The dilemmas of state response to cyber attacks. Understanding the phenomena, challenges and legal response.

Lukas van den Boom
Studentnummer: 2500665
l.r.vanden.boom@student.vu.nl
Utrecht, 23 december 2012

Bestemd voor:
Dr. J.S. Timmer

Vrije Universiteit Amsterdam
Faculteit Sociale Wetenschappen
Afdeling Bestuurswetenschappen
Table of contents

1. INTRODUCTION ................................................................................................................. 3

2. PLACING CYBER ATTACKS IN ITS CONTEXT .............................................................. 4
   2.1 Cyber threats .................................................................................................................. 4
   2.2 Forms of cyber attacks ................................................................................................. 6

3. SHIFT FROM PASSIVE TOWARDS ACTIVE DEFENSE MECHANISMS ....................... 6

4. INTERNATIONAL LAW CONCEPTS ................................................................................. 8

5. BROADENING THE SCOPE ............................................................................................. 9

6. CONCLUSION .................................................................................................................... 10

LITERATURE ...................................................................................................................... 11
1. Introduction

Our modern day society has often been characterized as a network society (Castells, 2010); boundaries are blurring (Tikkanen and Parvinen, 2006, p.41), hierarchies are becoming flatter and more recursive and people are more and more connected through multiple sets of overlapping relationships (Hogan, 2011, p.14). Globalization’s interconnectedness directly influences our thoughts, actions, norms and values. The role and application of the internet could not be underestimated in this sense. It can be truly said that Information and Communication Technologies (ICTs) became deeply rooted in our society (Herzog, 2011, p.50). More and more products contain software and electronics, and more and more of them are connected to the internet, making them all a part of cyberspace (Govert.nl, 2011, p.9). These interconnected systems bring many advantages to our daily life. At the same time, however, our dependence on ICTs makes our society vulnerable (Bekkers & Thaens, 2005, p.37). Vital infrastructures like the control of transportation systems, power grid, water systems and the flow of electronic transactions are highly sensitive for cyber attacks. Theorists such as Herzog (2011) and Yar (2006) classify these threats in terms of the new challenges for free societies. Democracies must find their way to strike a balance between maintaining adequate monitoring and early warning systems on one hand and allowing freedom on the internet on the other (Herzog, 2011, p.56).

In the year 2012 only, the Dutch iDeal payment service of the ABN Amro bank has been attacked by Ukrainian hackers; vulnerable information of citizens was captured by an Iranian hack on the DigiNotar security certificate system, and several governmental computer systems got infected by the Dorifel virus, spread by an Austrian server. Attackers are not bound by state borders, instead, they are gratefully taking advantage of botnets (networks of infected computers with malicious software), using unsuspecting third party computers. Since laws are varying from state to state, ‘safe harbors’ for cyber criminals subsist. According to Dutch Fox-IT computer scientists, the recent outbreak of the Dorifel virus could have been neutralized within hours if the police had the authority to break into the foreign computers of cyber criminals. Despite all knowledge of the source and the aggressor, precious time was spilled consulting an unwilling hosting provider for the voluntary removal of contents, putting the intervening processes on standstill for days. Due to incidents like this, the ability of states to protect their (digital) infrastructure without crossing jurisdictional borders themselves has been questioned.
The main goal of this paper is to investigate the extent to which international legal principles provide a practical outline for active response. Working from a theoretical point of view, this paper assumes that the enforcement on transboundary cyber threats can be seen in the wider perspective of modern day challenges regarding the increasing global connectedness. The following main question will be answered:

*What role does the international law play in shaping governmental behavior in countering cyber attacks?*

In order to answer this question, the following sub-questions will be asked:

- How does modern day literature define and distinct various types of cyber attacks?
- How do scholars interpret the legal principles and past state practices of the use of force in the digital domain?
- To what extent do international laws and agreements (for the use of digital force) contribute to addressing cyber attacks?

2. Placing cyber attacks in its context

2.1 Cyber threats

To define the legal issue, it is important to determine what constitutes a cyber attack. ICT security can be threatened by a wide range of activities including cyber crimes, cyber attacks, cyber espionage, cyber terrorism and cyber activism. These phenomena need to be defined to prevent them being conceptually confused with each other. However, this does not mean that they cannot be interrelated (Adviesraad Internationale Vraagstukken, Commissie van Advies inzake Volkenrechtelijke vraagstukken (AIV/CAVV), 2011, p.34). In general, cyber crime is used as the umbrella concept for all forms of crime in which ICT plays a crucial role (Stol, 2010, p.4). It is often defined as *the use of computer-based means to commit an illegal act* (Hathaway et al., 2011, p.20). Following Hathaway and colleagues, an act can only be considered as a cyber crime if it is criminalized under state- or international law and committed by a non-state actor.

A cyber attack, on the other hand, may be carried out by both state- and non-state
actors and must (be aimed to) undermine the function of a computer network. As in the case with cyber crime, the term ‘cyber attack’ can have several meanings, depending on the targets and the motivations of the perpetrators, and the scope, impacts and consequences of the attacks (Ghernaouti, 2011, p.1). Some actions could have a minor impact and might, or might not, be criminalized under state- or international law while others could be linked to crime, terrorism or even war. Despite of the fact there is no international consensus on the conditions and definitions of cyber attacks (to be discussed in chapter 4), our definition is heavily based on the broad interpretation used by Waxman (2011, p.422). By cyber attacks, this paper refers to the deliberate actions to alter, deceive, degrade, disrupt, or to destroy computer systems, networks, or the stored information on them.

While some cyber crimes can be considered as cyber attacks, others cannot. Take for example cyber espionage; trying to access a network in pursuit of valuable information is considered as a cyber crime (Ragnarsson & Bailes, 2011, p.63), but does it constitute a cyber attack? One of the conditions of a cyber attack is to undermine the function of a computer system. To be categorized as a cyber attack, actors must do more than passively observe a computer network, copying data (Hathaway et al., 2011, p.20). An actor must damage the operating system by adding misleading, false, or unwelcome information into the system.

Cyber terrorism refers to the attacks against computer systems, networks or the information on them for the purpose of intimidating a society to foster political or social objectives (Denning, 2001, p. 253). Cyber terrorists can be differentiated from other hacker groups by their motives (Hua & Bapna, 2012, p.104). Acts of cyber terrorism result in violence against persons or property and causes harm to generate fear. While also politically motivated, cyber activism (also known as hacktivism) differs from cyber terrorism in the way that the former seeks to protest and is not intended to physically injure or terrify. Hacktivists are using both legal and illegal means to effectuate their digital protest. Hacktivism refers to the marriage of hacking and activism and is defined as ‘the nonviolent use of legal and/or illegal digital tools in pursuit of political ends’ (Denning, 2001, p.239). One can conclude that there is a thin line between the various digital threats; the used techniques are often quite similar, only the intended objective is different (AIV/CAVV, 2011, p.34).
2.2 Forms of cyber attacks

The variety of actions that could be regarded as cyber attacks is extensive; ranging from website defacement and malicious hacking to distributed denial of service attacks (DDoS) and the demolition of infrastructures that rely on those networks (Waxman, 2011, p.422).

A common form is the defacement of websites; hereby, an attacker gains access to a server and changes the content. In 2008, for example, Russian hacktivists ‘defaced’ Lithuanian government websites with the hammer and sickle symbol after the Lithuanian Parliament passed a law banning the use of Soviet symbols (Tikk, 2011, p.126). According to Collins & McCombie (2012, p.81) hacktivists mostly use these attacks as an instrument to protest or just to show their technical skills.

Distributed denial of service attacks could have a larger, destabilizing impact on society. DDoS attacks are coordinated efforts that instruct infected PCs to send a flood of traffic to victims, designed to overwhelm their servers (Nazario, 2009, p.163). The DDoS attacks on Estonia in 2007 have been regarded as a ‘wake up call’. During a period of diplomatic tensions between Russia and Estonia, DDoS attacks overload Estonian government ICTs and commercial functions, including communications, media and banking, for weeks.

3. Shift from passive towards active defense mechanisms

To prevent the disruptive consequences of cyber intrusions from happening, security organizations and businesses apply various defense mechanisms on their systems. Traditionally, the perspective on defense is primarily concentrated on the so called ‘passive systems of defense’. Passive defense provides security in much the same way walled cities did centuries ago (Baker, 2011, p.14). Passive measures are designed to block intrusions on ICTs and are most frequently used as applications such as antiviral software, firewalls, and anti-spyware. Unfortunately, hackers are faster in creating malicious software than cyber security companies can develop new lines of defenses. It seems that always being one step behind would put the defender at a disadvantage. For the most sensitive targets, passive protections alone are insufficient (Kesan and Hayes, 2012, p. 435).

Apart from continuing to improve existing passive defenses, organizations and government agencies should consider combining strategies of passive defense with the more aggressive, active ones (McLaughlin, 2011, p.63; Wong, 2011, p.18). Active defenses enable
attacked parties to detect, trace, and then actively respond to a threat (Kesan and Hayes, 2012, p. 461). Basically, the process of active defense involves three steps: firstly the detection of an intrusion, secondly tracking the intruder and at last, doing some form of cyber counterstrike.

Apart from the digital resources, methods of active defense could be found in legal, economic, diplomatic and military means. Most non-technological aspects of active response would be relatively unproblematic if the detection traces to a single potential target, in one single country subject to a single unambiguous legal regime (Grove, Seymour, Goodman and Lukasik, 2000, p.90). Generally, this is not the case. Cyber criminals are aware of legal loopholes; they use for example servers that are physically located in other countries than where the attacker is located. In practice, Dutch law enforcers have to officially ask other countries to aid in further enforcement if a crime has effects that reach across borders (Schreurs, Kornelisse en Hermans, 2012, p.24). Even if countries are cooperating constructively, tracking an attack to its primary source may be complicated. If the apparent source state is not willing to cooperate, law enforcers in the target’s country must suspend their efforts and resort to other means.

The technologies available for executing a digital counterstrike are generally the same as the ones used in the initial attack. A counterattack can for example, be launched by infecting the attacker’s system with malicious software to permit the victim to take control (Kesan and Hayes, 2012, p. 420). Technologically, there are plenty of other options; however, the implications can be significant. Even though active defensive measures can be very effective, they are also controversial. Potential responses raises questions on ethical considerations (what behavior is acceptable?) and legal aspects (what behavior falls within the appropriate legal framework?).

Several scholars (e.g., Baker, 2011; Wong, 2011, p.30) warn that aggressive active defensive measures could endanger the global connected network. Active defenses have the potential to do more harm than good if not conducted in compliance with the international law and ethical principles. A counter attack may affect a third party more severely than the initial attacker. Given these problems with the prevailing view, Sklerov (2009, pp. 6-7) argues that states find themselves in a ’response crisis’, forced to decide between the legal path of defense and the more effective and possibly unlawful active measures.
4. International Law Concepts

One of the perspectives from which active defense measures can be studied is the *jus ad bellum* (in Latin: ‘right to war’). *Jus ad bellum* comprises a number of different criteria that regulates the use of armed force by states in their international relations (Waxman, 2011, p.425). Since International law is primarily based on global consensus, it has developed traditionally slow. Unfortunately, no clear statement in international law has been developed that outlines legally acceptable cyber defensive actions (Lotrionte, 2011, p.6). According to Waxman (2011, p.436) states cannot even agree how much physical damage must be sustained to qualify an attack as the use of force or an armed attack. While international actors are holding widely divergent views on acceptable conditions for active defense, there are past state practices and legal principles providing the outline for a valid legal response to acts of aggression (Lotrionte, 2011, p6). Under the legal principles based on the Article 51 of the UN Charter, a counter-attack might be justified as self-defense *if the necessity of that self-defense is instant, overwhelming, and leaving no choice of means and no moment for deliberation* (Obayemi, 2006, p. 28). Legal scholars, however, disagree on the proper interpretation of this article. It is often argued that all use of force is prohibited until a state has suffered an attack based on conventional weapons. This assumption, however, is not consistent with the more broad interpretation, claiming the presumed impact, rather than the type of weapons employed should be the guiding principle (Condron, 2007, 412). The Dutch Adviesraad Internationale Vraagstukken and the Commissie van Advies inzake Volkenrechtelijke vraagstukken (AIV/CAVV) see no reason, not to qualify a cyber attack as an armed attack if the consequences are comparable to those of an attack with conventional weapons. In other words:

*Cyber attacks could certainly be qualified as an ‘armed attack’ within the meaning of article 51 of the UN Charter if it causes substantial physical damage to vital infrastructure, civil property, military platforms or installations (AIV/CAVV, 2011, p.20).*

Claiming self-defense raises a number of issues. Firstly, it can be difficult to estimate the danger posed by an attack that has not yet occurred. Suspicious activity alone does not justify a counterstrike. Under the UN Charter legal principles, it is not clear what degree of
certainty in identification is required to justify a response. Secondly, there are questions about how to cope with the harm inflicted on third parties. A counter attack may affect the third party more severely than the attacker. This goes beyond all ethical principles and standards of proportionality (Hoskins, Liu and Relkuntwar, 2005, p.19). Launching a response against an innocent party could after all be qualified as an act of aggression instead of an act of self-defense (Farwell & Rohozinski, 2011, p.35).

Apart from the UN principles, several scholars (e.g., Sklerov, 2009, p.12; Kesan and Hayes, 2012, p. 511) suggest that victim states have the legal authority to use active defenses. States have the duty to prevent persons within their borders from perpetrating crimes against other states. Sklerov (2009, p.12) notes that victim states have the legal authority to use cyber counterstrikes if the attacker’s host state has insufficient criminal laws or declines to enforce them against the attacker. While the analysis is greatly simplified by looking at whether a state has violated its duty to prevent, states are still likely to find cyber attacks difficult to deal with in practice (Carr & Shepherd, 2010, p.83).

5. Broadening the scope

From a broader security perspective, states nowadays face series of ICTs threats that are difficult to control by their conventional tools of national security. The requirements of national security are changing rapidly and the lines between public and private, foreign and domestic are blurring (Tikkanen and Parvinen, 2006, p.41). Even though threats to critical infrastructures have always existed, threat scenarios now include peacetime attacks from anonymous non-state or state-sponsored hackers (Geers, 2009, p.1). As society’s dependence on information technology became more intense, cyber attacks became an increasing concern. Cyber attacks are more en more recognized as national security threats. In this respect, the words of CIA chief Leon Panetta are significant: “The next Pearl Harbor we confront could very well be a cyber attack” (Bumiller & Shanker, 2012). Legal scholars are increasingly recognizing that the current legal regime leaves states vulnerable to cyber attacks. Some scholars advocate new treaties to get past this legal shortcoming. The possibility of a substantial cyber attack now requires policymakers to rethink their approaches to secure critical infrastructures (Condron, 2007, p.421). A fundamental part of this discussion is how the territoriality of states is related to the sovereignty of cyberspace. While some scholars
deny the existence of the so called ‘digital sovereignty’, the majority acknowledges several layers that can be used to greater or lesser degrees by states¹.

6. Conclusion

While advances in computer technology have benefited several fields of society in general, they have also resulted in new dangers. This paper notes that criminal enforcement is complicated by complex jurisdictional issues. At the same time, it has been clear that the international laws on computer intrusions are much less developed than the rules and regulations of physical force in the non-digital world. While active defense is becoming less controversial, there is no international consensus on the legal guidelines for the active response. Difficult interpretive challenges with regard to the UN Charter can lead to randomness. Apart from the UN principles of self-defense, legal scholars are increasingly recognizing that the current legal regime leaves states and private parties vulnerable to cyber attacks. Some scholars advocate new treaties to get past this legal shortcoming. Unfortunately, there are no overnight solutions and no quick fixes. Based on the outcomes of this study, there is less reason to assume that the current international legal framework plays a guiding role in shaping governmental behavior in countering cyber intrusions.

Using the insights gained from examining the development of sovereignty in the air-, sea-, land- and space- domains, a more detailed analysis can provide insight in how international law might develop in the cyberspace domain.

Literature


