both state and non-state actors (Aaronson 2014).
Perhaps the most far reaching of these new vulnerabilities is the possibility to turn malicious code into weapons, which target physical infrastructure. Today insecurity in cyberspace is increasingly translated into physical insecurity. In 2005 former US General John Casciano noted that new uses of information communication technology were causing a revolution in military affairs. According to him these technologies were giving militaries a new medium through which to conduct operations (Barletta, Barletta, Tsygichko 2011:54). Currently over 100 countries are believed to have developed “cyberwar capabilities” (Wright, Singer 2013). Reports by the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, which is comprised of members representing the leading cyber powers also acknowledge the spread of cyber capabilities (Meyer 2012:18). The GGE has released two consensus reports the first in 2010 and the latest in 2013. The 2010 report recognised that ‘States are developing ICTs as instruments of warfare and intelligence’ (2010:7). The 2013 report similarly recognised that states view each other as sources of cyber threat (2013:6).

It is clear that the US military has put considerable effort into developing offensive cyber capabilities. In 2013 General Keith Alexander the former head of the NSA and Cyber Command reassured congress that “we believe our [cyber] offence is the best in the world” adding that developing such capabilities is crucial to denying an “asymmetric advantage” to adversaries (H.A.S.C. NO. 113-17 p87). Generally, the use of cyberspace in times of political conflict is becoming increasingly common. Recently the Ukraine has been the victim of a series of attacks linked to its conflict with Russia for example. It has been reported that Russia has successfully infiltrated the computer systems belonging to the Ukrainian military, border patrol, counterintelligence and local police. The invasion of Crimea also had a cyber element with the communication systems of Ukranian forces being rendered useless the blocking of the mobile phone network and government websites being taken offline (Coyle 2015). However, the most widely talked about and most astonishing attack remains the 2010 the attack on the Iranian Natanz uranium enrichment facility. This was the first
attack that gave observers a chance to see what a state created cyber weapon looks like and is capable of. Crucially, it proved that such a weapon could cause physical damage (Morton 2013:23; Farwell, Rohoznski 2011:25). The attack on Natanz also made clear how the weapon was used to influence the political situation (Morton 2013:231). The setbacks to the Iranian nuclear project gave more time for economic sanctions to take effect. Further it can be argued that, by deploying a weapon based on such sophisticated code the US demonstrated its proficiency in conducting cyber operations, thereby reinforcing its superpower status (Langer 2013).

**The proliferation problem**

We must take seriously the proliferation problem related to the use of cyber weapons. Once used they easily proliferate. Eugene Kaspersky co-founder and CEO of Europe’s largest antivirus company has likened cyber weapons to ‘boomerangs’; once you use them they come back to hit you (2013 17:50-18:34). Similarly, Ralph Langer an expert on critical infrastructure security has also pointed out that reverse engineering and re-appropriating code for something other than its initial intended purpose is much easier than developing new code (2011 8:30-9:45)¹. Meanwhile, both the International Telecommunications Union and the GGE in its 2013 report have also pointed to the dual use nature of cyber weapons (Barletta, Barletta, Tsygichko 2011:62; GGE 2013:6). Empirically such concerns are well founded to illustrate this we can turn to Stuxnet as a case study again. Parts of its code are likely to have been used by hackers who attacked the Saudi Aramco Oil Company in 2012. The attack succeeded in rendered 30,000 of the company’s computers useless (Rid 2013:55, 64)². Even

---
¹ Ralph Langer is the director of Langer communications a cyber security-consulting firm. He has over 25 years of experience in the cyber security of infrastructure and was the first to closely examine the Stuxnet code publishing several research reports about it.
² Thomas Rid is a professor at the Department of War Studies at King’s College London and a leading skeptic of cyber war. In his book *Cyber War Will not Take Place* he argues that cyber war is not a realistic threat. His argument however, is nuanced. He does agree that cyberspace is full of threats and that it will be used in times of war yet he argues that the role cyberspace will play is more limited than many expect.
before this attack took place a report compiled for the US Congress acknowledged the 'possible proliferation problem' resulting specifically from the use of Stuxnet (Kerr, Rollins, Theohary 2010:2). Further illustrating the re-appropriation problem a video on the Semantec youtube channel shows a security researcher who uses Stuxnet code to change the operating parameters of an air pump controlled by an industrial control system, causing the balloon he is inflating to burst (O Murchu 2010).

While re-appropriation is one problem compounding it is the fact that once a piece of malware is released it is difficult to contain. Stuxnet did not just infect computers in Iran. It infected at least 50,000 computers showing up in India, Indonesia, and Pakistan. It was also found on computers belonging to Chevron and German industry, most notably it is also thought to be responsible for the failure of an Indian satellite launch in 2010 (Schneier 2015:150). Given the ease, with which malware can spread and the potential for re-appropriation of code, it is questionable if the US is not making itself more vulnerable to attack by creating sophisticated malware.

The trade-off

What this thesis is examining is if the creation of cyber weapons may have the potential to stifle attempts at cooperation aimed at creating a more secure cyberspace. To better understand why there may be a fundamental choice between cooperating to improve cyber security and developing cyber weapons it is important to have an understanding of how it is possible to gain unauthorised access to a system and how to defend against it. To accomplish unauthorised access the attacker has to be able to exploit vulnerabilities within a system. Bruce Schneier\(^3\) describes such vulnerabilities as follows: “Vulnerabilities are mistakes. They’re errors in design or implementation – glitches in code or

\(^3\) Bruce Schneier is a cryptographer, computer security specialist, and privacy advocate. He is the Chief Technology Officer of Resilient Systems, a fellow at Harvard’s Berkman Centre, and a board member of the Electronic Frontiers Foundation. He has also been maintaining a blog on cyber security since 2004.
hardware – that allow unauthorised intrusion into a system” (2015:144). When a new vulnerability is discovered it can be used either for attack or defence. When used for defence one would alert the vendor so that it can be patched and the community of developers can learn from it. Conversely, when used for attack the vulnerability must be kept secret. As long as it remains undetected the attackers can use the vulnerability with impunity, as no one will be protected against it. Such vulnerabilities are known as ‘zero-days’ (ibid 145). All this results in a rather interesting caveat. The way in which the balance between offence and defence works in cyber security is different to the way it normally does. In cyber security the ability to attack actively undermines the ability to defend. Therefore, it is logical that actors interested in developing cyber weapons may be disinterested in cooperating to secure cyberspace which may involve making public their knowledge of zero-days. Further, it is also probable that actors who are developing cyber weapons or malware in general would be interested in hoarding or stockpiling as many zero-days as possible so they can pick and choose which ones to use when they are creating the malware (ibid 145).

Again we can turn to Stuxnet to further illustrate the problem of stockpiling. Stuxnet used multiple zero-days, which allowed the attackers (who are widely presumed to be the US and Israel) to infiltrate the targeted computer systems (Langer 2013:11). It also used stolen digital certificates, which allowed Stuxnet to pose as a legitimate piece of software making it impossible for anti-virus software to detect (ibid 22). In fact they used so many of these vulnerabilities when creating their malware that it seems the attackers had a stash of zero-days and stolen certificates to choose from (ibid 11). Confirming these suspicions, the office of the Director of National Intelligence has confirmed that it has a “Vulnerabilities Equities Process” which determines when knowledge about

---

4 Digital certificates are analogues to passports or ID cards and are used to signify ownership of a public key that allows for the secure exchange of information. Digital certificates use a trust model to ensure that end users can verify that they are genuine. They can be issued to users, computers, devices or webpages by a certification authority, which is a trusted third party. Digital certificates are an important link when communicating over the World Wide Web as they are intended to prevent an attacker from impersonating the party to which they are issued. Additionally digital certificates can also be used to set up encrypted connections allowing for secure communication.
zero-days may be made public (DNI 2014). Even more concerning on this front is that documents released by Snowden have revealed that the NSA has been deliberately inserting vulnerabilities into software and hardware. The NSA does so through its ‘SIGINT\(^5\) Enabling Project’ which, as the released slide states: “actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products’ designs. These design changes “make the systems in question exploitable through SIGINT collection” (Snowden document). All this points to the stockpiling of zero-days by the US and presents us with a problematic situation. If the US is stockpiling these zero-days then it is foregoing the opportunity to make that knowledge public and cooperate with others to fix the glitches it found.

Further, there also exists a link between the cyber crime community and the development of cyber capabilities. It is clear that cyber attacks from state actors nearly always involve “tradecraft, techniques, and code” which are connected to cyber criminals (Farwell, Rohozinski 2011:26). There even exists a grey market for zero-day exploits and skilled malware programmers (ibid 27). A French company called Vupen for instance openly sells exploits to clients, which, according to their website meet their criteria (Vupen website). While it is unclear exactly what these criteria are a Freedom of Information Act request has produced a contract between Vupen and the NSA for “binary analysis and exploits service” (Blackvault 2013). Two other well-known companies in this sector are HackingTeam and FinFisher\(^6\). Presumably these companies buy exploits from anonymous hackers and sell them on to other parties, who will use them to build malware.

\(^5\) SIGINT is a widely used acronym for Signals Intelligence i.e. the gathering of intelligence through the interception of signals.

\(^6\) Wikileaks has released 287 files relating to the surveillance industry as part of its ‘Spy Files’ project. These include sales brushes and PowerPoint presentations promoting products and services from a 160 intelligence contractors. The companies in question provide a wide range of services and products such as internet traffic interception capabilities, speech analysis tools allowing for tracking based on ‘voiceprints’, mobile phone location tracking as well as hacking tools (2011).
Clearly there is a conflict of interest between those creating cyber weapons and those who are in the business of securing our computing environment (Langer 2013:23). Nonetheless, it is estimated that the US is spending 2.5 to 4 times more on cyber offence than defence (Singer, Friedman 2014). Judging from these numbers it certainly seems like the former is taking precedence over the latter. Further illustrating the obsession the US has with developing offensive cyber capabilities is that policy makers only started thinking about defence after considerable resources had already been committed to the development of offensive capabilities. When reading Richard Clarke’s book Cyber War; The Next Threat to National Security and What to Do About It this becomes apparent. The way in which the organisations surrounding cyber security developed in the US drives the point home. In 2010 he wrote that the US army had already set up a centre for cyber operations that had between 6 to 8 thousand personnel (ibid 41). It was only at that point however; that high-level officials started to think about the defence of critical infrastructure. The task of defence was one former NSA director Minihan thought should be given to the DHS (ibid 43). Clearly developing offensive capabilities has been a priority from the start while little thought was given to the consequences. All this raises many questions about the way in which the US deals with cyber security today. It is clear that today cooperation in the field of cyber security is sub-optimal and that the developing of cyber weapons creates adverse incentives for cooperation. This thesis aims to shed light on to what extent there is a trade-off between cooperation and proliferation.

III - US cyber policy

Case and source selection

7 Clarke held several high level positions at the White House under Presidents Bush junior and senior and Clinton including the position of Special Advisor for cyber security under President W. Bush.
The choice was made to focus specifically on US policy for this thesis for several reasons. First, technologically the US has been instrumental with regards to the creation of the internet and has also developed the worlds most advanced cyber capabilities. It was the US in conjunction with Israel who have produced what is up until now the only known example of a cyber weapon. Stuxnet therefore gives us an interesting real world example from which we can draw lessons. Second, because the US has been breaking new ground technologically it has also had to think strategically about securing cyberspace and devise policies relating to the use of cyber weapons before other countries started to do so. At an early stage US policy makers faced a real choice about whether or not to develop and use cyber weapons, which other countries have not. Because of the advanced state of its cyber capabilities and early adaptation of cyber security policies the US has had a fundamental impact on how cyberspace is secured. Admittedly it would have been interesting to do a comparative analysis as the Nordic countries and Japan have adopted very different cyber security policies to those of the US for example. However, the time is ripe to study the policies relating to the use of cyber weapons in the US as recent leaks have removed the usual vial of secrecy surrounding it. As we shall see throughout this thesis the leaks by Edward Snowden are giving us unprecedented insight into US cyber policy. Further the US government has come under increasing legal pressure to declassify documents relating to cyber security issues providing us with even more insight.

**From the 2003 National Strategy to Secure Cyberspace to the 2011 International Strategy for Cyberspace**

The growing importance of cyberspace has prompted many countries and international organisations to devise policies concerning cyber security. The US published its first substantial public policy document on the matter in 2003 when it released the *National Strategy to Secure Cyberspace*. However, the military and intelligence agencies have been interested in cyberspace for much longer. The development of cyber capabilities started almost a decade earlier with the National Defence University graduating first class of officers trained to
lead in cyber war in 1995 (Clarke, Knake 2012:34). Because the cyber domain was seen as a significant new area of operations by the different branches of the armed forces and the intelligence agencies, competition over who would control operations in it emerged between them (ibid 35). By 2002 this resulted in a compromise agreement to integrated cyber command into STRATCOM (strategic command). This grouped cyber command together with nuclear and space command making it a centralised responsibility (ibid 36). Simultaneously, the decision was made to make the director of the NSA a ‘dual hatted’ four-star general in order to make the capabilities developed within the NSA available to the Pentagon. This allowed the different branches of the military to develop their own cyber units while profiting from the NSA’s expertise, which were more advanced than those of the military. Crucially it also ensured that the NSA would not be taking on a combat role as it is prohibited to do so by US law (ibid 39).

Interestingly, while the US has worked hard to develop cyber capabilities there has never been a serious effort at cyber arms control. Russia did propose such an agreement during the Clinton administration yet it was rejected outright as it was seen as a mere propaganda ploy. Since that time the US has single handily blocked proposals that propose controls on cyber arms (Clarke, Knake 2010:220). While this position may seem dogmatic it is the result of legitimate concerns. In 2011 for example China, Russia, Tajikistan, and Uzbekistan submitted a letter to the UN General Assembly proposing an International Code of Conduct for Information Security (A/66/359 2011). In the US the proposal was viewed with suspicion as it contained clauses that could be used to limit freedom of speech (Farnsworth 2011). It proposed that information and communication technologies should not be used to carry out “hostile activities or acts of aggression”. This included encouraging the proliferation of “information weapons or related technologies”. The proposal went on to emphasise that states have the right to protect their “information space” in accordance with their domestic laws (A/66/359 2011:4). The US government viewed this as an attempt to legitimise the placing of restrictions on sites such as Twitter and Facebook, which could be interpreted as ‘information weapons’ under the proposal (Farnsworth 2011). Nonetheless, while the US had legitimate concerns
the letter did raise well-founded issues. The proposal recognised that it is important to establish norms of behaviour in cyberspace that insure international stability and security. Moreover, it recognised that the developing of cyber capabilities may be detrimental to that. Until now however, there are no agreements that seek to limit the proliferation or development of cyber weapons.

While the US is weary of any cyber arms control agreements it has been cooperating on other fronts. As Stevens observed by examining the diplomacy surrounding US cyber security the US has worked on the development of cyber weapons since the 1990s while it has simultaneously played a role as a norm entrepreneur (2012:148). This focus on norms is outlined in the 2011 *International Strategy for Cyberspace*. This document sets out a vision were the US would rely on international engagement to build an ‘environment of expectations’. Within such an environment norms define acceptable behaviour and create stability (ibid 9). According to this policy document the norms the US is aiming to promote are freedom of expression, respect for intellectual property, privacy, protection from crime, and the states right to self-defence (ibid 10).

The most fruitful area of cooperation has been related to the fight against cyber crime. The Budapest Convention is instrumental in this area and has been ratified by the US and 44 other states. This convention aims to increase cooperation among law enforcement agencies were the investigation and prosecution of cyber crimes is concerned. It does so through various mechanisms most notably it provides a model for countries to update their laws with the aim of harmonising them in order to facilitate the sharing of evidence and extradition (2011:19). On issues more closely related to national security the US has worked with NATO and its member states to enhance their situational awareness and their collective defence capacity. Meanwhile, it has also pursued general policy of coordination and greater exchange of information to lessen the chances of misperception (ibid 21).
From the sources we have examined so far we are able to uncover that the US has offensive cyber capabilities and that these have been integrated into the military and intelligence agencies. However, there is much, which documents such as the *National Strategy to Secure Cyberspace* and the *International Strategy for Cyberspace* do not reveal. These documents only ever refer to any offensive capabilities in vague terms. The *International Strategy for Cyberspace* for instance makes frequent reference to deterrence and specifically identifies the right of the US to defend itself in cyberspace while avoiding any concrete discussion on how these measures may be put into practice. The document never reveals how or when such capabilities may be used.

**NSPD 54 and PPD 20**

Luckily then, we have recently gained access to two important documents related to cyber security issued by the White House which were previously unavailable. These give us more insight into US policy, especially where the use of cyber weapons is concerned. These documents are the declassified National Security Presidential Directive 54 (NSPD 54) and the leaked Presidential Policy Directive 20 (PPD20). Together these documents provide us with crucial insights into US cyber policy, which is particularly secretive.

NSPD 54 was drawn up in 2008 and is the legal text that underpins the Comprehensive National Security Initiative initiated by president Bush. In 2009 the White House described this initiative as a purely defensive program intended to protect critical infrastructure and networks belonging to the federal government from intrusion. Yet, after NSPD 54 was declassified in June 2014 it became clear that the program empowered government agencies to coordinate offensive actions against cyber threats (EPIC). NSPD 54 states: “The Secretaries of State, Defense, and Homeland Security, the Attorney General, and the DNI shall submit to the Assistant to the President for National Security Affairs and the Assistant to the president for Homeland Security and Counterterrorism a joint plan for the coordination and application of offensive capabilities to defend U.S.
information systems (2008:14)”. Thus, it became apparent that it is not just the intelligence agencies and the military that are involved were offensive cyber capabilities are concerned but that other agencies have a coordinating role. Also interesting is the frank language the document used to describe the cyber threats the US is facing. It directed the heads of all executive agencies to “assume that adversaries have the capability and intent to either capture the data or disrupt mission applications residing on unclassified networks (ibid 14)”. This indicates a high level of competition with states constantly compromising each other’s systems.

The document shows that the DHS has the responsibility to lead the “national effort to protect, defend, and reduce vulnerabilities of federal systems” while it is also tasked with the protection of critical infrastructure from cyber threats (2008:5). However, within this declassified and redacted version of the document, nothing of substance is revealed about any cyber capabilities the US may have or how and when it plans to use them. It merely states that, the “the United States must maintain unrestricted access to and use of cyberspace” for a variety of purposes and that cyberspace has enabled “huge gains” in several areas including military capabilities (2008:2). To learn more about the role the cyber weapons play we must turn to PPD 20, which was leaked by Edward Snowden.

PPD 20 is much more specific than NSPD 54, it “pertains to cyber operations, including those that support or enable kinetic, information, or other types of operations” (2012:4). In other words, PPD 20 pertains to cyber operations including those that involve the use of cyber weapons. This document is of particular interest to this thesis as it sheds light on a policy area, which the US government has been extremely secretive about. It is impossible to gain the level of insight revealed by PPD 20 when relying on officially released documents. Edward Snowden himself stressed the importance of PPD 20 when he commented: “on cyber operations the government’s public position is that we still lack a policy framework. This too is a lie. There is a detailed policy framework, a kind of martial law for Cyber Operations created by the White
House. It is called “Presidential Policy Directive 20” (Piotras 2014:10:35-10:54). Thus, the contents of PPD 20 provide this thesis with a window into US policy concerning the use of cyber weapons. Additionally, we will also be able to deduce how top-level policy makers think about the use of offensive cyber capabilities.

The document illustrates that US policy makers understand that the use of cyber weapons may have negative consequences yet, simultaneously they seem set on furthering the development of offensive capabilities as they see these as having great potential. The authors of PPD 20 clearly view “Offensive Cyber Effects Operations” or OCEO as having great potential. They write “OCEO can offer unique and unconventional capabilities to advance U.S. national objectives with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging [9]”. The document then proceeds to instruct the United States Government to identify potential targets on which to use its cyber capabilities9 (ibid 9). Further, PPD 20 also states that the US reserves the right to use offensive cyber capabilities in response “to circumstances when network defence or law enforcement measures are insufficient or cannot be put in place in time to mitigate malicious activity” (ibid 10). These statements give us some interesting insight into how US policy makers think about the use of offense cyber capabilities. First, they view offensive cyber capabilities as an essential tool and which they intend to integrate these into wider military, and political strategy. Second, they see them as useful not only militarily but are also willing to deploy them when a law enforcement approach is deemed insufficient to deal with malicious activity. Third, the fact that PPD 20 instructs the

---

9 This quote is an exert from correspondence between Laura Piotras and Edward Snowden. Laura Piotras is a documentary filmmaker and the first person Snowden contacted about the material he wanted to leak. Piotras is the director of the documentary "Citizenfour" which features excerpts from their first correspondences. Transcripts of the messages are also available, see Greenberg 2014.

9 PPD 20 states: "The United States Government shall identify potential targets of national importance where OCEO [Offensive Cyber Effects Operations] can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive (2012:9)".
Government to identify potential targets signifies that the integration of offensive capabilities into policy and strategy is at an early stage.

However, while the authors of PPD 20 have high expectations of what can be achieved with these new capabilities it is also clear that they understand that there are risks associated with their use. PPD 20 clearly states that before any cyber operation is launched careful consideration should be given to the risk involved. It draws particular attention to “the risk of (including economic), impact on the security and stability of the Internet, and political gain or loss to include impact on (including internet governance), and the establishment of unwelcome norms of international behaviour” (2012:20). Thus, any offensive actions carried out by the US in cyberspace have to be mindful of the “stability and security of the Internet” while avoiding the establishment of “unwelcome norms”. PPD20 then proceeds to specifically outline the “safe and reliable functioning of “critical infrastructure” as a matter of national interest (2012:3). This shows that policy makers understand that using offensive capabilities may have affects relating to norms of acceptable behaviour as well as the stability and functioning of cyberspace.

Together NSPD 23, PPD 20 and the earlier discussed cyber security strategies show that the US has two main goals were cyber security is concerned: 1) the protection of critical infrastructure and 2) maintaining access to a functioning and stable cyberspace where norms persist which are commensurate with those the US is promoting. The documents also show that US policy makers view their new offensive cyber capabilities as a tool, which has high potential and are willing to use. However, they also realise that using offensive cyber capabilities can have negative consequences regarding the technical functioning and stability of cyberspace as well as negative normative consequences. In the next section it will become more apparent why there are negative consequences associated with the development of cyber weapons. We will also start to analyse why it is questionable it developing them helps to achieve the goals the US has set for itself or to what extent these policy goals themselves are conflicting.
II - State of the art

This section will begin by showing how this thesis intends to contribute to the most recent literature on cyber security with its focus on the possible trade off between cooperation and proliferation. Subsequently the discussion will move on to outline some of the research done on the securitization of cyberspace. Examining how discourses surrounding cyber security have developed will provide us an overview of the wider context in the topic of this thesis is situated. Next, this chapter will proceed to outline three different conceptualisations or theories of cyberspace that relate to the use of cyber weapons and cooperation to secure it. Our investigation will focus on three such positions, which have been designated as cyber deterrence, cyber power, and the cyber ecosystem approach. While these theoretical positions are not entirely incompatible or separate for the purposes of this chapter they will be presented as three distinct theories as they do have their own set of underlying assumptions. Drawing out the differences between them will allow us to focus our attention on explaining why the policy recommendations being proposed by each these positions are so different. As we shall see throughout the chapter however, US cyber policy contains an interesting combination of elements from each of the conceptualisations. This calls into question if US policy makers have ever seriously considered the possible trade-off between cooperation and proliferation.

Researching the Trade-Off

Previously there has been some research that has focused on trade-offs associated with cyber security one example is Van Eeten and Bauer 2009 while another is Dunn Cavelty 2014. This section will provide a quick overview of these papers to illustrate how the focus on cyber weapons versus cooperation of
this thesis is what makes it unique. In 2009 Van Eeten and Bauer (assuming a rational actor model) pointed out that the decisions by individual users, as well as businesses and internet service providers regarding cyber security are the result of cost benefit analysis. In their paper they argue that the incentives for them to implement security measures that reflect the true cost to society are absent. The result is market failure with the actual costs being passed on to society in the form of negative externalities; in this case a less secure computing environment (2009:223). By this reasoning any solution to the resulting insecurity will have to include the re-alignment of incentives. To achieve this both the costs and benefits of security investment have to be borne by the parties involved (2009:229).

Van Eeten and Bauer further argue that such cost benefit analysis can also be applied from a national security perspective. Were national security is concerned they argue, the emphasis is on potential damage, instead of actual damage which most daily users of cyberspace are concerned with (2009:229). Framed in this way the question this thesis seeks to answer would be if the cost of developing cyber weapons to the US outweigh the benefits. Van Eeten and Bauer however, also observed that framing the issue in terms of national security tends to subordinate the interest of everyday users (2009:230). Framing the problem in terms of a state security versus human security perspective Dunn Cavelty has made a similar observation. However, her argument goes further claiming that the way in which cyber security is currently approached under produces security for both states and users. Her argument is that current in-security in cyberspace is not due to a skewed incentive structure but the result of the effort governments have put into offensive cyber capabilities. To be successful at developing these capabilities they stockpile zero-days making cyberspace fundamentally less secure for both states and users. The common ground states and users have she argues are vulnerabilities. If users and states work together to focus their efforts on reducing these vulnerabilities the result will be a

---

Michel van Eeten is Professor Governance of Cybersecurity at Delft University of Technology. He focuses specifically on producing incident data to form a picture of how markets deal with cyber security and risk.
fundamentally more secure cyberspace instead of one that is exploitable (2014:11).

What the research conducted by Van Eeten and Bauer shows is that states and users may have very different security concerns. Dunn Cavelty meanwhile shows that the development of offensive cyber capabilities may undermine the overall level of security in cyberspace. The focus of this thesis however, is different as it investigates if the developing of offensive cyber capabilities produces a situation that is detrimental to prospects for cooperation. As we saw earlier the US is developing offensive cyber capabilities and stockpiling zero-days in order to facilitate the development of such capabilities and as we shall see in more detail later the US is certainly not cooperating with others to the fullest degree possible in the area of cyber security. Is the lack of cooperation we are witnessing on the part of the US the result of its efforts to produce cyber weapons?

The securitisation of cyberspace and computer security

Work done on the securitization of cyberspace and computer security is of interest to this thesis as it shows how these have attracted increasing attention from policy makers and how they have become been articulated as a “security problem”. Differentiating different discourses provides us with a wider context in which to place our discussion about cyber weapons while different discursive rationales underpinning the logic of securitization will become apparent. As Hellen Nissenbaum observed in a 2005 paper there are two overlapping conceptions of security relating to the vulnerability of computers to attack. The first and oldest perspective is the “technical computer security” perspective while the “cyber security” is a more recent approach. Technical computer security is a technical field and has been the preserve of technical experts and computer scientist. Cyber security meanwhile links computer security to traditional conceptions of national security and is articulated by policy makers and corporate heads for example (63). By comparing these two discourses Nissenbaum showed that there has been a move from “technical computer
security” to “cyber security”. Cyberspace she showed has become portrayed as a “new medium” which can be used for a variety of malicious purposes including an attack on the US (ibid 73). This notion of vulnerability was subsequently amplified by high-level policy makers who dramatically raised concerns about the possibility of catastrophic and crippling cyber attacks (ibid 67). Indeed more recent research analyzing the discourse surrounding cyber security has found that it is still portrayed in this manner. Bernard-Wills and Ashenden for example concluded that the cyber security discourse is based around the premise that cyberspace “is ungovernable, unknowable, makes us vulnerable, is inevitably threatening, and is inhabited by a range of threatening and hostile actors on which it confers a number of advantages” (2012:116). Crucially, it is claimed that the targets of the cyber threats are not limited to the military sphere. Rather, malicious actors could use cyberspace to threaten a wide scope of entities including “critical societal infrastructures, including utilities, banking, government administration, education, healthcare, manufacturing, and communications media” (Nissenbaum 2005:64).

Such a representation of threat is very different to the way it is viewed by those approaching it from the technical computer security perspective. Within this perspective the threat is not always assumed to be severe or even existential. Rather, it accepts that the harm resulting from threats can vary from negligible to severe. Furthermore, Nissenbaum observed that those coming from a technical computer security background focus on the individual nodes of network security i.e. “people, agents, institutions” (2005:69). Therefore they are dealing with different referent objects to those who analyse from the cyber security perspective where the referent object is the state or the nation (ibid 69).

Subsequently, this research on the discourse surrounding cyber security has been developed into a more comprehensive theoretical framework. To achieve this Nissenbaum and Hassen have explored more deeply how cyber security has become securitised. Central to their theory is the claim that in security studies discourses are most accurately portrayed as “constellations of connected referent objects” (2009:1171). In the case of cyber security the referent objects
of “the network” and “the individual” are not significant in themselves but gain their significance by being linked to collective referent objects such as the national, the regime or state, society, and the economy. Within cyber security discourse therefore the linking of these referent objects is crucial to the securitization process. This linking process makes it possible to frame collective referent objects as being threatened (ibid 1115). Most significantly their research showed that cyber security involves a double securitizing move. The issue is taken from the political into the securitized and simultaneously from the political to into the technified (see footnote 10) (Nissenbaum Hassen 2009: 1172). It is extremely important to be aware of this as it illustrates that while it is necessary to have a sound technical understanding of the matters which relate to what we are analysing we should not let technical

Hypersecuritization discourses represent a threat as severe enough to justify far reaching counter measures. In cyber security discourse this often involves evoking the possibility of severe disaster scenarios in which cascading effects cause harm to society, the economy, and the military. Aiding the likelihood of hypersecritization in cyber security is the fact that it is shrouded in ambiguity, as there are no real world examples of these disaster scenarios allowing securitizing actors to argue that the stakes are high and that their warnings should not be ignored (ibid 1164).

Everyday security practices meanwhile refer to the way in which securitizing actors are able to include private organizations and businesses to join in their discourse to engage “normal” people (ibid 1165). These everyday security practices are important, as they are a way for securitizing actors to make their disaster scenarios to something normal people can relate to. By drawing banks into their discourse, securitizing actors for example are able to articulate that everyone with a bank account is vulnerable not just people who own a computer. Crating such links enables the rationale that makes the leap constituting threats to the network as threats to society (ibid 1165).

Third technification is an important method of securitization in cyber security. As touched upon earlier technical computer experts enjoy a high level of epistemic legitimacy as securitizing actors. Because cyber security is a highly technical and quickly evolving field computer experts are able to speak with authority about the unknown or “the possible”. In doing so they are often assumed to be politically and normatively neutral. This produces a situation when the logic of securitization can become technified. Cyber security becomes the preserve of technical experts as it is presumed that the subject is too technical for the general public or most politicians to grasp. This technification of cyber security in reality however, is not apolitical because it can is used by securitizing actors to depoliticize and legitimise their discourses (ibid 1168).
details get in the way of our investigation. Meanwhile we should not view
technical discourses as politically and normatively neutral. In fact, it has been
shown that cyber security discourse full of metaphors which are simple ways to
explain technically difficult concepts but are also important perception shapers.
As we shall see in more detail cyberspace is represented in a variety of ways as an
organic, inter-connected, and self-healing ecosystem but also as a space upon
which the state must establish control and order (Dunn Cavelty 2013:118).
Currently, Dunn Cavelty argues that the first is taking precedence over the
second while the cyber threat is also increasingly being represented as a
strategic threat. This threat representation she argues makes it more natural for
the military to become involved when it comes to ensuring the stability of
cyberspace (ibid 119). This observation provides us with an interesting point of
departure when analysing the US policy documents that have recently become
available, as they should corroborate this finding. In addition if PPD 20 and NSPD
54 confirm what Dunn Cavelty argues then we can assess if and how policy
makers view the trade-off relating to vulnerabilities.

Cyber deterrence

Especially after the ‘cyberwars’ in Estonia (2007) and Georgia (2008) there has
been a growing body of cyber deterrence theory (Stevens 2012:140). Goodman
for example sees states as the most important actors in cyberspace because they
have the greatest capacity to develop cyber capabilities. Therefore, he argues
states should be the main unit of analysis when analysing cyberspace. Crucially,
in his view, offensive capabilities are the only tool available to ensure national
security (2010:105). He comes to this conclusion because he contends that
interdependence and counter-productivity (the ability to convince an attacker
that a tactically successful attack has negative strategic consequences) have not
proven themselves in the cyber domain. This leaves defenders with the option of
prevention (the ability to foil an attack through defensive measures). However,
he argues that it is questionable if this is possible in cyberspace (2010:107).
Therefore, he explains, the best option for states is to develop offensive cyber
capabilities in order develop a deterrent posture, central to which is the ability to punish potential attackers through retaliation (2010:108).

There are many analyst however, who have serious doubts about the utility of a deterrence strategy for cyberspace. A 2009 study by Libicki entitled *Cyberdeterrence and Cyber War* is an example. It was commissioned by the US Air Force to determine the limits of power in cyberspace. The paper argues that using a deterrence strategy to effectively prevent cyber attack would be 'highly problematic'. Attribution, damage assessment, and finding the motives of an attacker could all be problematic (ibid 176). Further, it emphasised that it is unclear how retaliation works in cyberspace (ibid 178). How can a state retaliate if the attacker is able to maintain deniability? Also worth consideration is the fact that much of the infrastructure cyberspace is build on is civilian; what would constitute a legitimate target? The study concludes that using cyber weapons to retaliate should be a last resort (ibid 178).

What is perhaps most problematic about Goodman’s theorising about cyber deterrence is its state-centric nature. Joseph Nye for example contends that a cyber 9/11 is much more likely than a cyber Pearl Harbour (2011:22). While Goodman argues that states should be able to deter one another non-state actors fall outside of the scope of this analysis. It is very unlikely however, that non-state actors can be deterred. Further, it has been argued that the focus on state security has produced a situation were the security of individuals and the overall level of security of cyberspace is undermined (Dunn Cavelty 2014:1).

Although the concept of cyber deterrence has its critics it is important to understand cyber deterrence theory and the rationale behind it, as it is an important component of US cyber strategy. From PPD 20 it becomes apparent that the US views cyberspace as medium through which it can exercise a deterrence capability. The document states “the US has an abiding interest in the developing and maintaining use of cyberspace as an integral part of US national capabilities to collect intelligence and to deter, deny, or defeat any adversary that seeks to harm the US” (4:2012). It certainly seems clear that the US is set on
developing offensive capabilities and that it is not hedging its bets on relying solely on defensive measures. It will be interesting therefore to investigate if US policy makers agree with Goodman that prevention is impossible and that interdependence and counter-productivity have not take hold in the cyber domain as such axioms would leave little room for security cooperation. Subsequently, we can then ask if this situation has come about as the result of the proliferation of cyber weapons or if it has a different cause.

**Cyber power**

Goodman’s claim that interdependence has not been sufficiently tested in cyberspace is interesting but can be framed in a more nuanced manner. Nye for example has asked where, to what degree, and between which actors interdependence exists. Viewed through this lens actors in cyberspace find themselves in a situation of simultaneous interdependence and vulnerability (2011:24). This is also how Kuehl who lectures at the National Defence University in the US views cyberspace. He has focused on the analysis of cyber power i.e. how to leverage power in cyberspace. Although this approach is still state centric, discussion within the cyber power literature is much broader than with cyber deterrence theory. Kuehl characterises cyberspace as providing opportunities to exploit new capabilities while simultaneously also exposing the US to new vulnerabilities (2009:18). In the sense that cyberspace is a domain of warfare he views it from the same perspective as the air and sea domains, where nations invest in capabilities with the expectation that investment will help attain larger strategic goals (2009:10). This essentially boils the decision of whether or not to develop cyber weapons down to a cost benefit calculation while keeping the state as the main unit of analysis.

Those who analyse cyber power however, in contrast to cyber deterrence theorist, view non-state actors as having a significant role. Klimburg, who also theorises about the application of cyber power adds that because a large portion of the states cyber capabilities may lie outside of its direct control it has to find
ways to induce non-state actors to cooperate with it (2011:43). Cyber power theorists see the relationship between governments and non-state actors as crucial to attaining common objectives (Klimburg 2011:43). Within this context cyber power theory views the development of cyber weapons as a way to achieve broader military, economic, and political goals. Like in the sea and air domains Kuehl argues that power in the cyber domain is not attained by having physical control over the domain but rather by controlling how the domain is used (2009:15).

As we saw earlier such a focus on norms of behaviour is also found in US cyber policy. Thus, while it has a deterrent component and sets out to develop cyber weapons top level policy makers also recognise that the actions of the US shape norms of behaviour in cyberspace. Further, we also saw that the US has worked to integrate its cyber capabilities into a wider strategy were these can be deployed to maximise the effectiveness of other capabilities or policies. Such an approach is certainly commensurate with the way in which cyber power theorists expect to gain most the utility from these capabilities. However, US policy does not contain any major elements that indicate that it is wiling to cooperate with non-state actors to improve cyber security. Here one could envision states working together with anti-virus companies for example to fix vulnerabilities. However, we have recently learned that the NSA has been doing the opposite by spying on anti-virus companies in order to find ways to subvert the software they make allowing them to plant malware without detection (Zetter 2015). For our purposes then it will be important to understand why the NSA is engaging in such practices and if the development of cyber weapons are the underlying reason.

Cyberspace as an ecosystem

Typically ecosystem theorist view cyberspace as an ecosystem and focus on building resilience to provide security. In this line of thinking the state is not that is the referent object, rather, it is the ecosystem of connected devises that needs
to be kept secure and healthy. Exemplary of this approach is a 2011 paper published by the DHS which the argument that any malware is detrimental to the overall functioning of cyberspace. The paper envisions the creation of a fundamentally more secure environment by enabling cyber devices to communicate with each other about threats. This would allow for a dynamic approach in which preventive and defensive measures would be taken automatically. While this solution is highly technical and it does provide an alternative to the more national security oriented approaches. Such a system would harness the power that is distributed among participants to ensure a safe and secure environment. This approach minimises the role of the state while concentrating on generating cooperation between individual users (2011:2)\textsuperscript{12}. Such an approach then puts a strong emphasis on cooperation and views any malware or stockpiling of vulnerabilities as detrimental to the functioning of cyberspace.

In their book \textit{CyberSecurity and Cyberwar} Singer and Friedman also conceptualise of cyberspace as an ecosystem arguing that it can be viewed as containing a multitude of actors each of which has different interests and capabilities (2014:178)\textsuperscript{1314}. Crucially, they contend that it is not necessary to develop cyber weapons to secure cyberspace. In their piece \textit{Cult of the Cyber Offensive} (as in their book) they argue that the focus within the US military establishment on creating offensive cyber capabilities is counterproductive. Departing from balance of power thinking they contend that it is impossible to

\textsuperscript{12}According to the authors of the study a minimum of 30 to 35 per cent of devices would need to cooperate for the system to be effective (ibid 7). While such solutions may seem like a fiction to some, it is being taken seriously. Currently DARPA (Defence Advanced Research Projects Agency) is encouraging the development of such systems. By offering price money through its Grand Cyber Challenge it hopes to spur the development of systems that are able to automatically detect malware (DARPA 2014).

\textsuperscript{13}Peter Singer is a strategist and senior fellow at the New American Foundation. He is an expert on 21st century warfare and has consulted for the US military, Defense Intelligence Agency, as well as the Federal Bureau of Investigation. Before his current position he served as the Director of the Centre for 21st Century Security at the Brookings Institution. Alan Friedman is both a technologist and policy analyst. He is a Visiting Scholar at the Cyber Security Policy Research Institute at Georgetown Washington University.

\textsuperscript{14}Libicki has similarly argued that the military should focus on designing systems, which can continue to function while under attack (2003:163).
speak of any polarity in cyberspace were one side is trying to gain an advantage over the other. Instead, as proposed in the DHS paper, they would like to see more emphasis on building resilient systems that can rapidly recover when attacked (2014). It should be pointed out though, that while Singer and Friedman conceptualise of cyberspace as an ecosystem, which is not demarcated by borders or physical geography, they do envision an important role for the state. The physical infrastructure cyberspace is built upon after all is either located on the territory of a state or operated by companies that are tied to them. Further, the users of cyberspace cannot be taken in isolation but are subject to laws that regulate how they may use cyberspace (Singer, Friedman 2014:182).

Again when it comes to the ecosystem approach we are able to identify elements of it in US cyber policy. Within the US government, the ecosystem approach is most prominently articulated by the DHS. In its 2014 quadrennial review for example it states “Cybersecurity is a shared responsibility in which each of us has a role” (45). Then the document continues to highlight the need to “develop a strong team of cybersecurity professionals to design, build, and operate robust technology to reduce exploitable weaknesses” emphasizing that “the cyber ecosystem also needs self mitigating and self healing systems to address threats at machine speed” (45). However, NSPD 54 and PPD 20 do not refer to cyberspace as an ecosystem our earlier examination of these documents did show that maintaining access to a functioning and stable cyberspace is one of the main policy objectives of US cyber policy. Therefore, US cyber policy does conceptualise cyberspace as a single interconnected space. It also views cyberspace as borderless, PPD 20 notes that cyber operations “even for subtle or clandestine operations, may generate cyber effects in locations other than the intended target, with potential unintended or collateral consequences that may affect U.S. national interests in many locations” (2012:6).

The ecosystem approach then views cyberspace as a single inter-connected space while it turns our attention to vulnerability reduction and cooperation among users as the best way to provide security. While the DHS certainly supports such an approach we see little of it when it comes to international
cyber policy. The only aspect of the ecosystem approach high-level documents such as PPD 20 and NSPD 54 contain is the conceptualization of cyberspace as a single borderless space. Somewhere the focus on vulnerabilities which the DHS advocates seems to get in favor of more militaristic approaches. Whether or not policy makers have ever seriously considered the possible tradeoff when they chose one over the other is something we can investigate further.

**The potential for cooperation**

While there is agreement that norms of behaviour are important, observers are witnessing norms shifting towards the development of cyber weapons. Research by Stevens for instance concludes that, while there have been calls for the non-use of cyber weapons, it is more likely that norms for their will emerge. He argues, that the spread of military cyber capabilities may indicate “that states see little utility in global cyberspace agreements to deter or prevent conflicts or are attempting to develop punitive capabilities” (ibid 165). Similarly, Mayer also observes a lack of international cooperation around cyber security issues and has called for the “diplomacy to catch up with developments within the national security establishments” (2012:19). While Renard, like Meyer, is optimistic about the potential for cooperation he shows that between EU member states cyber security largely remains an “almost exclusively national prerogative” (2014:13). He also observes that there is much potential for cooperation on cyber security issues between the EU and the US, but the revelations by Edward Snowden have severely damaged trust between the two parties (ibid 22). Rantapelkonen and Kantola also raise the issue of trust; they argue that the expertise to improve cyber security already exist what is missing, they argue, is the “right attitude” (2013:33).

When it comes to cyber weapons however, there are many practical considerations that make security cooperation difficult. Geers brings some of
these to light when he compares cyber attack tools to nuclear weapons. In comparison they are easy to acquire, deploy, and hide. The training of hackers does not represent a substantial hurdle either. Conveniently, code can be developed in a closed environment and then stored on a flash drive making it almost impossible to find. Similarly testing can also be done within a controlled environment or on the internet while the attacker remains anonymous. This makes controlling the spread of malware extremely difficult. Last Geers points out that defining exactly what malicious code is can be difficult. As he points out, the basic design of the neutron bomb has remained the same since the 1950s while the design of malicious code changes constantly. These factors make a treaty similar to the Non-Proliferation Treaty for cyber weapons unlikely.

Nonetheless, there is some reason for optimism. The Nordic countries for instance have started sharing classified information between Computer Emergency Response Teams or CERT teams. The way in which Japan has approached cyber security is also instructive. Contrary to the US its cyber security policies have commercial rather than military and intelligence-driven origins. As a result it has shown leadership with its focus on cyber hygiene and facilitating international collaboration. It plays a leading role within the Asia Pacific Computer Emergency Response Team, which provides a platform for regional cooperation. Like Singer and Friedman the Chair of APCERT, Yurie Ito, envisions cyberspace as a shared recourse, an “ecosystem [which] must react to disruptive forces”. The US however, has taken the lead in creating cyber weapons has not been cooperating with others to the same extent. Here, it is important to consider as Vacca points out that the way the US Navy and Air Force think about cyber security has important implications for how related issues are framed and policy options are evaluated. In light of the way in which cyber security has been approached elsewhere it is possible that the way in which the US has

---

15 Kenneth Geers has spent more than 20 years working for the US government. He has held positions at the NSA, NATP, and NCIS (Naval Criminal Investigative Service). At the time of writing he was the U.S. representative at the NATO Cooperative Centre for Excellence in Estonia.
favoured the development of cyber weapons has skewed its overarching strategy.

**Assumptions and impact on policy recommendations**

To conclude this section we are now able to compare the underlying assumptions of the approaches discussed. First, cyber deterrence theory was analysed. This perspective is the most state centric of the approaches and views the cyber realm as one of competition where the concepts of counter productivity and interdependence have not take hold. This is what leads theorists such as Goodman to argue for the developing of cyber weapons and a deterrence based strategy of cyber security. While its assumption that states are the most powerful actors in cyberspace is probably correct the omission of non-state actors is problematic for any analysis. As we have seen earlier cyber capabilities have not just proliferated among states but also among non-state actors.

Both cyber deterrence theorist and cyber power theorist start their analysis from a perspective were it is a given that states will develop cyber weapons. However cyber power theorist emphasise the importance of norms and controlling how cyberspace is used. They come to this conclusion by viewing cyberspace as a space in which interdependence and vulnerability exist simultaneously while broadening the scope of analysis to non-state actors. However, their approach is still relatively traditional as their emphasis is limited to state security leaving aside human security considerations.

This is where those who conceptualise cyberspace as an ecosystem diverge. While most of these theorists do agree that the state plays an important role, the focus is on creating resilience. This is largely achieved by cooperation below the governmental level through cooperation among users, the anti-virus industry, and CERT teams while securing the devices connected to cyberspace, and making
those devices communicate amongst themselves enabling them to react to disruptive forces. Power is viewed as diffuse instead of centralised through the lens of the ecosystem approach. Here cyberspace itself becomes the referent object which leads to the view any malware including cyber weapons are detrimental to the overall health of the system.

Throughout this chapter we found that US cyber policies contain elements of each of the three conceptualisations. It is clear however that these elements sit alongside one another rather uncomfortably. PPD 20 makes reference to deterrence and has a clear focus on developing cyber capabilities. These elements are compatible with the cyber deterrence approach. As the cyber power approach recommends however it also plans to integrate cyber capabilities to be used with other instruments of power while there is also awareness among top-level policy makers that it is important for the US to promote certain norms of behaviour in cyberspace. Further, within PPD 20 we find no references to cyberspace as a bordered or national space, rather the focus is on the location of the effects caused by cyber operations. Within DHS documents in particular however cyberspace is viewed as an ecosystem taking an approach to cyber security that views malware as detrimental to the health of the system. Yet, when we turn to international cyber policy documents such views remain absent.

Therefore we can view US cyber policy as a synthesis of these approaches. On the one hand it views cyberspace as a borderless space yet departing from cyber ecosystem theory it views power as centralised and does not view malware as detrimental per se. Instead policy makers see the potential of offensive cyber capabilities as an instrument of national power as cyber power and cyber deterrence theorist do. Simultaneously US policy makers see some degree of interdependence in cyberspace illustrated by their concerns about collateral damage. Further, we can see an aspiration to create a predictable environment through the establishment of norms. At the same time however, we are not witnessing any substantial attempts at cooperation aimed at making cyberspace
more secure which may indicate competition in this area, which could be the result of the proliferation of cyber weapons.

III - What is a cyber weapon?

Despite the growing interest among a variety of institutions in cyber security there has been a lack of conceptual clarity regarding what a cyber weapon is. It seems that it is often assumed that no formal definition is needed. The assumption seems to be that it is obvious what a weapon is and therefore what a cyber weapon is. However, defining what a cyber weapon is needs careful consideration. The Japanese government for example has contracted Fujitsu to create a virus that seeks out computers infected with malware in order to clean them (Thomson 2012). Is this anti-virus virus a cyber weapon? How should this piece of computer code be classified? We will come back to this question later.

The inability to differentiate between a weapon and a non-weapon has practical as well as political and legal implications. Before we are able to regulate the use of cyber weapons we have to be able to define what they are (Rid, McBurney 2012:11). The lack of common definitions relating to the cyber domain among states can easily cause misunderstandings making dialogue difficult (OSCE 2013:12). The recent, allegations about Russian cheating of the Intermediate-Range Nuclear Forces Treaty coming from US commentators perfectly illustrates the importance of semantics. The disagreement is in part the result of un-clarity surrounding the definition of the term ‘cruise missile’ (Lewis 2014).

Furthermore, consider, that in cyberspace as anywhere else, an armed intrusion is politically much more significant than an unarmed one (Rid, McBurney 2012:11). In general the lack of a common definition is becoming increasingly problematic as cyberspace is being militarised showing that diplomacy

---

16 The idea of a benevolent virus is not new in his 1984 paper Cohen describes how a virus could be used to save disk space by finding uncompressed files and compressing them.
The lack of definition

Thus far the definitional problem has not been approached with any urgency nor is there any consensus regarding a definition. One of the few efforts at tackling the problem has been initiated by the Organisation for Security and Cooperation in Europe (OSCE). As part of a set of confidence building measures the Permanent Council of the OSCE agreed that member states should voluntarily provide a list of the most important national terminology related to ICTs and their definitions (2013:2). However, within international organisations there have been no specific calls to define what cyber weapons are. Unfortunately, there seems to be little progress regarding the formation of international consensus on a common definition.

Currently the assumption that what a cyber weapons is needs no definition seems to be pervasive. The Tallinn Manual for example, does not define what a cyber weapon is. This is strange for a 302-page document published by a think tank connected to NATO, which set out to examine how international law is applicable to cyber war. Its glossary contains definitions for basic terms such as ‘computer’, ‘data’, ‘server’, and ‘worm’, yet the term ‘cyber weapon’ remains undefined (Schmitt et al 260-262). National cyber strategies also completely lack definitions of the term ‘cyber weapon’. A study by the Organisation for Economic Cooperation and Development (OECD) that analyses 10 different national cyber strategies shows that these strategies are mainly concerned with identifying new sources of threat and the motives behind them. States are strongly viewed as emerging sources of cyber threat but so are ‘hacktivist’, organised criminals, and terrorist. Motivations include espionage, financial gain, and spreading propaganda. Many national strategies also like to differentiate between traditional and non-traditional sources of threat (2012:16). Yet, they do not define what cyber weapons are even though military institutions are investing in
offensive cyber capabilities. This confronts us with a situation where for the purposes of this thesis we have to look for sources that will help us to define conceptually what a cyber weapon is which may not do so directly.

Towards a definition

Presidential Policy Directive 20 comes closer than any publicly available government document to defining what a cyber weapon is when it discusses policy relating to ‘Offensive Cyber Effects Operations’ (2012:3, 9). However, this term is quite broad and is used to describe certain capabilities the US has. It does not provide us with a way in which to differentiate between malware that is a cyber weapon and malware that is not. In order to work towards a definition for the term cyber weapon, looking at a general definition for the term ‘weapon’ is useful. The Manual on International Law Applicable to Air and Missile Warfare produced by a group of experts for the Program on Humanitarian Policy and Conflict Research at Harvard University contains such a definition (2009:iii)17. It defines a ‘weapon’ as a “means of warfare used in combat operations, including a gun, missile bomb or other munitions that is capable of causing either (i) injury to, or death of persons; (ii) damage to, or destruction of, objects” (ibid:6). Means of warfare are defined as “weapons, weapon systems or platforms employed for the purposes of attack” (ibid:4). A weapon then can be defined as a means of attack that causes harm.

For a more precise definition of what a cyber weapon is however we can turn to an academic source. Within the literature Rid and McBurney have put forward one of the only definitions18. They define a cyber weapon as “Computer

---

17 The document was created as a restatement of existing international law to promote practical understanding.
18 The only other definition from academic sources I could find was in a paper, which attempts to define a cyber weapon in the context of war by Stefano Mele (2013). However, it is rather convoluted. Therefore I will not examine it. Mele defines a cyber weapon as: “A part of equipment, a device or any set of computer instructions used in a conflict among actors, both National and non-National, with the purpose of causing, even indirectly, a physical damage to equipment or people, or rather of sabotaging or
code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings” (2012:7). While this definition seems sound it is worth taking a closer look at the Tallinn manual. While it does not specifically define what a cyber weapon is we can infer from it how a cyber weapon may be defined in terms of international law. Examining the definitional problem from the perspective of international law is important as this thesis focuses on US policy and the cyber capabilities it is developing. As the focus is on the US which is bound to the laws of armed conflict it is important to ensure that the definition used for this thesis is one, which is at least generally applicable in that context. Using a definition which does not correspond to the way in which international law defines a weapon would mean that it had very little applicability to US policy. Therefore the Tallinn manual is useful to this discussion as it deals specifically with the use of cyberspace in war. In doing so it considers several important issues, which are specific to cyberspace from an international law perspective. Examining this document closely should give us a good idea of the criteria a piece of malware must fulfil before it can is deemed a weapon in the eyes of international law.

To begin our investigation the Tallinn manual provides us with two important terms, ‘cyber attack’ and ‘cyber operation’. A cyber operation is defined as “the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace” (Schmitt et al 2009:258). A cyber attack meanwhile is defined as “a cyber operation, whether offensive or defensive that is reasonably expected to cause injury or death to persons or destruction to objects” (ibid 106). Thus, if we take a cyber weapon to be a means of attack, we can infer that one would need a cyber weapon to use in a cyber operation to launch a cyber attack.

However, it is important to note a few nuances. First the notion of attack is not limited to the direct “release of kinetic force”, “the crux of the notion lies in the effects that are caused”. Therefore, the manipulation of a industrial control
system resulting in the release of water from a dam would be considered an attack as it would cause destruction downstream even though the system itself was not damaged (Schmitt et al 2009:106-7). Second, given the humanitarian purpose of the law of armed conflict the notion of attack can reasonably be extended to causing "serious illness and severe mental suffering that are tantamount to injury (ibid 108)". 'Mental suffering' in this case can also result from the threat of violence (ibid 108). Third, intent is important. If an attack does not do harm because it was intercepted for example it is still considered an attack. Thus, the expectation that harm may have resulted from certain actions is important (ibid 110).

Taking these points into consideration regarding how a cyber weapon should be defined in terms of international law we can already conclude that such a definition would be similar to the one proposed by Rid and McBurney. However, it does contain some aspects that have not been covered. First, their definition refers specifically to computer code. This is much more specific than the phrase 'in or by the use of cyberspace' which refers to a cyber operation. When we are specifically dealing with cyber weapons, not with cyber operations (which can include the spreading of propaganda) a definition that focuses attention on code is more accurate. Any malware after all is based on code in the same way that nuclear weapons are based on fissile material and chemical weapons are based on toxic chemicals and their precursors.

Second, the definition proposed by Rid and McBurney refers to 'living beings' not 'persons' as the Tallinn Manual does. This is the result of Rid and McBurney's definition being a more general definition not only applicable in war. However, the Tallinn Manual does make reference to “widespread, long-term, and severe damage” to the environment as possible forms of damage and therefore certainly does not disagree with the notion that something can only be classified as a weapon if it is designed to cause harm to humans (Schmidt et al 2009:107). Since this thesis is not concerned specifically with the use of cyber weapons in war a broadening the definition in this way to include 'living beings' is quite useful.
Third, the definition by Rid and McBurney refers to ‘functional harm’. The threshold for when functional harm is caused to a computer system is one area where the experts contributing to the Tallinn Manual could not come to a consensus (Schmidt et al 2009:108). Most of the experts agreed that ‘if restoration of functionality requires replacement of physical components’ it would qualify as damage (ibid 108). However, the group was split over whether the “‘damage' requirement is met in situation where functionality can be restored by reinstalling the operating system (ibid 109)”. Finally there was a small group who argued that interference with functionality also results when data restoration is required (ibid 109). Thus, the extent to which data has to be affected before it constitutes harm is unclear. For our purposes however, it is safe to say that at least some malware, which affects data, can be classified as a weapon. The debate over how much that data has to be affected before harm is done can largely be left aside. Importantly, physical violence is not always necessary before an attack can be said to have taken place19.

We should also carefully consider that there is a difference between an attack and a weapon. While a weapon can be used to attack not every attack is carried out using a weapon. As was evident from the Tallinn Manual effect and intent are important when judging if an attack has taken place. However, as Rid points out a weapon is an instrument of harm and “instrumentality means shaping an opponent’s or victim’s behaviour” (2013:53). For this reason the SQL slammer worm for example can be classified as a cyber attack but not as a cyber weapon. This worm was able to spread so rapidly that it succeeded in slowing down global internet traffic. It caused “network outages, cancelled airline flights, failures in ATM machines, and even interference with electronics” (ibid 49). However, the worm’s creator was not trying to influence behaviour by releasing it nor did he have control over it. Therefore, while SQL slammer caused

19 The cyber attack on Saudi Aramco is a good example of a cyber attack, which affected functionality by attacking data. As mentioned previously, in 2012 it was attacked by a piece of malware, which succeeded in rendering 30,000 workstations useless. It did so without doing physical harm through wiping the hard drives of the machines. The attack severely impeded the day-to-day operations of the company while also causing reputational damage (Rid 2012:61, 55).
functional damage it cannot be considered a cyber weapon (ibid 53). Thus, when determining if an attack has taken place the criteria are effect or intent. However, to determine if something is a weapon it has to meet the instrumentality criteria. A weapon has to be instrumental and be used with the intent of causing harm.

Finally we should also consider the psychological the dimension cyber weapons may have. To illustrate how important this is it is useful to examine the DDoS attack on Estonia. The attacks lasted about two weeks in April of 2007 and were sparked by controversy surrounding the removing of a soviet era war memorial. The attackers used commercial botnets to send so many bogus request that they caused the attacked servers to become overloaded and crash. Many sensitive targets such as government websites and banks were targeted. The Estonian government reacted by calling for the invocation of NATO's article 5 in order to launch a coordinated multinational counterattack (Mueller 2010:22). Within the media talk of 'cyber war' prevailed (ibid 24). The general public in Estonia also seems to have felt genuinely threatened (Rid McBurney 2012:9). Later however, after the dust had settled the Estonian government more accurately referred to the events as a 'cyber riot' (Mueller 2010:24). The vital point here is that if something is perceived and used as a threat then it is a weapon; once the threatened party stops perceiving the device used as threatening it no longer is. Therefore, any weapon has an important psychological dimension (Rid McBurney 2012:8). In the Estonian case there was initially a clear over-estimation of the aggressor. At their peak the attacks were able to take down only 58 websites simultaneously (ibid 9). A coordinated effort between Internet Service Providers and CERT teams in different countries was able to defeat the attacks (Mueller 2010:25). Nonetheless, the DDoS attacks were

---

20 A DDoS or distributed denial-of-service attack is a type of attack, which aims to make a connected device or service unavailable to its users. These types of attacks are accomplished by flooding the target with so many external communication requests causing a traffic overload making it impossible for legitimate communication to reach the target. Such attacks can be carried out using so called Botnets of computers infected with malware, which can be commanded by their operators to preform certain tasks.

21 Milton Mueller is a Professor at the Syracuse University School of Information Studies and has participated in ICANN (Internet Corporation for Assigned Names and Numbers) since 1997. As one of the founders of the Internet Governance Project his is a leading figure in the mobilization of civil society in ICANN.
certainly perceived as a threat (Rid McBurney 2012:9). Thus, DDoS attacks can be cyber weapons when they are successfully used to threaten.

It now becomes possible to distinguish between an armed and an unarmed intrusion. Being able to do so is important as the very same code can be used for different purposes. Duqu, a cyber espionage tool for instance used some of the same code as Stuxnet, which is a cyber weapon (Rid McBurney 2012:11). Analyst at CrySys lab who discovered Duqu describe it as “highly modular [allowing] sophisticated attackers to build a targeted attack from various pieces of code, similar to the way carmakers build new cars from available parts” (Bencsath, Pek, Buttyan, Felegyhazi 2011:5)22. The fact that Duqu is a cyber espionage tool and Stuxnet is a weapon is clear. In the Tallinn manual cyber espionage is defined as “any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intent of communicating it to the opposing party” (193). Duqu was designed to extract information. As Symantec writes in their report “Duqu’s purpose is to gather intelligence data and assets from entities such as industrial infrastructure and systems manufacturers”; it was intended to steal and exfiltrate data (1-2:2011). Code that is designed to spy does not intend to do harm therefore it cannot be considered a weapon.

**The anti-virus virus**

To conclude this section using the definition provided by Rid and McBurney we can now determine if the Fujiitsu anti-virus virus is a cyber weapon. First, we have to consider if the creators are intending to harm. The answer to this question is no. Although it would constitute an unauthorised intrusion its creators are not intending to do harm in any way. The anti-virus virus is not designed to do physical, functional, or mental harm or threaten; in fact it is designed to repair instead of damage. Our second consideration is

---

22 The Laboratory of Cryptography and Systems Security was founded in 2003 and is part of Budapest University of Technology and Economics. In October 2011 it discovered Duqu and released an open-source detection toolkit for the malware.
instrumentality. Is it trying to shape an opponent or victim’s behaviour? The answer to this question is yes. This virus seeks out computers that are being used as part of malicious botnets. Its goal is to make life difficult for those operating these illegal botnets by fixing the recruited computers. From the above discussion however, it is clear that a weapon has to be both instrumental and used with the intention of causing harm. Therefore, the anti-virus virus is not a weapon. Whether its use is ethical or not is another question.

IV - What is cyberspace?

This chapter will explore what cyberspace is. The first section the chapter will trace the origin of the term. It will show that the terms haphazard origins and its metaphoric nature explains how it has taken on multiple meanings. Throughout this chapter it will be important not to let the loose usage of the term hinder our analysis. Rather, the terms ubiquity should be seen as a sign of its significance not as a conceptual weakness (Strate 1999: 382). Conversely however it is also important to have an awareness of how metaphors may distort reality (Taleb 2007:75). What we should be careful of in our later analysis is not to overstretch the cyberspace metaphor. Therefore, this chapter, after dealing exploring the origins of the term ‘cyberspace’ will focus on how cyberspace functions technically. Having a basic technical understanding will allow us to appreciate what the dynamics of cyberspace are and how it compares and relates to physical space. Only with such an understanding will we be able to understand how US policy makers conceptualise of cyberspace and the impact this may have on how they view the use of cyber weapons or security cooperation. This will be examined in next chapter.

Origins
The science fiction writer William Gibson coined the ‘cyberspace’ term in 1982 deriving it from ‘cybernetics’ (Solomon 2007) (Strate 1999:382)\textsuperscript{23}. The concept of cyberspace (a virtual space) however goes beyond that of cybernetics. In his novel *Neuromancer* (1984) Gibson describes cyberspace as “A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding (Gibson 67).” In the documentary *No Maps For These Territories* Gibson explains that he made up the word because he needed to move his characters through the new space he had imagined. “I needed a buzzword... a signifier of technological change, and provide me with a narrative engine and a territory in which the narrative could take place” (Neale 2000:49:50-55:20). He further elaborates that his inspiration grew out of his observation of children playing arcade games who “wanted to reach right through the screen”. This sparked the idea that the spaces behind and in front of the screen were “on some level maybe only metaphorically the same” (ibid 56:15-57:00).

Generally speaking metaphors are didactically powerful; everyone immediately has an idea of what is being talked about when we use them (Rid 2013:165). Evidently the cyberspace metaphor is one people identified with. Thus, a science fiction writer had the honour of coining this now ubiquitous term as he was already imagining what the implications of new technologies could be before the vast majority of us started doing so. Today, the term ‘cyberspace’ has become so widely accepted that we are now able to use it unselfconsciously (Olsen 1994). However, as Taleb cautions “we want to be told stories, and there is nothing wrong with that – except that we should check more thoroughly whether the story provides consequential distortions of reality” (2007:75). Understanding

\textsuperscript{23}‘Cybernetics’ was popularised by Norbert Wiener in his history of automata *Cybernetics: or control and Communication in the Animal and the Machine* first published in 1948 (Tomas 1995:23). Wiener in turn derived the term ‘cybernetics’ from the Greek κυβερνήτης or steersman. It was used to describe the new interdisciplinary science of feedback mechanisms, which combined communications and control theory with statistical mechanics. “We have decided to call the entire field of control and communication theory, whether in machine or in animal, by the name Cybernetics” (Wiener 1948:19).
when the cyberspace metaphor is stretched too far will be important to the later analysis.

**Conflicting definitions**

Given the terms origin it is not surprising that there are multiple definitions for the term. Kuehl for instance lists 14 different definitions (2009:31-32). Strate meanwhile deals with conceptualisations from 18 different authors (1999:385). While most definitions conceptualise of cyberspace as a space Rid argues that it is not a space at all and has simply become a “common metaphor to describe the winding reaches of the internet” (2013:166). Rid does not buy the cyberspace metaphor arguing that it is “just a network” (2013:166)\(^2\). While his statement is true to some extent, others have argued that it misses the point of the cyberspace metaphor. The spatial metaphor they argue is not meant to convey a Cartesian space that one can map and in which we can pinpoint places using coordinates. Rather, as Cohen has argued, it is a “metaphor [which] expresses an experienced spatiality mediated by embodied human cognition” (Cohen 2007:226). Such a conceptualisation is certainly much closer to what Gibson had in mind when he coined the term. Rid however is correct when he cautions that there is a certain point were metaphors break down. As mentioned earlier we should be careful not to cross this line.

**The technical functioning of cyberspace**

\(^2\)Like other definitions, the definition proposed by Rid is helps him to advance his argument. Rid contends that using special metaphors is “ill-fitting” as cyberspace is “not even a space” (2013:166). Such a conceptualisation of cyberspace which sees it a “just a network” makes it easy to jump to the conclusion that the US Air Force should stop talking about “flying, fighting, and winning... in cyberspace”. Instead Rid argues “the debate on national security and defence should be well served if debating war was cut back to the time-tested four domains” (2013:166). What Rid misses is that it is not the thinking of cyberspace as a space, which is the problem, but rather how we approach the securing of it.
Therefore leaving aside the cognitive argument it is useful to examine how cyberspace actually functions in order to judge the merits of the special metaphor and what dynamics the space has. The way in which this system works is quite different from analogue telephone networks for example which is a hub and spoke system with calls being routed directly from one point to another. The internet is designed to move data around efficiently using scalable infrastructure. In order to satisfy these criteria data is not sent in single chunks but instead is split into smaller packets. These data packets contain the ones and zeros trying to travel from one destination to another and because they are moved in small packets they are all able take different routes to reach their destination. As they make their way from one router or switch to another they are simply sent to take the least congested route. In order to rout packages the network relies on an addressing system, the Domain Name System (DNS) and a transmission protocol, the Transmission Control Protocol, and Internet Protocol known as TCP/IP. The TCP/IP and DNS protocols set out the basic operating parameters of the network. These are the rules everyone follows; each packet is addressed to a specific address and can be routed through the network any number of different ways to get there. The beauty of this is that any application can send data from one place to another as long as it adheres to the rules of the TCP/IP protocol (Rosenzweig 2013:18). Crucially it also means that the physical infrastructure cyberspace relies upon is used as a shared resource.

### The Dynamics of Cyberspace

The way in which this system function is of tantamount importance to our discussion as it defines the relationship between cyberspace and physical geography. While the physical infrastructure cyberspace relies upon has a geographical location the concepts of distance or physical location have little meaning to the data that travels through the network. As Post describes it, while it is possible to map cyberspace by representing all its connection points, such a map would have no scale. Each part of the network is connected to another through a few ‘hops’ and distance does not matter as the data moving through
the network (when traveling through fibre optic cables) is literally traveling at the speed of light (2009:28). The significance of this is that cyberspace does not function like a Cartesian space. It is this attribute combined with the fact that data is not transmitted directly between connection points within cyberspace that define the type of space it is. These attributes also lie at the root of the new vulnerabilities of cyberspace is exposing us to. National borders have little meaning in a space where distance is negligible.

To conclude this discussion, it is clear that the term cyberspace has multiple definitions and that we should be careful not to over-stretch the metaphor. Knowing where to draw the line (i.e. how cyberspace is similar or different to physical space) is important. While keeping this in mind there are several basic characteristics, which we can ascribe to cyberspace. We saw that it is a space where distance is inconsequential and where the physical infrastructure is used as a common resource. The physical infrastructure does look like a network yet those resources are shared because of the way in which our computers are programmed to use that infrastructure. It is also important to keep in mind that cyberspace is not separate from physical space. It is connected to physical space through its physical infrastructure and users. In summary, cyberspace is a metaphor, which is meant to convey a sense of experienced spatiality mediated by human cognition. It is a space connected to physical space by its shared physical infrastructure where distance is negligible.

---

25 David Post is a professor of intellectual property law and law of cyberspace at Temple University who has been working on internet law for 15 years. He is also a Fellow at the Institute for Information Law and Policy at New York Law School and an Adjunct Scholar at the Cato Institute. In his article “Against ‘Against Cyberanarchy’” (2002) he takes the position that communication in cyberspace works fundamentally different to the way it does in physical space. His book Jefferson’s Moose in Cyberspace is a thought experiment. He asks if the internet was a newly discovered place, a planet or an island what is the kind of law we would want to have in that place. He then compares this to the actual law we currently have.

26 The attributes of negligible distance and data on the network not taking direct routes should be seen as defining features of cyberspace as their combination has profound implications. If I want to data from my house to a friend in a city a few kilometers away for example the data will be split up and send in individual packets. Depending on network traffic those packets of data could potentially travel all over the world before they arrive on my friend’s computer. However, because of the speed at which data is transmitted on the network the distance it travels is negligible.
V - US Policy and Cyberspace

Now that we have established these basic dynamics we can proceed to analyse the way in which US cyber policy conceptualises cyberspace. When doing so it will be important to recognize that as Strate has argued there has been a tendency to focus on “one particular variety of specific combination of elements” i.e. those elements of interest to the analysis are focused upon while others are left aside (1999:406). Two things to look for when examining the definition used by US policy makers will be if this definition justifies the assertion of state control over cyberspace and if it tries to segment cyberspace into national segments. This has profound implications for the way in which they could justify the use of cyber weapons. If a definition is used that tries to segment cyberspace into distinct bordered ‘national’ segments for example it becomes difficult to justify the use of cyber weapons, as doing so would constitute an attack on the territory of another state. Conceptualizing cyberspace as a single borderless space however also has far reaching consequences, as one would loose the traditional way of distinguishing what is and what is not part of the state.

NSPD 54 and PPD 20 both define cyberspace as “the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries” (2008:3)(2012:2). It immediately becomes apparent that this definition is quite wide encompassing any connected devices. Simultaneously however, the definition is quite specific drawing attention to ‘embedded processors and controllers in critical industries’ indicating a special area of concern. Further, the definition recognizes that the network is interdependent. Meanwhile neither NSPD 54 nor PPD 20 reason that cyberspace is a bordered space. This illustrates that the authors of these documents understand the shared nature of the infrastructure cyberspace relies on. What is also interesting is that the documents never explicitly make any distinction
between the national and international. This indicates that their authors are also aware of the fact that distance in cyberspace is inconsequential. This gives us some insights, which can help us understand how US policy makers may think about the use of cyber weapons and cooperation to secure cyberspace. First however, we will look at how US policy sees the role of the state when it comes to cyber security.

As we saw US cyber policy does not frame cyberspace as a space upon which the state must establish direct control. Rather, corroborating the trend observed by Dunn Cavelty it conceptualizes cyberspace as a single inter connected space (Dunn Cavelty 2013:118). In first instance this seems to make justifying the involvement of the state in cyberspace difficult, as it does not connect well with traditional notions of territorial sovereignty. However, the focus on national security in this case is re-introduced in a different way. As the afore mentioned theory developed by Nissenbaum and Hassen suggest PPD20 does so by linking several different referent objects to cyber security. PPD 20 sums up these referent objects when it defines US national interest in relation to cyber security as “national security, public safety, national economic security, the safe and reliable functioning of “critical infrastructure,” and the availability of “key resources.” PPD 20 and NSPD 54 focus on how the destabilization of cyberspace might affect US interest regardless of where the destabilizing effect might emanate from thereby recognizing the borderless nature of cyberspace. Nonetheless, there still persists a inside/outside logic. Dunn Cavelty observes this logic when she argues that through its ability to keep certain infrastructures functioning the state is able to distinguish between life inside its territory and outside it. By protecting certain critical functions the state is able to preserve a way of life and the wellbeing of its citizens. As she explains “the relationship between state and infrastructure emerges as an alternative to the image of

27 The term "critical infrastructure" is defined in section 1016(e) of the USA Patriot act 2001 as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". "Key resources" are defined in section 2(9) of the Homeland Security Act 2002 as “publicly or privately controlled resources essential to the minimal operations of the economy and government”. 

46
Abraham Bosse’s Leviathan on the frontispiece of Hobbes famous book: Instead of being made up of its citizens, the state is regarded as consisting of the things inside its territory that make life ‘good’; assets that are not directly identified with its citizens, but material assets that give substance (and significance) to the state through being its foundation” (2014:6). From such a standpoint arguing for action through cyberspace that has effects outside of the territory of the US actually becomes easier as it does not try to segment cyberspace into national portions. Simultaneously, sovereignty is asserted by defining several national interests that will be defended.

Here we see the state emerge as the protector of critical infrastructure and the way of life its citizens enjoy. Reading through NSPD 54 and PPD 20 it is not quite clear what role cyber weapons are envisaged to have by the authors of these documents in pursuit of this goal; it remains unexplained from a tactical or strategic standpoint how these new capabilities are going to help protect critical infrastructures. References to how the capabilities will be used remain vague, deterrence is mentioned and so is the idea that offensive capabilities may be used when law enforcement is unable to deal with a threat (PPD 20 2012:4, 10). Rather the emphasis is on the high potential cyber weapons have to enhance US military and diplomatic power. Such a view is detrimental to the prospects for cooperation especially any cooperation that focuses on the reduction of vulnerabilities. Further, such a view may partially be down to wishful thinking resulting in an overestimation of the utility cyber weapons may have. This in turn would lead to a miscalculation regarding the benefits of developing cyber weapons. Therefore, to some extent at least, this view among US policy makers may contribute to the proliferation of cyber weapons.

VI - Miscalculation?
While policy-makers at the highest level of the US government see the developing of cyber weapons as a way to increase US diplomatic and military power we saw earlier that there has also been strong opposition to their development. To understand if US policy makers have made such a miscalculation this chapter will examine the threats emanating from cyberspace and subsequently what role cyber weapons may be able to play to mitigate these.

How much utility do cyber weapons have? In what context could cyber weapons be used?

Could cyber weapons be used in a cooperative context with different actors confronting threats emanating from cyberspace using cyber weapons? By examining this it will become possible to analyse the reasons why are cyber weapons being developed and subsequently how policy makers may view the trade-off between developing cyber weapons and more cooperation. Furthermore, it is also worth examining if cyber weapons themselves can be used in a cooperative context.

The role of cyber weapons in cyberspace

This section shall examine the threats emanating from cyberspace and the cyber capabilities being developed. To answer this question we will start by looking at a categorisation of cyber conflict developed by Rosenzweig\textsuperscript{28}. Rozenweig categorises cyber conflict by dividing it into four pyramid shaped layers. The four layers range from the most common type of cyber conflict at the bottom to the least common at the top. Within each layer we will examine the specific type of conflict taking place and whether cyber weapons have a role to play within that layer. Finally at the end of this section it we will be able to assess if cooperation that combats cyber threats may be possible using cyber weapons.

\textsuperscript{28} Paul Rozenweig teaches cyber security at the George Washington University School of Law.
At the bottom of the pyramid we find the most common threats. These include cyber crimes such as identity theft, online scams, fraud, and cases of extortion. While such activity in cyberspace is a common problem for internet users it does not threaten the functioning of cyberspace itself or national security. The criminals perpetrating these crimes use tools that are generic and readily available (2013:15). The second layer of the pyramid consists of cyber espionage. The malware used by these actors is much more sophisticated and include a mixture of state or non-state actors who try to steal intellectual property or state secrets (2013:15). On the next level of the pyramid we find what Rosenzweig labels ‘cyber insurgency’. It is on this layer where we find competing factions that include hacktivist or patriotic hackers that deface websites or deny services. The tools and financial means these actors have at their disposal are often limited but character of conflict in this layer is distinct from what we find in the first and second layers pyramid (2013:15). Then, there is the top layer of the pyramid where cyber war occurs. Here, the main actors are states, which have access to the most sophisticated cyber capabilities. These capabilities include the ability to sabotage and cause physical damage using code (2013:15-16).

What is interesting about this categorisation for our purposes is that cyber weapons seem to play a marginal role within cyber conflict itself. Cyber weapons

29 Cyber criminals often use tools that are generic and readily available to perpetrate crimes in the bottom layer of the classification we are working with. One example of such a hacking tool is the Blackshades malware suite. This was a remote access Trojan which could be bought from a website for 40 to 50 US dollars. Through this malware package hackers could take complete control of the infected computers (Symantec 2014). Some cyber criminals however do have access to sophisticated malware a gang of cyber criminals dubbed Carbanak is a good example such an actor. Discovered in 2015 it succeeded in stealing up to 1 billion dollars from 30 different banks (Kaspersky 2015).

30 There are plenty of examples of these cyber espionage campaigns. Kaspersky labs, has for instance, uncovered what it calls the Equation group (probably the NSA) (2015). There is also a well-documented cyber espionage campaign with Russian origins dubbed Uroburos by G-Data security labs (2014).

31 One of the most well known actors in this layer is a group of hacktivist know as Anonymous which was most active from 2008 to 2012. The group’s tactics comprise mostly of DDoS attacks although they have also had success using fairly simple hacking techniques. The most visible operation Anonymous has carried out to date was its 2010 DDoS attack against PayPal, Visa, and Master Card in retaliation for their refusal to process donations for Wikileaks (Zetter 2014).
only come into play on the top layer of the pyramid. Their role on the first three layers is non-existent. To illustrate this further it is useful to quickly focus on each of the layers in order to determine if cyber weapons could be of any use to combat the various threats.

The actors on the first and third levels of the pyramid (cyber criminals, activist and patriotic hackers) have in common that they make use of common hacking techniques while they can usually remain anonymous. When combating these types of threat causing damage to the computers owned by these actors is of little use. The computers they use are easily replaceable while they carry out their attacks through the common infrastructure of cyberspace. Even if the source of the attack is identified it could easily be a hacked computer of an unsuspecting victim (Geers 2011:120). To counter such actors, first, it is paramount that users secure their own devises. Second, the people perpetrating such crimes should be arrested. In order to achieve this cooperation among law enforcement agencies is extremely important, as cybercrime is transnational. Rendering the cyber criminals computers useless will not aid any investigation. Cultivating this type of cooperation is something the Budapest Convention on Cybercrime has made a start on. However, currently the situation is that hackers can easily route an attack through a country with which the country the target is in has poor diplomatic relations or no agreements on law enforcement cooperation (Geers 2011:120). When it comes to the DDoS attacks meanwhile, as we have seen coordinated efforts between Internet Service Providers and CERT teams in different countries can defeat these attacks (Mueller 2010:25). Here cyber weapons are unable to play a constructive role to mitigate threats while cooperation between different actors is key. This cooperation can come in different forms including cooperation among law enforcement agencies, CERT teams.

When we move our focus to the second layer of the pyramid in which cyber espionage takes place the hackers active within this layer have access to sophisticated malware and a high level of expertise. Those carrying out cyber
Espionage frequently work from within intelligence services\textsuperscript{32}. Although these actors do have substantial assets, which can be retaliated against, again, cyber weapons are of little use. Taking action using cyber weapons to retaliate against cyber espionage is highly unlikely as the level of proof needed to carry out such action is unlikely to be attained. Further, generally speaking states are reluctant to use military force and there is certainly no precedent of using it in retaliation for espionage (Geers 2011:120). Reducing the threats posed by such actors is possible only with knowledge about the vulnerabilities they are able to exploit.

Within the bottom three levels of the pyramid then there is little use for cyber weapons. Using them against non-state actors is unlikely to have a deterrent effect. State actors meanwhile are also difficult to deter while doing-using weapons against those carrying out espionage activities has no precedent. Given this situation we are left with the possibility of cyber weapons being used in the context of a war or a tactical strike as we have seen with Stuxnet. However, up until now we have never encountered a conflict between two cyber capable actors creating a situation were any talk of cyber weapons in such a context is almost entirely theoretical.

Nonetheless, this has not stopped the US from integrating cyber capabilities into military doctrine. Here it seems to be taking a relatively careful approach reflecting its great reliance on cyberspace\textsuperscript{33}. This is illustrated in the latest

\textsuperscript{32} See footnote 30 for examples of cyber espionage campaigns run by various intelligence agencies.

\textsuperscript{33} Chinese cyber doctrine is much more heavy handed and has evolved out of an analysis of how the US operated during the First Gulf War. Chinese observers noticed that the US as a technologically more advanced adversary was able to eliminate the ability of Iraqi forces to communicate and thereby their ability to move and carry out effective strikes. Conversely however, the US 'informationized' forces relied heavily on electronic communication to dominate its adversary and were heavily reliant on real-time information to be effective (Hagestad 2012:46-49). This gave rise to the idea that China must be able to destroy the enemy’s capabilities of “observation, decision-making and command-and control” while China will maintain an “organic” ability to communicate negating the technologically superior enemy’s information superiority (ibid 50). This idea has resulted in the adaptation of a rather interesting version of a deterrence strategy. Its strategy is simply to shut down all means of digital communication. While the strategy does recognize that there is mutual dependence on cyberspace the strategy seeks to take advantage of this. However, because this is rather heavy handed; it is only
documentation declassified by the Joint Chiefs of Staff entitled *Cyberspace Operations*. The Joint Chiefs write that, Offensive Cyber Operations are “intended to project power by the application of force in or through cyberspace” (2013:II-2). They view these cyber operations as enabling tactical strikes while also adding to existing capabilities when used in concert with them, causing “synergistic effects” (ibid I-1). At the same time however, the document states that any offensive military operation in cyberspace must be accompanied by defensive operations (ibid II-2). It warns that "overlaps between military, civil, government, private, and corporate activities on shared networks in cyberspace make the evaluation of probable cascading and collateral effects particularly important when planning for [cyber operations]” (IV-4).

This confirms that the US, is attempting to adopt a combination of the strategies of those proposed by cyber power theorist and those who recommend building resilient systems. It wants to use cyber weapons in conjunction with its other capabilities to project power while keeping their own systems secure. Perhaps the way the joint chiefs envisage the use of their cyber weapons is similar to the way in which they use Special Forces (Geers 1201:17). It is a capability, which enables the US to strike high value targets, which are otherwise difficult to reach. Simultaneously it will use an “active cyberspace defence” as proposed by those in favour of building resilience. This active stand consists of a “real-time capability to discover, detect, analyse, and mitigate threats and vulnerabilities to defend networks and systems” (II-3). However, it will only use this capability to defend its own systems and the systems of its allies. It is not a capability, which it plans to apply to cyberspace as a whole.

As we have seen however, this tactic of simultaneous offence and defence in cyberspace it questionable on a technical level. If one stockpiles zero-days one simply undermines their own ability defend effectively. The fact that the US has

---

likely to be used in the event of an invasion of China itself when it is abundantly clear that the country is under attack. It could therefore be seen as a more credible alternative to a nuclear strike (Hagestad 2012:49).
such contradictory policy goals indicates that policy makers may not have a clear understanding of the potential trade-off they are facing. Instead as we have seen they emphasise the potential advantage the US may gain from developing offensive cyber capabilities. In his book Clarke perfectly illustrates this line of thought with a hypothetical example in which a US Navy ship sailing in international waters off the coast of North Korea is attacked by a missile. The ship however in this case is equipped with a cyber weapon, which it uses to target the missiles guidance system directing it away from the ship saving American lives in the process (Clarke Knake 2010:239). The fact that Clarke viewed cyber weapons as having so much potential in 2010 when there are no empirical indications that they have anywhere near this much potential shows a clear case of miscalculation.

Thus, in this chapter it has been illustrated there are no practical uses for cyber weapons in the first three layers of Rozenweig's pyramid. The threats within these layers are best confronted through cooperation by law enforcement agencies and CERT teams and by focusing on reducing software vulnerabilities. It is only were military operations are concerned that cyber weapons enter the discussion. However it is clear that the role of state created cyber weapons is mainly limited to military operations by one state against another, probably in the context of a war between them. In peacetime their role is marginal and limited to the rare tactical strike. Such a tactical strike could be aimed against a state or non-state actor, however so far Stuxnet is the only example. The prospects for cooperation in this area are probably limited to cooperation of a military nature between close allies. The only example we have so far of such cooperation happened between Israel and the US when they worked together to develop Stuxnet (Langer 2013:11). It is also clear that US policy makers are overestimating the potential of cyber weapons. This may significantly reduce the prospects for any cooperation, which focuses on vulnerabilities.
VII - The Prospects for Cyber Arms Control

If states were to agree to give up their cyber weapons does that mean they could cooperate more effectively on cyber security issues? What motivates states to give up a particular capability? To come to an understanding this this chapter will examine the Chemical Weapons Convention and will compare it to a possible cyber weapons treaty based on similar principles; banning the development of a capability instead of attempting to control the materials used to develop them.

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destroutions also known as the Chemical Weapons Convention (CWC), which came into force in 1997. The CWC treaty is particularly successful with all but 6 states having ratified it. In the 17 years since it has come into force 57 percent of chemical munitions and 84 percent of the declared stockpiles of chemical agents have been destroyed. However, the banning of cyber weapons has never been seriously considered in policy-making circles. Thus, comparing the CWC to a possible cyber weapons treaty should shed some light on why it has never been considered.

When we compare chemical weapons to cyber weapons we find two major similarities. First, both capabilities are relatively easy to acquire. Second, one of the key motivations behind the prohibition against chemical weapons was the fear that terrorist groups could acquire them (Geers 2011:127). These two factors should also motivate states when they consider a possible ban on cyber weapons. Because the knowledge required to create malware is relatively easy to acquire this arguably creates an advantageous situation for non-state actors especially given the fact that states are driving the development of ever more sophisticated malicious software which can be re-appropriated. Further, it can be argued that malware represents a common problem, one that threatens the

---

34 This coincidently, was around this time that discussion about the possibility of a cyber weapons convention first surfaced (Clarke, Knake 290:2010).
security of all states. Combating the existence of safe havens from which non-state actors can operate could therefore become a cornerstone of a convention prohibiting cyber weapons. Such a universal goal would be analogous to the goal of ridding the world of all chemical weapons found within the CWC (ibid 129).

However, there are also some crucial differences between cyber weapons and chemical weapons which represent problems for a possible ban. First a large portion of the success of the CWC lies in the fact that chemical weapons sites can be inspected and the weapons verifiably destroyed. As we have already explored, in contrast, cyber weapons can be developed in secret and are easy to hide. Adding to the problem of inspection is the fact that malware evolves rapidly (Geers 2011:130). This means that those trying to detect malware are constantly struggling to keep up with the latest developments. Illustrating this are the 123,054,503 “unique malicious objects” Kaspersky labs found in 2014 (2014:3). While it should be possible to overcome the second problem by properly defining what a cyber weapon is in a treaty the problem of verification is more difficult to overcome. Richard Clarke writes that in his role as National Coordinator for Security, Infrastructure Protection, and Counter-terrorism under the Clinton administration a Russian proposal for a cyber arms control treaty was rejected for partly this reason (220:2010). Because of this verification problem the spread of the technology underpinning cyber weapons should be seen as inherently difficult to control. How would it be possible for one state to verify that another does not have any cyber weapons? How would confidence-building inspections work?

Nonetheless, this is no reason to assume that an agreement to ban cyber weapons would be impossible. This after all the question of their development and use as with chemical weapons is a normative one; if the use of such weapons becomes unacceptable then using them would become counterproductive, as it invite some form of punishment. Yet, the US at least has been reluctant to even think about giving up its ability to use cyber weapons. This indicates that there may be a lack of political will to counter the proliferation of cyber weapons. This brings us to another major difference between the CWC and cyber arms control.
In 1997 it was clear that both the US and Russia stood behind the CWC when presidents Yeltsin and Clinton made a joint statement confirming their commitment. This leadership was an important signal to others, increasing the pressure on them to join. Underpinning the CWC is a genuine belief that the horrors of chemical warfare should not be repeated (Geers 2011:127). Unfortunately such political will is completely lacking when it comes to cyber security. Instead the opposite view has prevailed in some circles, war in cyberspace is seen as a ‘cleaner’ way to wage war putting less lives at risk (Clarke Knake 2010:239).

While the touting of cyber weapons as a means of ‘clean’ warfare is one thing the high potential US policy makers envision cyber weapons to have does not correspond to what we have seen empirically. This leaves one to wonder if US policy makers are grossly overestimating the impact cyber weapons could have and if this causes a skewed analysis of the costs and benefits associated with developing them. If one thinks cyber weapons could be revolutionary in the way that Clarke does, then entering into an agreement foregoing the use of such capabilities, while it is very hard to verify that your adversaries are doing the same makes little sense.

However, agreeing to a complete ban on cyber weapons may not be necessary to improve cooperation. An international community that is more frank about current developments in this area would already be helpful. At the very least it would force the international community to come to terms with the possibilities cyber technologies are opening up. For a start it would be useful to come to agreement about how cyber weapons should be defined as proposed within the OSCE. This would work toward lifting the veil of plausible deniability off everything related to the work intelligence and military agencies are doing in cyberspace. Currently the situation seems to be that many countries around the world are working to develop cyber capabilities yet this development is not talked about in terms of the wider implications it may have because everyone is implicitly taking part. Talking more frankly about cyber weapons should at the
very least alleviate this situation and allow the international community to move on to issues surrounding the use of these capabilities. In this sense then the developing of cyber weapons itself is not at the root of the lack of cooperation but rather the prevailing wisdom that as long as plausible deniability is maintained gains can be made.

Only if policy makers start to abandon this mind-set it will become possible cooperate on a much deeper level by focusing on reducing vulnerabilities. As Dunn Cavelty has argued this is were the interest of users and states intersect; reducing vulnerabilities would make cyber space significantly more secure for both (11:2014). However, doing so would also bring a significant trade-off with it from the standpoint of governments. While the argument that significance and impact cyber weapons has been overstated is strong, the one area where the ability to hack into systems has been revolutionary is espionage.

While it is difficult to pinpoint exactly what information and how much of it cyber espionage campaigns are extracting the Snowden leaks have given us some insight into this. NSA slides published by DerSpiegel state that there have been at least 30,000 ‘incidents’ and 500 ‘significant intrusions’ into the systems belonging to the Department of Defence (DoD) in attacks emanating from China. Unfortunately the slides do not mention a time period but the stolen data amounts to 50 terabytes of data, which is equivalent to 5 Libraries of Congress. The data stolen is wide in variety; it includes air refueling schedules, 33,000 officer records, 300,000 user ID’s and passwords, information about B-2, F-22, F-35, space lasers, nuclear submarines etcetera (DoD slides). While these slides only provide us with details about information being infiltrated from DoD systems by a single actor it does show us that the ability to do so is truly revolutionary. Explaining the significance of this Clarke and Knake write “cyber espionage is in many ways easier, cheaper, more successful, and has fewer consequences than traditional espionage” (2010:232). In their book they explain that during the Cold War spies had to physically carry documents out of classified facilities and leave them in dead drops. One of the Cold War’s most notorious spies, Robert Hanssen, was only able to deliver a few hundred pages of
documents to the Soviets in the two decades he spent spying for them (2010:234). Today such methods have been replaced by the use of spyware which is able to extract much larger quantities of information.

The significance of this for this analysis is that as we have seen cyber espionage tools and cyber weapons depend on the same building blocks. This presents us with a situation where even if the use or development of cyber weapons is banned cooperation that focuses on vulnerabilities will be severely impeded unless governments are willing to make a significant trade-off in the form of their cyber espionage capabilities. Without a focus on vulnerabilities however the drive to develop cyber weapons and cyber espionage tools has resulted in competition and secrecy instead of cooperation in the field of cyber security. While there is some cooperation between CERT teams this cooperation cannot be optimally effective when it is in the interest of military and intelligence agencies to hide knowledge about zero days and even actively insert them. For cooperation that goes beyond diplomatic efforts and actually increases the security of cyberspace itself the current environment is not conducive.

To end this section we can draw several important conclusions about why the lack of serious cooperation in the area of cyber security exists. Undoubtedly, the connection between cyber weapons and cyber espionage tools is critical and should be seen as the most important factor behind the lack of cooperation. These are built upon the same knowledge of zero-days as cyber weapons and therefore strongly incentivise governments to keep this knowledge secret. Conversely serious cooperation would entail the sharing of this knowledge. Such cooperation however is not taking place, which plays into the hands of those developing any type of malware, not just cyber weapons or cyber espionage tools. Because cyber espionage tools were developed first and up until now these tools can be said to be revolutionary while cyber weapons have not had a significant impact it is reasonable to view cyber weapons as a by-product of cyber espionage. The development of cyber weapons therefore is not at the core of the lack of cooperation we are witnessing today. The significant impact cyber espionage tools have had explains why cyber security is characterised by such
competition and secrecy. Governments are simply unwilling to forego the ability to use cyberspace to spy.

The initial decision by policymakers to start stockpiling zero-days however has different roots and can be said to be the result of miscalculation. As we saw high level policy makers such as Clarke thought cyber weapons could truly revolutionise warfare making it less bloody in the process. Similarly the military and intelligence agencies seemed to have high expectations as they were thinking of attack long before considering the consequences. A revolution in military affairs around cyber weapons however has failed to take place yet the expectation that it would did mean that policy was taken in the direction of competition and secrecy from the start. The political will to cooperate has simply always been absent in the US. This is partly due to expectations, which never became reality but also to several technological factors. These make controlling the proliferation of cyber weapons inherently difficult. As we saw cyber weapons are easy to develop in secret while it is also easy to remain anonymous once they are used.

**Conclusion: Proliferation or cooperation?**

From this analysis it is now possible to conclude that there is a trade-off between the developing of cyber weapons and cyber security cooperation. It is clear that any form of cooperation that focuses on reducing vulnerabilities faces serious obstacles because of the fact that cyber weapons rely on keeping secret knowledge of zero-day vulnerabilities. Any serious cooperative efforts to reduce vulnerabilities however would entail governments giving up their stockpiled zero-days presenting them with a serious trade-off. Any attempt at this type of cooperation would abolish or significantly reduce the cyber espionage and cyber
weapons capabilities of states. This forms a serious obstacle for any form of cooperation that focuses on vulnerabilities. As Dunn Cavelty has illustrated, a focus on vulnerabilities would result in a more secure cyberspace for everyone: for both everyday users and states. Such an approach however, would be revolutionary, as it would rely on cooperation among all users of cyberspace and transparency.

However, until now there is no sign that there is any commitment to an international approach that focuses on reducing vulnerabilities within the US government, which has committed itself firmly to the developing of cyber weapons. Instead what we observe within US cyber policy is a policy-area characterised by secrecy and competition not one of cooperation and openness. Internationally the US has viewed attempts at cooperation that focuses on banning cyber weapons or vulnerability reduction with suspicion. This is illustrated by the way it has refused to engage with the Russian proposals for cyber arms control while it has only recently admitted to the simple fact that it even has cyber weapons when the Joint Chiefs published *Cyberspace Operations* in 2013. Further, recently it has also come to light how US intelligence agencies are actively undermining the ability to secure the computing environment by inserting vulnerabilities and reverse engineering security software. Such practices point to the obsessive stockpiling of zero-days, which is detrimental to the prospects for cooperation. To a large extent we can explain this obsessive stockpiling by taking into account the extremely high expectations policy makers within the White House had of cyber weapons. This locked the US into a mode of competition and secrecy before the consequences of such an approach were considered. Understanding this miscalculation on the part of policy makers therefore is key to explaining why cyber security is currently characterised by competition and secrecy.

As Nissenbaum and Hassen have pointed out it is clear that cyber security has been taken out of the political and simultaneously securitized and technified. As a result cyber security has received much more attention yet policy makers have not approached the problem in a realistic and thoughtful manner. Threats have
been misrepresented, the potential of new capabilities exaggerated, and the tradeoffs associated with different approaches to securing cyberspace have not been taken into serious consideration. Securitization therefore has lead to policies that advance goals of the state, mainly the ability to carry out cyber espionage and develop cyber weapons at the expense of the overall level of security attainable for everyone.

What is desperately needed is to bring politics into cyber security. Currently it is vital that we open up a dialogue about security issues between all users of cyberspace. This is not an issue, which should only be the concern of states. Currently however, there is so much secrecy surrounding the issue of cyber capabilities that states are barely able to admit to one another that they are developing cyber capabilities. This is impeding frank and open discussion and is detrimental to diplomatic efforts. As we have seen currently states are unwilling to simply define what a cyber weapon is. Nonetheless, despite the fact that cyber diplomacy is currently mired in secrecy and competition it is still theoretically possible for the international community to ban the use and development of cyber weapons. Such a ban after all could be based on normative principles alone. However, such an agreement currently seems unlikely. This is not only due to the current state of cyber diplomacy but also to some technical aspects of cyber weapons themselves. As we have explored cheating an agreement would be quite easy as developing and testing cyber weapons in secret is very easy.

Furthermore, the way in which states view their responsibility vis-à-vis cyber security may be problematic. There is an uncomfortable relationship between of what the state views as its responsibility to protect key infrastructure, which introduces the notion of sovereignty into cyber security and the borderless nature of cyber space. This logic of segmentation allows states to abstain from taking collective responsibility of securing cyberspace. This logic however, is problematic, as a logic of segmentation does not reflect the dynamics of cyberspace. We see acknowledgement of this tension when documents published by the White House and the Joint Chiefs. While these documents recognise the borderless nature of cyberspace and warn about to the potential for collateral
damage resulting from cyber operations they largely focus on securing particular portions of cyber space thereby ignoring the borderless nature of it. It is likely that as long as this logic persists and governments continue to ignore the simple fact that securing cyberspace is something that can only be accomplished by sharing responsibility we will see the continuation of the secrecy and competition which characterises current cyber security policy.

Cyber deterrence theorist such as Goodman then are correct then when they argue that the concept of counter-productivity has not taken hold in cyber security. Interestingly however, this has taken hold in a different way than he envisioned. While Goodman uses this as a way to argue in favour of a cyber deterrence strategy which calls for the developing of cyber weapons the effect of such a strategy, which we are witnessing today, is the opposite of what he indented. What we are observing is that the reluctance or inability of high level policy makers to see beyond the consequences of stockpiling zero days has contributed to a computing environment which is so insecure that it has revolutionised spying. In other words, US policy makers have been unable to grasp that this stockpiling through which they hoped to gain a tactical advantage is having strategically negative consequences. As we have seen sensitive information is constantly being leaked from US systems while cyber weapons have had no impact on the battlefield and everyday users are faced with a less secure computing environment.

When we pull cyber espionage tools into the picture we also see that the developing of cyber weapons may not be at the core of the current competition and secrecy. Currently cyber espionage tools are proving much more useful than cyber weapons. Therefore cyber espionage tools should really be seen as being at the centre of the trade-off between cooperation and proliferation. If cyber espionage tools did not prove to be as revolutionary as they are today it is more likely that policy makers would be more open to approaches that reduce vulnerabilities.
The developing and proliferation of cyber weapons however does not necessarily close off all areas of possible cooperation. First, their development leaves open the possibility of military cooperation among allies. It is possible that countries with close military ties will work together closely on the development of cyber capabilities. This is something we have already seen with the developing of Stuxnet where the US and Israel probably worked in tandem. As we have seen however, such capabilities have little or no use were law enforcement or defending against cyber espionage is concerned making cooperation which makes use of such cyber weapons a purely military matter.
Bibliography


Langer, R. 19-11-2013. *Stuxnet’s Secret Twin; The real program to sabotage Iran’s nuclear facilities was far more sophisticated than anyone realized.* Foreign Policy. http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack


Mele, S. 2013. Cyber-weapons: Legal and Strategic Aspects (version 2.0). Italian Institute of strategic studies


http://www.osce.org/pc/109168?download=true


Program on Humanitarian Policy and Conflict Research at Harvard University . 2009. The Manual on int law applicable to air and missile warfare.


http://www.foreignpolicy.com/articles/2014/01/15/cult_of_the_cyber_offensive_first_strike_advantage

Singer P. and Wright T. 2013. An Obama Doctrine on New Rules of War,
http://www.brookings.edu/research/papers/2013/01/an-obama-doctrine-on-new-rules-of-war


Thomson, I. 2012. Fujitsu Creates Antivirus Virus for the Japanese Government Fujitsu anti virus
http://www.theregister.co.uk/2012/01/04/fujitsu_virus_japanese_government [Accessed 03-07-2014].


https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf


