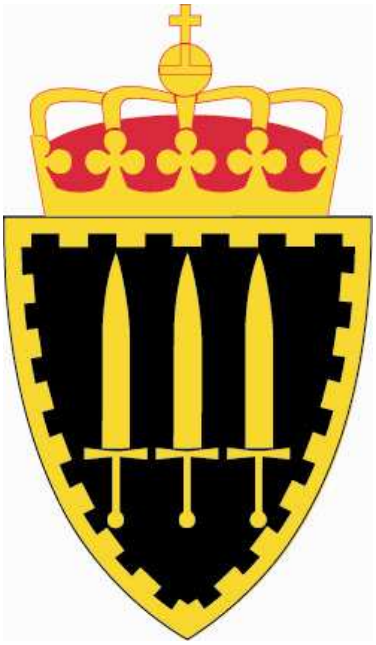

Forsvarets høgskole

våren 2012

Masteroppgave

Offensive Cyber

What are the possibilities of the use of offensive cyber as an offensive capability within the existing international legal framework?

Collin Engelbert Peter van Loon

Royal Netherlands Army

Intentionally left blank


Q.
WHAT WILL THE WARRIOR-GUARDIAN OF THE FUTURE LOOK LIKE?
YO! DUDE... BACK HERE
CYBER

Abstract

This master thesis is focussing on whether offensive cyber can be used by modern military forces within the existing international legal framework. The study consists of two parts.
The first part is discussing what cyber attack and offensive cyber is, and what the capabilities, opportunities and possibilities of the use of offensive cyber are.
The second part is analysing the role of offensive cyber in the existing international legal framework, and answers whether and how offensive cyber fits in, and complies with that framework. This analysis is conducted in a case study, by analysing the three main principles within the Laws of Armed Conflict (LoAC), proportionality, necessity and distinction, on the four recent cyber cases of Estonia 2007, Georgia 2008, Stuxnet 2010 and Libya 2011.

The conclusion of the thesis is that the existing international legal framework is not fully suitable for the use of offensive cyber. Especially the attribution problem, collateral damage, and distinction between military and civil objects are problematic. To set the boundaries for the use of offensive cyber, it is necessary to develop a new internationally accepted (cyber) legal framework. This framework also will enable the offensive cyber capability to be exploited efficient and effective.

Summary

Cyber is hot. Although the international community, scientists, military and NATO primarily focus on how to defend themselves against cyber attacks, this study mainly focuses on the offensive side of cyber. The thesis analyses the possibilities of the use of offensive cyber as a capability within the existing international legal framework. The thesis consists of two parts.

The first part discusses what offensive cyber is and what its possibilities and capabilities are. Offensive use of cyber is new within modern warfare. Therefore it is important to describe and explain cyber attacks and offensive cyber operations thoroughly. In this part the definitions are set, and the base characteristics of cyber attack are discussed. Not only the possibilities of offensive cyber are described, but also dilemmas for the use of offensive cyber are explained. This first part concludes with possible scenarios for the use of offensive cyber operations.

The second part of this thesis is a case study and analyses whether and how offensive cyber fits in, and complies with the existing international legal framework. Firstly, the aspects in the existing international legal framework are discussed, which are unambiguous for regular war scenarios, but seem difficult to interpret when it comes to cyber operations. Secondly, the case study is conducted by analysing the three main principles within the Laws of Armed Conflict (LoAC), proportionality, necessity and distinction, on the four recent cyber cases of Estonia 2007, Georgia 2008, Stuxnet 2010 and Libya 2011.

The conclusion of the thesis is that the existing international legal framework is not fully suitable for the use of cyber as an offensive capability. Especially the attribution problem, collateral damage, and distinction between military and civil objects are problematic. As long as there is no consensus on international accepted cyber law that sets the boundaries for the use of offensive cyber, the existing international legal framework is applicable, and the use of offensive cyber will have its challenges and grey areas. A new international accepted legal cyber framework should limit, and set boundaries for the use of offensive cyber. On the other hand, developing a new international accepted legal framework, in which offensive cyber is appointed, is also an opportunity to exploit the optimum use of offensive cyber, within that framework.

Acknowledgements

This thesis is the end product of two years studying at the Norwegian Defence University College in Oslo. These two years were a great experience. I had the opportunity to look in the 'kitchen' of the Norwegian Defence, studied interesting subjects and above all, met some great people. I want to express my gratitude to the Norwegian and Dutch Defence and Army for offering me this opportunity.

I also have good memories to my Stabstudiet Kull 6, especially group A2, and Masterstudiet Kull 6 colleagues. Thank you, it was interesting, instructive and I hope we'll meet again.
Takk for alle interessante, hyggelige og lærerike momenter. Det var to fantastiske år i Europas vakreste land. Vi ses!

I also owe sincere gratitude to LtCol (NORAF) Harald Høyback, for leading me through the process of writing my thesis. He always gave me the feeling I was on track, but also made me understand I was not there yet.
I also want to mention my colleagues 'Han' Bouwmeester and Peter Teeuw, and thank them for making time and effort to read through my notes, ask questions, be positively critical, correct me and advice me. This was very helpful.
Special thanks to my classmate and colleague Chris Siler (USMC), who was my friend and buddy during these two years. He was often a good sounding board and also put time and effort to help me with this thesis.

Last but not least, I especially want to thank my great wife Monique and my children Bo en Bram for the support I have received during the work on this project, and these two past years.
You were my inspiration!

Oslo, May 2012
Collin van Loon

Table of Content

1 Introduction

1.1 Background

In the spring of 2007, a cyber attack on Estonia blocked websites and paralysed the country's entire internet infrastructure. At the peak of the crisis, bank cards and mobile-phone networks were temporarily frozen, setting off alarm bells in the country and in NATO as well.
The cyber attacks came at a time when Estonia was embroiled in a dispute with Russia over the removal of a Soviet-era war memorial from the centre of Tallinn, Estonia's capital. Moscow denied any involvement in the attacks, but Estonian officials were convinced of Russia's involvement in the plot (Czosseck, Ottis, & Talihärm, 2010, s. 57).

> The methods used in this incident were not really new. However, considering Estonia's small size and high reliance on information systems, the attacks posed a significant threat. Estonia did not consider the event as an armed attack and thus refrained from requesting NATO's support under Art. 5 of the NATO Treaty[1]. Instead, the attacks were simply regarded as individual cyber crimes. The incident quickly drew worldwide attention and media labelled the attacks the first 'Cyber War' (Czosseck et al., 2010, s. 57).

1.2 NATO and Cyber

NATO (and other) countries focussed, from that moment, even more on adversary cyber attacks and paid increasing attention to cyber security. This still is the main focus of NATO and its allies within cyber space. Cyber security (which includes cyber defence) is an effort that asks for a comprehensive approach to protect a country's civil, economic and military resources and networks. There is already a lot written about cyber security. It is a hot item.
Today there is daily news about cyber attacks on financial institutions, governments and even military organisations, such as the Norwegian Defence Department in 2011 (Andreassen, 2011).

[1] Art 5 NATO treaty: The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security (NATO, 2010a, s. 2A-2).

These attacks, often relatively inexpensive in organisation, preparation and execution, cause a huge amount of investment in cyber security. The peace time attacks on our civil, military and social institutions and systems are to be categorised as cyber crime or cyber terrorism because of our current legal foundation. However, cyber can also be used by a military organisation, as a non-lethal and non-kinetic weapon, to influence and attack an adversary. Talking about the offensive side of cyber however, is still a delicate discussion in military organisations. It isn't offensive cyber, in general, that causes these delicate discussions, but the availability and possibility to use offensive cyber as a tool and weapon. There are several options and scenarios thinkable, on how to use offensive cyber as an effective weapon. Not all options are applicable for us as a modern western military force.

Ethics, international law, the unknown capabilities and effects of using offensive cyber, and a state's willingness of using offensive cyber, are just some examples of issues why NATO and many countries do not openly encourage the use of offensive cyber. As far as NATO is concerned, they openly state that for the coming period NATO will stick to their cyber defence policy and concept, and NATO will definitely not develop any cyber offense or cyber exploit concepts, unless the North Atlantic Council (NAC) and Military Committee (MC) decides differently. This will presumably not happen soon, as a certain amount of member states do not support the implementation of offensive capabilities at this moment (NATO, 2011).

1.3 Nature of Cyber War

Nevertheless many scientists and military specialists are getting convinced that offensive cyber is a tool, which can be an option for a state, in order to decide or influence a conflict. Also, it can be used in close corporation, synchronisation and orchestration with kinetic operations in an overarching military operation or campaign. In such a case, the effect of a cyber attack is used to support conventional combat methods.

Today, a pure cyber war between states, which only use cyber attacks, is almost unthinkable. The technology and systems attacked by cyber can, in most cases, be restored relatively quickly. So a conflict can not be resolved only by attacking the technology of a country. Thereby, no country will, presumably, react only with cyber if attacked through cyberspace. If a conflict evolves, a nation will use all possible means to decide the conflict toward its advantage. This can, besides

using offensive cyber, be at political, diplomatic or economical levels, or by using kinetic military means.

1.4 Relevance

Many cyber attacks will not be lethal and will not be able to inflict permanent damage to physical objects. This is of course extremely dissimilar from nuclear weapons, and other traditional weapons of war (Libicki, 2009). Moreover, cyberspace is a relatively new terrain of which the boundaries are not clear, and where the legal aspects are under construction.

Defending ourselves against cyber threat will blur the borders between military, economical, civil and other networks. This will definitely lead to a more comprehensive approach in cyber security and integration of processes and procedures. This process is already happening.
Cyber offense (i.e. the military use of cyber as a non-kinetic and non-lethal weapon) is a topic that needs more investigation. What exactly is cyber offense and what can be achieved with the use of offensive cyber? It is expected that in time, with the availability of cyber assets, the options of warfare multiply, the dimension of warfare changes and current military decision making and planning processes will be modernised.

Many countries are building a Cyber Command or Task Force now. This is done because they are convinced that cyber is a future capability, opportunity and thus possibility in warfare. Even if NATO is not considering offensive cyber at this moment, individual countries like the US, UK, Norway (Forsvardepartementet, 2012) and the Netherlands, openly state that they investigate the possibility of using cyber offensive in the future. This can be as a reactive defence (i.e. counter attack), or as a first strike opportunity. However, investigating the opportunity will not automatically mean that these countries are really organising an offensive cyber capability.

1.5 Thesis

This master thesis will answer the following question:
"What are the possibilities of the use of offensive cyber as an offensive capability within the existing international legal framework?"
To answer this question the study will divide the thesis into two parts.

1. The first part will answer the question: *What is offensive cyber and what are its possibilities and capabilities?* This question will be answered in three chapters. Chapter 2 will deal with important definitions. Chapter 3 will explain what a cyber attack is and chapter 4 will discuss the whole of offensive cyber operations, in which the cyber attacks are an essential part. Offensive use of cyber is new within modern warfare. Therefore it is important to describe and explain cyber attacks and offensive cyber operations thoroughly. This basis is necessary to understand the situation and details of the cases described in chapter 6.
2. The second part will answer the question: *What are the challenges for offensive cyber operations to comply with the existing international legal framework*? This question will be answered in two chapters. Chapter 5 will discuss aspects in the existing international legal framework that are unambiguous for regular war scenarios, but seem difficult to interpret when it comes to cyber operations. In chapter 6 three principles of the Law of War will be reflected via four different cases of cyber attacks that have occurred in the near past. This will tell whether and how offensive operations fit in, and comply with the existing international legal framework, and whether cyber operations can be used by western sophisticated democratic countries as a supplement to the currently available weapons.

1.6 Restrictions/Boundaries/Out of Scope

1. This thesis will use the existing international and humanitarian law to analyse the several cases and discuss offensive cyber operations. The thesis will not discuss national law or national regulations of any specific country.
2. Offensive cyber is a weapon that for this study is considered to be only used by official military organisations. Otherwise this thesis considers offensive cyber as cyber crime and cyber terrorism, which is a non-legal use of cyber, and therefore falls outside the scope of this thesis.
3. Non-state actors and individuals using cyber are out of this thesis' scope. Nation-state attacks on non-state actors are also not in the scope of this thesis. This thesis considers only cyber attacks from nation-state to nation-state.
4. Beside the introduction, where this study explains the position of offensive cyber in cyberspace and the relations to cyber security (which includes cyber defence), the

thesis will not further discuss the role of cyber security and will neither go in depth in the terms itself.

5. The principle of self-defence, which can imply the use of offensive cyber as a reaction, or used pre-emptively, will also be considered as cyber defence and therefore not specifically discussed, but sometimes mentioned.
6. NATO will, as an organisation, not discuss and develop the use of offensive cyber in the near future, as described in the previous sections. This thesis will therefore not discuss NATO's point of view any further, but considers the possible use of offensive cyber as an option for every individual modern country that respects and acts according the globally accepted international legal framework (such as Law of Armed Conflict, (Customary) International Humanitarian Law and UN Charter).

1.7 Method and Sources

The study will use the qualitative method to analyse reports, books and publications related to cyber in general, and offensive cyber specifically. The thesis will only make use of unclassified sources to do the research.
The first part of the study will be a theoretical, qualitative and explaining study. In that part the study describes what offensive cyber is, what the role is of offensive cyber in cyber space, the characteristics of offensive cyber, and why offensive cyber can be a useful asset.

In the second part of the study the gained theory on offensive cyber in relation with the legal framework will be discussed. This part is also theoretical and qualitative. Chapter 6 will be a case study, where three important principles of the existing international law will be reflected and considered in four cases:

1. Estonia (cyber attack on social media, internet sites, etc. by assumingly Russia),
2. Georgia (military cyber attack from Russia on Georgia, during the short Georgia-Russian war),
3. Stuxnet (attack on an Iranian nuclear power plant with a virus, which infected a thousands of windows computers around the world) and
4. The special case of Libya (the US considered using offensive cyber to disable enemy radar installations, but at the end decided not to do so).

The study will use three important parameters/principles within the international legal framework: proportionality, necessity and distinction. The outcome of the case study will tell whether and how offensive cyber operations can be a possible additional asset to nations' offensive capabilities.

2 Cyber Definitions

2.1 Introduction

Cyber is hot. When reading the newspapers and discussions on the internet you notice every day messages and articles about cyber warfare, cyber space, cyber attacks, etc. This paper, however, will mainly discuss the offensive side of cyber. It is still important to define and explain the most used cyber terms. The terms discussed in this chapter form the basis of further analysis and will be used throughout the paper. This chapter will define the terms cyber space, cyber war and cyber attack. The definitions of Cyber crime and Cyber terror will be described in Annex A, because they are out of the scope of this paper. However, it is important to show the differences between the different kinds of cyber attacks, and show the difference between the use of offensive cyber by a nation state, and by criminal organisations, terrorists or other non-state actors.

2.2 Cyber Space

Cyber is a relative new term. The term 'cyber' was first used in 1982 by the American writer William Ford Gibson in his book 'Burning Chrome'. The story is about two computer users who used hardware and software to break in the computer system of a criminal, which also contained financial information (Sundseth, 2012). Since then, cyber has become a general accepted term. Today cyber can not be excluded in the world of computers and networks, and it even has its own domain: cyber space.

The expansive, global nature of cyberspace and the rapid rate of change of ICT (Information & Communication Technology) make defining cyberspace a challenge. Dr. Dan Kuehl, an information operations expert at the United States National Defence University identified over a dozen definitions of cyberspace in circulation, ranging from Google's '*the place between the phones*' to several variations within the United States Department of Defence (Kuehl, 2008) .
In the October 2008 update of Joint Publication (JP) 1-02, the official US military dictionary, defined cyberspace as a "*global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*" (DoD, 2011, s. 86). This definition still stands in the November 2011 update.

NATO's CCD CoE (Cooperative Cyber Defence Centre of Excellence) in Tallinn, Estonia, rephrased this definition and looked further than just the physical layer of computers, networks and systems. CCD CoE identified that the definitions do not properly address the dynamic nature of cyberspace. In order to correct this they came to the following definition:

"Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems" (Ottis & Lorents, 2010, s. 2).

Note that they have included the human users in the definition. Cyberspace is an artificial space, created by humans for human purposes (Ottis & Lorents, 2010).
President George Bush Jr. underscored the US national security implications of cyberspace when he characterised it as the nervous system of the nation's critical infrastructures, controlling public and private institutional assets in all possible thinkable sectors, such as food, water, government, energy, etc. (Bush, 2003, s. 5-6).

2.3 Cyber War

The definition of cyberspace provides the basis for defining cyber war. Richard Clarke, Presidents Clinton and Bush's national coordinator for security, infrastructure protection and counterterrorism, and yearly guest speaker at the Masterstudy at the Norwegian Defence University College, gives a good definition on cyber war in his book 'Cyber War: The Next Threat to National Security and What To Do About It'. He defines cyber war as:

"Cyber war are actions by a nation state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke & Knake, 2010, s. 6).

This definition can be explained as if cyber warfare consists of military acts in the digital domain. Clarke is talking about actions of nation states, which has a direct connection with the legal aspects of cyber warfare. Because of these aspects, this is the definition that will be used in this paper.

2.4 Cyber Attack

> Cyber attacks can include a wide-range of technical and social methods to pursue an ultimate goal; the propagation, extraction, denial, or manipulation of information. The US military, in particular, has engaged in an extensive analysis of cyber attacks, and its definitions are widely used today, even though these definitions are generally considered to have weaknesses (Klimburg & Tirmaa-Klaar, 2011, s. 6-7).

As seen with the previous definitions, there are no single definitions that cover the whole spectrum, as every scientist views cyber from a different point or interest. The terminology used by the US DoD however, does cover the majority of attacks and attack-types experienced in cyberspace. The military definition of cyber attacks is largely covered by the term Computer Network Operations (CNO).

CNO can be defined as "***actions taken to defend, exploit and/or attack information resident on Information Systems (IS) and/or the IS themselves"*** (Bernier & Treurniet, 2010, s. 229).

> CNO itself includes Computer Network Attack (CNA), Computer Network Exploitation (CNE) and Computer Network Defence (CND). CND includes a wide number of different approaches and organisations, of which the most significant are specific entities often known as CERTs (Computer Emergency Response Teams) and which also represent a basic element of civilian cyber security (Klimburg & Tirmaa-Klaar, 2011, s. 6).

CNA is defined as "**Operations designed to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"** (DoD, 2006, s. GL-6), while CNE is defined as "**enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks"** (DoD, 2006, s. GL-6).

> These definitions therefore effectively differentiate between 'offensive actions' (CNA) and 'espionage' (CNE). The difference is that CNA is most likely an act of war, and CNE most likely not. This segmentation is problematic for a number of reasons. Not the least because, technically, CNA requires CNE to be effective (see Figure 1)(Klimburg & Tirmaa-Klaar, 2011, s. 7).

In other words, what may be preparations (the reconnaissance phase, see chapter 3) for cyber warfare, can well be cyber espionage initially, or simply be disguised as such (Klimburg & Tirmaa-Klaar, 2011, s. 7).

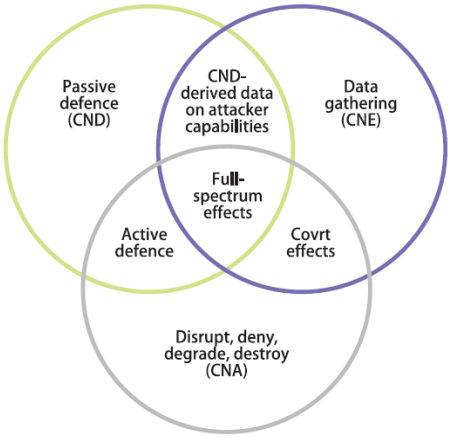

Figure 1: CNO model with overlap between CNO disciplines (Bernier & Treurniet, 2010, s. 230)

As Cyber attacks are widely covered by the term CNO, CNO is just a part of the whole that is called cyber operations. The US considers cyber operations as: "*the employment of cyberspace capabilities where the primary purpose is to achieve military objectives or effects in or through cyber space"* (DoD, 2011, s. 86).

Cyber operations can be either offensive or defensive[2]. This paper will focus on the offensive cyber operations, which can, from a military point of view, be defined as "***actions taken in the cyber environment to deny the actual or potential adversary's use of or access to information or information systems and affect their decision-making process"*** (Bernier & Treurniet, 2010, s. 230).

Besides the military use of offensive cyber operations there are also other parties that can attack in cyber space. These cyber attacks are not legal and can be distinguished as cyber crime and cyber terror (Annex A), and fall out of the scope of this thesis.

[2] Defensive cyber operations: "actions taken in the cyber environment to protect one's own information and information flow, and maintain freedom of action in the cyber environment for friendly decision-makers" (Bernier & Treurniet, 2010, s. 230).

3 Characteristics of Cyber Attack

3.1 Introduction

In the future, the ultimate goal of warfare will presumably not change. “However, the tactics of war are radically different in cyberspace, and if there is a war between major world powers, the first victim of the conflict could be the Internet itself” (Geers, 2011, s. 26).
Looking to the future, the Internet will change the nature of warfare. Computers are both a weapon and target. In fact, cyber warfare may favour nations who are robust in IT (Information Technology), but the Internet is a prodigious weapon for a weaker party to attack a stronger conventional enemy. Internet-dependent nations have more to lose when the network goes down (Geers, 2011), as the Estonia 2007 case will show.

This chapter concentrates and zooms in on the characteristics of cyber attack. This background is important, because it provides understanding for the later case studies. This chapter will answer the question: What is a cyber attack? It focuses on all kind of facets that directly involve a cyber attack, such as technology, infrastructure, attribution, approaches, operational considerations and effects. In the next chapter this paper will discuss and zoom out to the opportunities of offensive cyber operations, in which cyber attack and its characteristics play an important role.

3.2 The Basic Technology of Cyber Attack

3.2.1 Information Technology and Infrastructure

“Before considering the basic technology of cyber attack, it is helpful to review a few facts about IT in general, and today’s IT infrastructure in special” (Dam, Lin, & Owens, 2009, s. 82).

1. “The world of IT, internet, WiFi[3], networks, operating systems and applications is not restricted to any nation’s military. It is globally available and accessible, to nations large and small, to sub-national groups and to individuals” (Dam et al., 2009, s. 82).

[3] WiFi: Wireless Fidelity, also called Wireless Local Area Network (WLAN)

2. “The basic use and demands of this technology are determined largely by commercial needs rather than military needs. Military IT leans heavily on commercial IT rather than the reverse”(Dam et al., 2009, s. 82).
3. “A great deal of the IT infrastructure is shared among nations and between civilian and military sectors. Systems and networks used by many nations are built by the same IT vendors. Government and military users often use commercial Internet Service Providers (ISP), which consequently mean that private entities have considerable influence over the environment in which any cyber conflict may take place” (Dam et al., 2009, s. 82).

3.2.2 Vulnerability, Access and Payload

A successful cyber attack requires a vulnerability, access to that vulnerability and a payload to be delivered. Simply put in metaphors, a vulnerability might be an easily pickable lock in the file cabinet. Access would be an available path for reaching the file cabinet. From an intruder’s perspective, access to a file cabinet located on the International Space Station, would pose a very different problem from that, in relation with the same cabinet being located in an office in NATO HQ in Brussels. The payload is the action taken by the intruder after the lock is picked. For example, one can destroy the papers inside or one can alter some of the information on those papers (Dam et al., 2009, s. 83).

3.2.2.1 Vulnerabilities

A vulnerability is a weakness that from an attacker’s point of view is a chance to exploit.

Such weaknesses may be accidentally introduced through a design or implementation flaw, but may also be introduced intentionally. An unintentionally introduced defect (‘bug’) may open the door for opportunistic use of the vulnerability by an attacker who notices its existence (Dam et al., 2009, s. 83).

Attackers with the time and resources may also discover unintentional defects that they protect as valuable secrets, also known as zero-day exploits. As long as those defects are unknown to the owner or user of the system, the vulnerabilities of the zero-day exploit may be used by the attacker” (Dam et al., 2009, s. 83).

Two additional factors have increased opportunities for the attacker:

1. "The use of software in society has grown rapidly in recent years, and the sheer amount of software in use continues to expand across societal functions. More software in use, inevitably means more vulnerabilities" (Dam et al., 2009, s. 84).
2. "Software has also grown in complexity, and is difficult to understand, evaluate and test. In addition, software is generally developed to provide functionality for a wide range of users and for any particular user only a limited set of functionality may actually be useful. But whether used or not, every available capability presents an opportunity for new vulnerabilities" (Dam et al., 2009, s. 84).

Through covert and non-public channels, nation-states may even be able to persuade vendors or willing employees of those vendors to insert vulnerabilities, secret 'back doors', into commercially available products, or require such insertion as a condition of export approval". These actions can be done by "appealing to their patriotism or ideology, bribing, blackmailing or extorting them or applying political pressure. In other situations, a nation-state may have the resources to obtain (steal, buy) an example of the system of interest (Dam et al., 2009, s. 85).

Some vulnerabilities useful to cyber attackers are:

1. **Software**. "Application or system software may have accidentally or deliberately introduced flaws" (Dam et al., 2009, s. 85).
2. **Hardware**. "Vulnerabilities can also be found in hardware, including microprocessors, power supplies, storage devices, etc. Tampering with such components may secretly alter the intended functionality of the component or provide opportunities to introduce hostile software" (Dam et al., 2009, s. 85). In the Stuxnet case in chapter 6, this vulnerability is exploited.
3. **Seams** between hardware and software. "An example of such a seam might be the reprogrammable read-only memory of a computer (firmware) that can be improperly and clandestinely reprogrammed" (Dam et al., 2009, s. 85).
4. **Communications channels "**between a system or network and the 'outside' world can be used by an attacker in many ways. An attacker can for example pretend to be an 'authorised' user" (Dam et al., 2009, s. 85).
5. **Configuration**. "Most systems provide a variety of configuration options that users can set, based on their own security versus convenience needs. Because

convenience is often valued more than security, many systems are, in practice, configured insecurely" (Dam et al., 2009, s. 85).

6. **Users and operators**. Authorised users and operators of a system or network can be tricked, manipulated or blackmailed by the later attacker. The next section (Access) will go deeper in this vulnerability (Dam et al., 2009, s. 85).
7. **Service providers**. "Many computer installations rely on outside parties to provide computer-related services, such as maintenance or internet service. An attacker may be able to persuade a service provider to take some special action on its behalf, such as installing attack software on a target computer" (Dam et al., 2009, s. 86)

3.2.2.2 Access

In order to take advantage of a vulnerability, a cyber attacker must have access to it. Targets that are 'easy' to attack are those that involve relatively little preparation on the part of the attacker, and where access to the target can be gained without much difficulty. An example is a target that is known to be connected to the internet, such as public websites (Dam et al., 2009, s. 86).

Difficult targets are those that require a great deal of preparation on the part of the attacker and where access to the target can be gained only at great effort or may even be impossible for all practical purposes. In general, it would be expected that an adversary's important and sensitive computer systems or networks would fall into the category of difficult targets (Dam et al., 2009, s. 86).

Access to a target can be obtained by three different categories of cyber attack that may overlap:

1. **Remote-access cyber attacks**. This way of cyber attack is launched at some distance from the adversary computer or network of interest. A typical example of a remote access attack is that of an adversary computer attacked through the access path provided by the Internet, dial-up modem or a WiFi-network (Dam et al., 2009, s. 87).
2. **Close-access cyber attacks.** These are cyber attacks in which "an attack on an adversary computer or network takes place through the local installation of hardware or software functionality by friendly parties (e.g., covert agents, vendors) in close proximity to the computer or network of interest. Close access is a possibility anywhere in the supply chain of a system that will be deployed and it may well be

easier to gain access to the system before it is deployed" (Dam et al., 2009, s. 87). In the Stuxnet case it said this was a probable way of infection.

3. **Social engineering:** Compromise of operators, users and service providers. Human beings who operate and use IT systems of interest constitute an important set of vulnerabilities for cyber attack. They can be compromised through recruitment, bribery, blackmail, deception or extortion and even removable media devices dropped in parking lots (i.e. an often used method to get access in a closed system. This is another possible way of infection in the Stuxnet case). In many instances involving the compromise of users or operators, the channels for compromise often involve e-mails, instant messages or files that are sent to the target at the initiative of the attacker (Dam et al., 2009). In an experiment at West Point in 2004, an apparently legitimate e-mail was sent to 500 cadets asking them to click on a link to verify grades. Despite their start-of-semester training (including discussions of viruses, worms, and other malicious code or malware), over 80 percent of recipients clicked on the link in the message (Ferguson, 2005).

Close-access attacks and social engineering are activities in which national intelligence agencies specialise. In practice, it is often cheaper and easier to compromise a person than it is to break through firewalls and decrypt passwords. So in many situations human subversion and physical action are the two quickest, cheapest and most effective methods of attacking a computer system or network (Dam et al., 2009, s. 106).

3.2.2.3 Payload

"Payload is the term used to describe the things that can be done once a vulnerability has been exploited" (Dam et al., 2009, s. 88).

Payloads can have multiple capabilities when inserted into an adversary system or network, so they can be programmed to do more than one thing. The timing of these actions can also be varied. If a communications channel to the attacker is available, payloads can be remotely updated (Dam et al., 2009, s. 88).

Annex B (Techniques) shows a list of all kinds of techniques, which can be used as payload, such as a Trojan horse[4] or a rootkit[5]. For discussion on the most useful techniques it is essential to keep the different levels of operations in mind: offensive cyber operations at strategic level might use other techniques than cyber operations at tactical level.

> Once a payload is introduced into a targeted system, the payload sits quietly and does nothing harmful most of the time. But at the right moment, the program activates itself and proceeds to destroy or corrupt data, disable system defences or introduce false message traffic. The 'right moment' can be triggered because a certain date and time is reached, because the payload receives an explicit instruction to activate through some covert channel, because the traffic it monitors signals the right moment or because something specific happens in its immediate environment (Dam et al., 2009, s. 88),

like in the Stuxnet case in chapter 6.
"Payloads for cyber attack may be selective or indiscriminate in their targeting. This means that some payloads for cyber attack can be configured to attack any computer to which access may be gained and others can be configured to attack quite selectively only certain computers" (Dam et al., 2009, s. 89) as in the Stuxnet case.

3.2.3 Attribution

The Internet's puzzling architecture permits cyber attackers a high degree of anonymity. They can route attacks through countries with which the victim's nation-state has deprived relations (NATO, 2010b). Many cyber experts agree that the main challenge, from a defensive point of view, is the ability to attribute the offense. Accurate attribution is important when considering whether to take action, or to retaliate using military force to address an attack. In the cyber realm, attribution is far more difficult than in the realms of nuclear and conventional forces (Kugler, 2009, s. 337-338).

[4] Trojan Horse: a program that appears to be innocent but in fact has a hostile function that is triggered immediately or when some condition are met (Dam et al., 2009, s. 88).

[5] Rootkit: is a program that is hidden from the operating system or virus checking software but that nonetheless has access to some or all of the computer's functions. Rootkits can be installed in the boot-up software of a computer and even in the BIOS ROM hardware that initially controls the boot-up sequence (Dam et al., 2009, s. 88).

If an attack is not attributable this is a significant violation of the Law of War, especially the principle of distinction, as will be discussed in chapter 5 and 6. There is no standard for how much evidence for attribution of the attack is required. The open question is whether a target state can lawfully act against the likely source of the attack, even though the target is by no means certain that the attacks originated there. This fact would give many cyber attacks credible deniability, especially since in many cases nations can plausibly claim that the attacks may have originated from within their territory but their governments did not initiate them (Libicki, 2009). This 'attribution problem' is very much present in the Stuxnet, Georgia and Estonia cases in chapter 6. Attribution is a sensitive and difficult activity with technical, political and legal implications. For a nation-state attacker in modern sophisticated western democracies the attribution problem can hamper, and be a major problem in planning and executing effective offensive cyber operations.

3.2.4 Phasing of a Cyber Attack

Searching for vulnerabilities, finding an access path, determine the right payload and deciding how to attack are not actions that can be executed instantly. That needs planning. Despite using the most advanced technology, the phases of a cyber attack generally follow the same pattern. Although there are different theories and models about the phasing of cyber attacks, they all include the following:

1. **Reconnaissance** of the intended victim. By observing the normal operations of a target, useful information can be obtained such as used hardware and software, and regular and periodic communications. Commonly CNE takes place in this phase. Before executing a cyber attack in a continuous changing cyber space the reconnaissance phase is one that is essential, must be executed very thoroughly and therefore, is time-consuming.
2. **Penetration**. Until an attacker is inside a system, there is little that can be done to the target except to disrupt the availability or access to a service provided by the target.
3. **Identifying and expanding the internal capabilities** by viewing resources and increasing access rights to more restricted, higher-value areas of the victim system.
4. **Attack.** The intruder does the damage to a system or confiscates selected data and/or information.

5. **Removal.** The last phase can include the removal of any evidence of a penetration, theft and so forth, by covering the intruder's electronic trail by editing or deleting log files (Janczewski & Colarik, 2008, s. xv).

Janczewski and Colarik state that at the end, an attacker wants to complete all five stages successfully (Janczewski & Colarik, 2008).

3.3 Operational Considerations

The previous section addressed the basic technologies of, and approaches to cyber attack. This section considers the operational implications of using cyber attack. It will zoom out to discuss the effects and damage assessment, which this paper will revisit during the case studies.

3.3.1 The Effects of Cyber Attack

> Although the ultimate objective of using any kind of weapon is to deny the adversary the use of some capability, it is helpful to separate the effects of using a weapon into its direct and its indirect effects". The direct effects of using a weapon are experienced by its immediate target, while the indirect effects of using that weapon are associated with the follow-on consequences. "For example a runway may be damaged (the direct effect) so that the aircraft cannot land or take off (the indirect effect). This distinction between direct and indirect effects is particularly important in a cyber attack context (Dam et al., 2009, s. 110).

3.3.1.1 Direct Effects

The range of possible direct targets for a cyber attack is quite broad. Nevertheless, they all have in common that they seek to cause a loss of integrity, a loss of authenticity or a loss of availability as a direct effect (which includes theft of services):

1. **Integrity**. "An attack on integrity seeks to alter information (a computer program, data or both) so that under some circumstances of operation the computer system does not provide the accurate results or information that one would normally expect"(Dam et al., 2009, s. 111).
2. **Authenticity.** "An authentic message is one that is known to have originated from the party claiming to have originated it. An attack on authenticity is one in which the source of a given piece of information is obscured or forged. A message whose

authenticity has been compromised will fool a recipient into thinking it was properly sent by the asserted originator" (Dam et al., 2009, s. 111). This will influence the adversary's confidence in its system.

3. **Availability**. "A secure system is available for normal use by its rightful owner even in the face of an attack. An attack on availability may mean that e-mail sent by the targeted user does not go through, or the target user's computer simply freezes or the response time for that computer becomes intolerably long (possibly leading to catastrophe if a physical process is being controlled by the system)" (Dam et al., 2009, s. 111; Lin, 2010, s. 67-68).

These attributes may be targeted separately or together.

> In some situations integrity is the key target, as it might well be for a tactical network. A commander, who doubts the trustworthiness of the network used to transmit and receive information, will have many opportunities for second-guessing himself, and the network may become unreliable for tactical purposes. In other situations authenticity is the key target. A cyber attack may take the form of a forged message apparently from a unit's commanders to move from one location to another. (Dam et al., 2009, s. 112)

"And in still other situations availability is the target. A cyber attack may be intended to turn off the sensors of a key observation asset, for the few minutes that it takes for kinetic assets (e.g., airplanes) to fly past it" (Dam et al., 2009, s. 111), as was the plan in the Libya 2011 case in chapter 6.

> The direct effects of some cyber attacks may be easily reversible. Reversibility means that the target of the attack is restored to the operating condition that existed prior to the attack […] If backups are available for example, an attack on the integrity of the operating system may take just a few minutes of reloading the operating system. Many effects of kinetic attacks are not as easy to reverse (Dam et al., 2009, s. 111).

3.3.1.2 Indirect (and Unintended) Effects

> Although the direct effects of a cyber attack relate to computers, networks or the information processed or transmitted therein, cyber attacks are often launched in order to obtain some other, indirect effect and in no sense should this indirect effect be regarded as secondary or unimportant.

> The adversary air defence radar controlled by a computer is of greater interest to a military commander in the field than the computer itself, and the adversary's generator controlled by a computer is of greater interest to a headquarter than the computer itself (Dam et al., 2009, s. 113).

> Indirect effects are generally not reversible. Imagine a cyber attack that disrupts a computer controlling a generator. The attack on the computer may be reversible (leaving the computer as good as new), but the follow-on effect, the generator overheating and destroying itself, is not. […] Cyber attacks are particularly well suited for attacks on the psychology of adversary decision makers who rely on the affected computers (Dam et al., 2009, s. 113).

In this case such effects can be regarded as indirect effects.
For example, "a single database that is found to be deliberately corrupted, even when controls are in place to prevent such corruption, may call into question the integrity of all of the databases in a system. Awareness of the fact that a database may have been compromised has definite psychological effects on a user" (Dam et al., 2009, s. 113).

> The unintended consequences of a cyber attack are almost always indirect effects. For example, a cyber attack may be intended to shut down the computer regulating electric power generation for an enemy air defence facility. The direct effect of the cyber attack could be the disabling of the computer. The intended indirect effect is that the air defence facility loses power and stops operating. However, if unknown to the attacker, an enemy hospital is also connected to the same generation facility (i.e. a dual-use system[6]), the hospital's loss of power and ensuing patient deaths are unintended indirect effects of that cyber attack (Dam et al., 2009, s. 114).

3.3.2 Effects Prediction and Damage Assessment

The possible effects of a cyber attack are very important to know beforehand for planning purposes. After the attack it's important to determine if the attack had its desired effect. In the cyber realm "munitions effects and damage assessment are complex and difficult challenges, because the effectiveness of cyber weapons is a strong function of the intelligence available" (Dam et al., 2009, s. 121).

[6] 'Dual-use' is an adjective that is not found in the law governing the conduct of hostilities but that has been coined by the military in order to refer to objects that serve both civilian and military purposes. The label is primarily applied to essential civilian infrastructure such as electricity-generating installations and oil-refining facilities, which produce energy that is used by civilians and combatants alike. Other examples: telecommunication and computer networks and transportation networks (Boivin, 2006).

> In the kinetic world, weapons (or, more precisely, munitions) are aimed against targets. Predicting the effect of a weapon on a given target is important to operational planners, who must decide the most appropriate weapons-to-target matching […] Damage assessment for physical targets is conceptually straightforward. One can generally know the results of a strike by visual reconnaissance, although that may be deceived by on-the-ground details or adversary deception (Dam et al., 2009, s. 121).

Unlike conventional weapons, determining how many places are damaged in cyber space is difficult, since often damage is not apparent except under special tests. This encourages more massive attacks than necessary to be sure they cause sufficient damage. This, however, may violate the necessity principle of the Law of Armed Conflict, as will be discussed in chapter 5 and 6 (Janczewski & Colarik, 2008).

3.3.3 Possible Objectives of Cyber Attack

So far, the basic characteristics of cyber attack, the effects of cyber attack and the difficulty of cyber damage assessment is discussed. In this subsection the possible objectives of a cyber attack will be addressed. There are several objectives an attacker might want to obtain, whether a cyber attack is conducted remotely, through close access or social engineering.

1. Destroy a network or a system connected to the network. This means destroying the data stored within and/or eliminating the application or operating systems programs that run on that hardware.
2. Be an active member of a network and generate false traffic. This method is not in line with the distinction principle in the Law of Armed Conflict, which will be discussed in chapter 5 and 6.
3. Clandestinely alter data in a database stored on the network.
4. Degrade or deny service on a network. Distributed Denial-of-Service[7] (DDoS) attacks can be used to prevent an adversary from using a communications system and thereby force him to use a less secure method for communications.

[7] A Distributed Denial-of-Service (DDoS) attack is a coordinated effort that instructs PCs to send a victim a flood of traffic designed to overwhelm their servers or consume their bandwidth to degrade the quality of service available to network users (Nazario, 2009)(see also Annex B).

5. Assume control of a network and/or modulate connectivity, privileges, or service. “An attacker might assume control of an Internet service provider in an adversary nation and decide who would get what services and connectivity” (Dam et al., 2009, s. 114-115).

Thereby, cyber attacks can be carried out in conjunction with kinetic attacks, and often the effect of a cyber attack may be maximised if used in such a manner (Dam et al., 2009, s. 116)

3.4 Cyberspace Favours the Attacker

Several characteristics of cyberspace tilt the playing field in favour of the attacker. First, cyberspace has no boundaries. Second, cyberspace changes constantly. Sites are added and dropped daily, which means that assuming a new identity is far easier in cyberspace than it is in the physical world. What this means is that it is not possible to stop all attacks. Firewalls and intrusion prevention systems will thwart only so many attacks. Defenders must be right all the time, the attacker only once (Porche, Sollinger, & McKay, 2011).

William Lynn agrees on this. He states that in an offense-dominant environment, a fortress mentality will not work. Referring to the US, William Lynn states that the US cannot retreat behind a Maginot Line of firewalls or it will risk being overrun (Lynn, 2010).

Furthermore, mounting a response to a cyber attack requires knowing that such an attack has occurred. In cyberspace that is not necessarily easy. Malicious activity is common in cyberspace, but not all such activity constitutes an attack. However, they could pave the way for destructive activity or they could be used to plant a worm that, at some later time, could launch its own attack. Thus, the actual attack can occur days, weeks, or even months after the initial exploit (Porche et al., 2011).

Although the conduct of offensive cyber operations is internationally known, as shown in the introduction chapter, it is still a very sensitive matter. Nonetheless, it is much easier to execute an offensive cyber operation than to set up an effective cyber defence system. A defender rarely knows where, how and when the attacker will start his cyber operation. The challenge to effective defence is to patch all vulnerabilities, and the attacker’s opportunity lies in finding only that one key vulnerability in a complex system (Hunker, 2010). So offensive operations dominate and have the initiative in cyber space.

As we have seen, cyberspace as a war-fighting domain favours currently the attacker, which stands in contrast to our historical understanding of warfare, whereby the defender normally enjoys a significant home field advantage. Further, the terrestrial proximity of adversaries is unimportant because in cyberspace everyone is a next-door neighbour (Geers, 2011).

3.5 Subconclusion

This chapter showed that several characteristics of weapons for cyber attack are worthy of note (see also Figure 2).

1. A successful cyber attack requires a vulnerability, access to that vulnerability and a payload to be executed.
2. The indirect effects of weapons for cyber attack are almost always more consequential than the direct effects of the attack. That is, the computer or network attacked is much less relevant than the systems controlled by the targeted computer or network.
3. The outcomes of a cyber attack are often highly uncertain. Minute details of configuration can affect the outcome of a cyber attack and cascading effects often cannot be reliably predicted. One consequence can be that collateral damage and damage assessment of a cyber attack may be very difficult to estimate.
4. Cyber attacks are often very complex to plan and execute. Cyber attacks can involve a much larger range of options than most traditional military operations. Because they are fundamentally about an attack's secondary and tertiary effects, there are many more possible outcome paths. The time scales on which cyber attacks operate can range from tenths of a second to years and the spatial scales may be anywhere from 'concentrated in a facility next door' to globally dispersed.
5. The identity of the originating party behind a significant cyber attack can be concealed with relative ease compared to that of a significant kinetic attack (the attribution problem).
6. Offensive cyber operations, as part of an actor's larger cyber security, are more favourable in relation to only passive defensive measure.

	Kinetic Attack	Cyberattack
Effects of significance	Direct effects usually more important than indirect effects	Indirect effects usually more important than direct effects
Reversibility of direct effects	Low, entails reconstruction or rebuilding that may be time-consuming	Often highly reversible on a short time scale
Acquisition cost for weapons	Largely in procurement	Largely in research and development
Availability of base technologies	Restricted in many cases	Widespread in most cases
Intelligence requirements for successful use	Usually smaller than those required for cyberattack	Usually high compared to kinetic weapons
Uncertainties in planning	Usually smaller than those involved in cyberattack	Usually high compared to kinetic weapons

Figure 2: A Comparison of Key Characteristics of Cyber attack Versus Kinetic Attack (Dam et al., 2009, s. 80)

4 Offensive Cyber Operations

4.1 Introduction

In the previous chapter was described *what* a cyber attack is, by explaining the basic characteristics, let say the building blocks of a cyber attack, its effects and its possible objectives to attack. The chapter concluded that cyberspace favours the attacker. This chapter will zoom out and explain *how* cyber attacks can be deployed and used in offensive cyber operations.

Cyber operations are not meant to be independent operations but need to be part of a holistic approach in operations. The use of offensive cyber operations is also related to the topic of deterrence. If an actor is able and willing to conduct offensive cyber operations, it might deter, scare or at least dissuade a potential opponent. This chapter will discuss further, within the scope of offensive cyber operations, the utility, offensive considerations, deterrence, and the different offensive scenarios where cyber operations can be conducted. At the end of this chapter it will be clear what constitutes a cyber attack and offensive cyber operation. This includes their capabilities, possibilities, restrictions, and how offensive cyber operations can be used. In Annex C is also a list of important features of offensive cyber operations, which can be helpful for planners and researchers of offensive cyber operations. The theory in chapter 3 and 4 form the basis for the second part of the thesis, where the focus of offensive cyber will be on the existing Law of War.

4.2 Utility

This section describes the utility of offensive cyber operations, and how it relates to cyber security in general. The advantages of offensive cyber capabilities are, that during a crisis or ‘hot’ conflict, an attacker will benefit from a cyber-related attack, as soon as he neutralises, pre-emptively, the C4ISR (Command Control Communications Computers Intelligence Surveillance and Reconnaissance) capabilities of an opponent. That will make an opponent blind and he will also lose his nerve system, and thus his freedom of action. The offensive cyber capability is a sophisticated (military) instrument that can contribute to warfare if necessary, also while restricted by adequate Rules of Engagement (RoE’s), as some cases later will show (Minkwitz, 2003, s. 21).

It is also said, that there must be a balance between offensive cyber capabilities and defensive measures achieved, in order to attain an acceptable level of network security. Increased passive defensive measures can reduce vulnerabilities, thereby mitigating the threat of cyber-attacks. However, public and industrial interests will continue to challenge the strength of passive defensive measures, creating network vulnerabilities that can be taken advantage of. Therefore, an actor should not only rely on passive defensive measures, but offensive cyber capability also has the potential to reduce threat in the cyber space. Offensive cyber capabilities grant an attacker the ability to take direct action against a perceived threat, although there is a risk for attacking an innocent bystander (Marshall, 2010). Thereby it is advised to possess a large range of cyber capabilities to conduct different kind of cyber activities with far reaching effects, including defensive as well as offensive (Tettero & Graaf, 2010).

4.3 Offensive Considerations

Offensive cyber is not only a super weapon that enriches the arsenal of weapons and capabilities, and which is the hope of future warfare. It is a new, still to be discovered weapon that already raises some dilemmas. Richard Clarke, together with other scientists and military, is reserved in his stance on offensive cyber actions. He foresees some challenges and dilemmas that go together with an offensive posture in the cyber space:

1. **First use strike**. One of the parties in a crisis can decide to make the first move in cyberspace. An actor in a conflict might start with using offensive cyber operations, to signal both the seriousness with which the actor viewed the crisis, and to show its compelling capabilities (deterrence). On the other hand, first use can frame the public opinion. It can make a victim more politically acceptable in the eyes of the world to defend itself. That makes ‘first use’ for an actor, based on public opinion, very sensitive. In the case study in chapter 6 this dilemma will be addressed in the Libya case. On the other hand, in some cases (e.g. when an actor is confronting a strong cyber opponent) it is almost inevitable for an actor going in first, otherwise its capability to use the cyber space may be reduced by its opponent. Clarke calls it the ‘first mover advantage’ (Clarke & Knake, 2010). This dilemma has strong similarities with the dilemma of the use of (nuclear) Weapons of Mass Destruction (WMD) during the cold war.

2. **Preparation of the battlefield.** When a conflict with cyber-attacks occurs, both sides probably will have hacked previously into each other's systems and networks (for example by CNE in the reconnaissance phase of a cyber attack).
3. **Ambiguity of intent.** On one hand, an actor would like to eliminate a (military) command and control system with a cyber-attack, to prevent the political and military leadership from giving orders to their units, or to cut off certain units from their higher command. On the other hand, if there is a cyber-attack with such intent, it could be difficult to prevent or terminate a kinetic war. Cyber attacks should be carefully constructed so that there is still a surviving communications channel for negotiations and ways in which the leadership can order its forces to stop fighting.
4. **Escalation of a global war and collateral damage**[8]**.** This can be the case once cyber attacks start in a local conflict. Even in an age of intercontinental missiles and aircraft, cyber war moves faster and crosses borders more easily than any form of hostilities in history. Once nation-state has initiated war, there is high potential that other nations will be drawn in, as the attackers try to hide both their identities and the routes taken by their attacks. There can be the possibility of collateral damage, as malicious programs jump international boundaries and affect unintended targets (Clarke & Knake, 2010), as in the Stuxnet 2010 case.

4.4 Deterrence

A different, but important way of using offensive cyber as a weapon, is to use it to deter the opponent, or the environment. In general, deterrence is a state of mind. "It is the concept of one state influencing another state to choose not to do something that would conflict with the interests of the influencing state" (Beidleman, 2009, s. 16).

[8] 'Collateral damage' means incidental loss of civilian life, injury to civilians and damage to civilian objects or other protected objects or a combination thereof, caused by an attack on a lawful target (Doswald-Beck & Henckaerts, 2005).

4.4.1 US DoD

The subject of deterrence in cyber space is subject to research in the United States. The central idea of deterrence from the perspective of the US DoD is to decisively influence the adversary's decision-making process in order to prevent hostile actions against US vital interests (US Strategic Command, 2006). Deterred states decide not to take certain actions because they perceive or fear that such actions would produce intolerable consequences (Gray, 2000). The idea of influencing states' decisions assumes that states are rational actors "*willing to weigh the perceived costs of an action against the perceived benefits and to choose a course of action"* logically based on *"some reasonable cost-benefit ratio"* (Dorffa & Ceramib, 2001, s. 111). Thus, the efficiency of cyber deterrence relies on the ability to convince others that you can impose or raise costs and deny or lower benefits related to cyber attack, in a state's decision-making calculation. Offensive capabilities are the primary tools used to impose or raise those costs in deterrence.

Credible cyber deterrence is also dependent on a state's willingness to use these abilities and a potential aggressor's awareness that these abilities, and the will to use them, exist. In 2006, the US published the National Military Strategy for Cyber Operations with the expressed intent to achieve 'military strategic superiority in cyberspace' (Pace, 2006, s. vii). One of its main goals was to ensure that adversaries are deterred from establishing or employing offensive capabilities against US interests in cyberspace (Pace, 2006). However, the US is not alone in pursuing such cyber attack. Over 120 countries already have, or are developing computer attack capabilities (GAO, 1996). In addition to offensive means, defensive capabilities play a critical role in deterring cyber attack. Ultimately they reduce the probability of success that an aggressor will achieve its goals (Beidleman, 2009).

4.4.2 Legal Framework

The globalised interdependence of cyberspace requires a global solution against cyber aggression. Over and above offensive and defensive cyber capabilities, a robust, international legal framework, that addresses cyber aggression, is the most critical component of a comprehensive approach to deter cyber attack. International law and norms are fundamental to deterrence. Multilateral agreements provide the most efficient way of realising these shared interests (Freeman, 1997). International law provides, among others, a measure of protection to

states that lack robust defensive and offensive cyber capabilities, and serves as their first and possibly only line of deterrence.

Today, the lack of international norms, laws, and definitions to govern state actions in cyberspace has led to a gray area that can be exploited by aggressive states, as long as their actions skirt the loose thresholds stated in the UN charter (Tikk et al., 2008). A typical example of this is the reaction of the head of the Russian Military Forecasting Centre, in response to accusations of state-sponsored cyber war against Estonia. He stated that the attacks against Estonia *"had not violated any international agreements because no such agreements exist"*, suggesting that even if Russia's involvement could be proved, Estonia's options for reprisal were limited (Fritz, 2008, s. 61). Here the attribution problem thwarts deterrence, because it lowers the probability of reprisal, even if the attacker's identity is suspected.
In addition to a non-existent regulatory framework, ineffective attribution of cyber attacks further undermines deterrence in cyberspace and widens the exploitable gray area. The threat of offensive cyber capabilities will not deter aggression, if the attacked state cannot identify its attacker. Likewise, deterrence falters if one cannot identify whom to target with sanctions.

"While offensive and defensive cyber capabilities are critical to deterring aggression, employing these capabilities depends on robust international norms for state behaviour in cyberspace. So international law is the first line of deterrence in cyberspace" (Beidleman, 2009, s. 22).

4.5 Different Offensive Scenarios

In this section, all cyber offensive options from this and the previous chapter come together, and give some insight in how to use these offensive cyber capabilities in possible scenarios.

During diverse conflict scenarios, planners and decision-makers could opt for different sorts of offensive cyber operations, with the features of offensive cyber kept in mind. Rattray and Healey distinguished between different offensive cyber operations that may be a future utility. This paper will only discuss the scenarios in which nation-state military (cyber) forces can be involved.

1. **A surprise cyber-attack conducted by military force(s)** and directed towards military objectives of the opponent, followed by a major war, perhaps a traditional and kinetic war, possibly also by a mix of major kinetic and cyber-attacks. These

operations imply the ‘first use’ element. A historical comparison can be made with the aerial Japanese attacks on Pearl Harbour.

2. **Covert offensive cyber operations**, as an option between doing nothing in a situation in which vital interests may be threatened, and sending in military forces. Deterring covert operations is only credible if attribution is possible.
3. **Direct support for special operations**. Unlike their use in a Pearl Harbour kind of attack, offensive cyber operations could even more easily be used for targeted covert operations in support of special operations. These operations could disable the opponents alarm system or create false alarms, or the disruption of a voice-over-IP network. Gaining access is a critical first step.
4. **Operational support for traditional kinetic operations**. It could be that during a cyber conflict cyber-forces engage heavily, on both offense and defence, in support of conventional military operations. In some cases, the opponent may have cyber capabilities to shoot back, but at other times, it may be that one side has superiority of the cyber domain.
5. **Overt force-on-force cyber conflict with near-peer nation**. This is a stand-alone cyber conflict between nations fought entirely within the domain of cyberspace, and fully engaging each side’s attackers and defenders, probably both in government and private sectors. This category of cyber conflict may develop swiftly, through various phases moving up from smaller, less-organised attacks, growing into full force-on-force violence. However this scenario is a theoretical option, it must be said, as is mentioned before, that a cyber alone conflict is not apparent, as nations will probably not wait and see how the cyber battle develops, but use kinetic capabilities quickly to gain an advantage.
6. **Large covert force-on-force cyber conflict with near-peer nation**. It is possible that two national opponents might choose to engage in a long series of offensive operations that neither of the two is willing to admit publicly. A similar analogy may be the hot intelligence competition during the Cold War. The actions of secret agents and associated covert actions illustrate how two alliances can fight in the shadow and maintain plausible deniability to the world.
7. **Cyber threat removal**. An offensive cyber operation might also be an operation conducted to counter computers engaged in mass attacks. In such scenario, a nation state would identify botnet zombies or their controllers or masters and use offensive operations to keep them offline (Rattray & Healey, 2010, s. 83-92).

It can also be concluded that the scenarios show that offensive cyber can be used in the full spectrum of (cyber)war. However, if a western nation considers using offensive cyber capabilities, the operation should fit in the international agreed legal framework and the Law of Armed Conflicts (LoAC). This will be further discussed in the next chapters.

4.6 Subconclusion

Offensive cyber operations and cyber-attacks have some specific considerations, which make offensive cyber operations unique. The varied kind of cyber conflicts scenarios together with the used different kind of offensive cyber operations provides a good framework for researching and planning offensive cyber operations. The framework might also be useful considering whether offensive cyber operations are useful for a nation. However, the conduct of offensive cyber operations should be within the existing international legal framework. Thereby it can also be concluded that the scenarios show offensive cyber can be used in the full spectrum of (cyber)war. Offensive cyber can at one side of the spectrum be deployed in covert operations, but also used in SOF operations, regular conflict operations, and at the other end of the spectrum in the full overt offensive cyber operations.

Offensive cyber operations can be conducted independently, but that makes them less influential. The main objectives in an operation will be reached not only with cyber operations, but also by ‘boots on the ground’. Planners of offensive cyber operations should keep the dilemmas of ‘first use’, ‘preparation of the battlefield’ and ‘ambiguity of intent’ in mind. Those are important criteria to determine whether to deploy offensive cyber at the first place.

Deterrence is a different view on the use of offensive cyber. While offensive and defensive cyber capabilities are critical to deterring aggression, employing these capabilities depends on robust international norms for state behaviour in cyberspace. International law is the first line of deterrence in cyberspace. Still today there is no existing legal framework, made especially for cyber operations.

5 International Law and Ethics

5.1 Introduction

Looking at the legal aspects of cyber operations is essential, because cyber operations are already technological developed, and without restrictions cyber attacks can do a lot of harm. Military and politicians need to be assured that the use of offensive cyber has no legal restrictions or consequences. Knowing the legal restrictions and possibilities makes cyber useful in strategies and campaigns. Until today there is no special international cyber law, so we still have to act according the existing conventional Laws of War. Military ethicist Randall R. Dipert quoted in the article 'Do we need a Geneva convention for cyber warfare':

> "The urge to destroy databases, communications systems and power grids, rob banking systems, darken cities, knock manufacturing and health-care infrastructure offline, and other calamitous outcomes, is bad enough. But unlike conventional warfare, there is nothing remotely close to the Geneva Conventions for cyber war. There are no boundaries in place and no protocols that set the standards in international law for how such wars can and cannot be waged" (Solon, 2010).

As said before the cyber terminology is not clear. The danger of the multiple explanations of the different cyber terms, laws and cyber definitions among the different nations and institutions, is that nation-states might interpret international and customary law in different ways. This can lead to different reactions to the same kind of cyber-attack. For example, if two states have contrasting vocabulary for activities related to cyber conflict, one could view a cyber-attack as an act of war, while the other could see it merely as an act of cyber crime (Kaminski, 2010).

The lack of cyber law forces us to see the modern cyber methods of warfare in the light of the existing international laws and rules concerning warfare. This chapter looks deeper in the relationship between offensive cyber operations and the current Laws of War. Especially 'armed attack', 'use of force' and ethics will be highlighted. Looking at the offensive side of cyber warfare one speaks about a possible need for cyber arms control. This chapter will also shortly highlight this aspect.

In the next chapter this paper will look at some important principles of the existing Laws of War, in four cases of cyber operations that has occurred in the near past. This chapter will explain those principles at the end. The case study will eventually analyse whether and how cyber operations are suitable for application on the existing Laws of War, and why.

5.2 The Law of War

One of the purposes of the Law of War is to get states to behave in ways that are acceptable to the international community.

> The Law of War is divided into two principal areas. Jus ad bellum, also known as the law of conflict management, is the legal regime governing the transition from peace to war. It basically lays out when states may lawfully resort to armed conflict. Jus in bello, also known as the Law of Armed Conflict[9] (LoAC), governs the actual use of force during war (Carr & Shepherd, 2010, s. 48).
>
> Historically, the transition from peace to war fell under the prerogative of the sovereign; however, it came under international law following World War II with the ratification of the United Nations (UN) Charter. Although the UN Charter is not the only source of jus ad bellum, it is the starting point for all jus ad bellum analysis (Carr & Shepherd, 2010, s. 49).

The relevant articles of the UN Charter, which provide the framework for modern jus ad bellum analysis are Articles 2(4), 39[10] (with art 41[11] and 42) and 51 (UN, 1945), which will be discussed in the next section.

5.3 General Prohibition on the Use of Force

Article 2(4) prohibits states from employing *"the threat or use of force against the territorial integrity or political independence of another state, or in any other manner inconsistent with the Purposes of the United Nations"* (UN, 1945, s. Chapter I, Article 2).

---

9 "Law of (international) armed conflict" means all the principles and rules of treaty and customary international law binding on a State and governing armed conflict between States; the term "law of international armed conflict" is synonymous with "international humanitarian law relating to international armed conflict" (Doswald-Beck & Henckaerts, 2005).

10 Art 39: The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security (UN, 1945).

11 Art 41: The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations (UN, 1945).

> In effect, it criminalises both the aggressive use of force and the threat of the aggressive use of force by states as crimes against international peace and security. Although the UN Charter's protections apply only to states that are parties to it, the prohibitions of Article 2(4) are so widely followed that they have come to be recognised as customary international law (Doswald-Beck & Henckaerts, 2005), binding on all states across the globe (Carr & Shepherd, 2010, s. 49).

Thus, states may not threaten to use or actually use force against another state unless an exception is carved out within the UN Charter. This position is further supported by Article 2(3), which requires states to '*settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered*.' (UN, 1945, s. Chapter I, Article 2) Only two exceptions exist on the use of force:

1. The first exception is actions authorised by the UN Security Council (UNSC). Article 42 of the UN Charter allows the UNSC to use military force to restore international peace and security (UN, 1945, s. Chapter VII, article 42).
2. The second exception is self-defence. This right is recorded in Article 51 of the UN Charter, which proclaims that '*nothing in the present Charter shall impair the inherent right of states to engage in individual or collective self-defence*' (UN, 1945, s. Chapter VII, article 51) in response to an 'armed attack.'

The Charter, however, never defines 'armed attack'. This debate has become even more pronounced regarding cyber attacks, which are far more difficult to classify than traditional attacks with conventional weapons.

5.3.1 Cyber Attacks as Armed Attacks

While the law of war is comprised of well known and widely accepted principles, applying these principles to cyber attacks is a difficult task. This difficulty arises out of the fact that the law of war developed, for the most part, in response to conventional wars between states. When evaluating armed attacks in that paradigm, it was easy to assess the scope of an attack and the identity of an attacker. Unfortunately, when a cyber attack is in progress, it becomes difficult for states to assess the scope of an attack, or figure out who is responsible for it (the attribution problem). Whether cyber attacks can qualify as armed attacks, and which cyber attacks should be considered armed attacks are thus left as open questions in international law.

As stated before, 'armed attack' is not defined by any international convention.

> The framework for analyzing armed attacks is relatively well settled, as are the core legal principles governing its meaning. The international community generally accepts Jean S. Pictet's test as the starting point for evaluating whether a particular use of force constitutes an armed attack. Under Pictet's test, a use of force is an armed attack when it is of sufficient scope, duration and intensity (Carr & Shepherd, 2010, s. 58).

In the French-language version of the UN Charter, which speaks about 'armed aggression' rather than 'armed attack,' the UN General Assembly passed the Definition of Aggression resolution in 1974 (Assembly, 1974, s. resolution A/RES/3314(XXIX)).

> The resolution requires an attack to be of "sufficient gravity" before it is considered an armed attack. The resolution never defines armed attacks, but it does provide examples that are widely accepted by the international community. Although the resolution has helped settle the meaning of armed attacks for conventional attacks, the more technology has advanced, the more attacks have come in forms not previously covered by state declarations and practices. Consequently, states recognise that unconventional uses of force, may warrant treatment as an armed attack when their scope, duration and intensity are of sufficient gravity. As a result, states are continually making proclamations about new methods of warfare, slowly shaping the paradigm for classifying armed attacks (Carr & Shepherd, 2010, s. 58).

5.3.2 Ethical Attacks

LoAC (jus i bello) regulates how wars can be legally fought. The Hague Conventions (1899 and 1907) and Geneva Conventions (1949 and 1977) are the most important in this. While most cyber war attacks do not appear to fall into the category of 'grave breaches' or 'war crimes' as per the 1949 Geneva Conventions, they may still be illegal or unethical. Article 51 of the 1977 Additional Protocols of the Geneva Conventions prohibits attacks that employ methods and means of combat whose effects cannot be controlled or whose damage to civilians is disproportionate (ICRC, 2005, s. 32). Article 57 says '*Constant care shall be taken to spare the civilian population, civilians, and civilian objects*' (ICRC, 2005, s. 36).

Cyber weapons are difficult to target and difficult to assess in their effects. The Hague Conventions prohibit also weapons that cause unnecessary suffering (ICRC, 2005, s. 159).

5.4 Lack of Legal Framework.

Offensive cyber operations are not covered by an international agreed legal framework. The consequence is that it is hard to distinguish between the different kind of cyber attacks, their purpose, their origin and under which existing law the attacks fall. LoAC only covers the jus i bello kind of attacks. When the LoAC were first drafted, only nation-states had the legal ability to wage war and to execute operations. Since cyber attack weapons are easy available for everyone, non-state actors and even individuals are capable getting involved in cyber incidents, cyber operations or cyber conflict. Thus, the lines between state, non-state, and individual attackers are unclear in a legal regime that discriminates between LoAC on the one hand and national criminal laws and law enforcement on the other (Dam et al., 2009, s. 22).

The lack of a decent legal framework also endangers a decent distinction between cyber attacks conducted in the cause of warfare, or cyber attacks as a simple hacker's activity in the cause of law enforcement. The means and methods used by a nation-state to conduct cyber attacks can vary greatly and can also be classified in a number of ways. However, although this variety, these attacks can be similar if not identical to those used by hackers in the context of cyber crimes. Moreover, cyber attacks can occur both in times of peace and war (Palojärvi, 2009). The blurring in these different types of cyber attack makes the need for a general international accepted cyber legal framework even more necessary.

5.5 Cyber Arms Control

Cyber warfare is arguably the first major new form of warfare since the development of nuclear weapons and intercontinental missiles. This novelty means that at present there is a virtual policy vacuum (Libicki, 2009). As any computer is a potential cyber weapon and anyone with advanced knowledge of information systems is a potential cyber combatant, this makes treaties banning cyber weapons virtually impossible from the outset (Libicki, 2009).

However, as with nuclear bombs, the existence of cyber weapons does not in itself mean they will be used. Moreover, an attacker cannot be sure what effect an assault will have on another nation, making their deployment highly risky. All this creates a dangerous instability. Cyber weapons can easily be developed secretly, without discussion about how and when they might be

used. Nobody knows their true power, so nations must prepare for the worst (Economist, 2010). The Chatham House Report states that the shared objective of the arms control approach to cyber warfare would be to prevent a global arms race in cyber space (Cornish, Livingstone, Clemente, & Yorke, 2010).

The Norwegian legal expert on cyber, Stein Schjølberg, prefers a prominent role for the United Nations during the process of working towards a cyber space treaty. The creation of a global framework of a United Nations Cyberspace Treaty on cyber security and cyber crime should help develop a common understanding of all aspects of cyber security among countries at various stages of economic development. All stakeholders need to come to a shared understanding on what institutes cyber crime, cyber terrorism, cyber attack and other forms of cyber threats. That is prerequisite for developing national and international solutions that harmonise cyber security measures (Schjølberg, 2010).

From a defensive point of view cyber arms control is an understandable issue and an important part of cyber security. Nevertheless, a solution in which every nation agrees seems far away. From an offensive point of view offensive cyber operations offer such a huge increase in warfare opportunities, that it is a question whether cyber arms control will ever happen or will be effective.

Until a treaty is there, the military ethicist Dipert predicts a long Cyber Cold War, marked by limited but frequent damage to information systems, while nations, corporations and other agents test these weapons and feel their way toward some sort of equilibrium (Solon, 2010).

5.6 Preparation Case Study

5.6.1 Introduction

As seen in this chapter, the existing legal framework does not account for the existence and use of offensive cyber means. This means that it is important to deal as good as possible with the existing international legal framework concerning cyber, until a new ‘international cyber law’ is introduced.

This paper will use the LoAC further as a guideline, to determine if offensive cyber can be conducted properly, and if the cyber attacks can be conducted according these existing rules. First, LoAC applies only after armed conflict has been initiated, as in the case of jus i bello. Next, cyber incidents that correspond with the armed conflict must be attributable to a specific government. Then there is the issue of harmful intent. Did the cyber incident cause injury or damages (financial, physical or virtual)? (Carr & Shepherd, 2010, s. 36-37). Furthermore, under traditional LoAC, only a nation's military forces are allowed to engage in armed hostilities with another nation (Dam et al., 2009, s. 22).

Every attack within this framework must apply to principles, of which the three most important are:

1. **Proportionality,** which "requires actions to be limited to the amount of force necessary to defeat an ongoing attack or deter future aggression" (Carr & Shepherd, 2010, s. 72).
2. **Necessity,** means that force may only be used if it is essential to achieve the military objective (Defensiestaf, 2005, s. 35) and when a reasonable settlement could not be attained through peaceful means.
3. **Distinction** requires armed forces "to make reasonable efforts to distinguish between military and civilian assets and between military personnel and civilians, and to refrain from deliberately attacking civilians or civilian assets" (Dam et al., 2009, s. 247).

In the four cases in the next chapter, these three principles will be analysed and discussed whether and how they are applicable in that specific situation. The three principles will be explained further in the next subsections.

Humanity is also an important principle in the LoAC. Humanity prohibits the use of weapons designed '*to cause unnecessary suffering*' (ICRC, 2005, s. 22). Offensive cyber in this paper is considered a non-kinetic weapon, which, having direct and indirect effects, will probably not cause unnecessary suffering and does not have a harmful intent. Should this nevertheless happen as a side effect, this paper will consider that as collateral damage and a breach of one of the other three principles.

5.6.2 Proportionality

Understanding that attacks on legitimate targets will often cause incidental damage beyond the lawful target itself, proportionality limits the use of force to situations in which the expected military advantage outweighs the expected collateral damage to civilians and their property. This principle is derived from Additional Protocol I, Article 51(5)(b), which states that it is prohibited to use force that "*may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated"* (ICRC, 2005, s. 33).

In the traditional military realm of applied kinetic force, this principle manifests itself in notions such as the requirement that bullets remain fully jacketed, and the banning of hospitals, churches, and schools from all target lists, just to minimise unnecessary suffering (Mulligan & Growden, 2009). Cyber attacks are not kinetic, but must still apply to the proportionality principle, because damage inflicted can also have a huge indirect effect. It is difficult to evaluate whether an attack would be proportional, as the direct effects of cyber-attacks may be non-lethal or temporary. Furthermore, how should the temporary incapacity of critical systems be evaluated? For example, a cyber-attack that effectively stops the transmission of information through the Internet might merely inconvenience the populace, or it might result in hospitals being unable to communicate vital information, leading to loss of life (Hathaway et al., 2011). "LoAC always obligates an attacker to make reasonable proportionality judgements, for example in the event that military and non-military assets are organised as dual-use targets" (Dam et al., 2009, s. 246).

> Because cyber attacks exploit vulnerabilities of software, and the increasing standardisation of software means that military organisations often use the same software as civilians do, and much of this software has the same vulnerabilities, many viruses and worms that could cripple a command-and-control network could just as easily cripple a civilian network.[…] Military systems try to isolate themselves from civilian systems but are not very successful, because access to the Internet simplifies many routine tasks. Furthermore, information flow from civilian to military systems is often less restricted than flow in the other direction, which actually encourages an adversary to first attack civilian sites. […] It is easy to create disproportionately greater damage to civilian computers by a cyber attack, since there are usually more of them than military computers, and their security is often not as good. In addition, it can be tempting to attack civilian systems anyway for strategic reasons. Crippling a few sites in a country's power grid, telephone system or banking system can be more damaging to its capacity to wage war than

> disabling a few command-and-control centres, considering the back-up sites and redundancy in most military command-and-control systems (Rowe, 2008, s. 106-107).

This makes the proportionality principle for cyber attacks a more difficult principle.
Proportionality in the context of self-defence has both a quantitative and a qualitative dimension. In effect, proportionality means the action must be directed at ending the attack and preventing further attacks in the near future. Moreover, it must be in proportion to the scale of the attack. Proportionality does not presume a specific response to an attack, nor does it require the response to be of the same nature as the attack. A cyber attack that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber weapons or conventional weapons, provided the intention is to:

1. end the attack,
2. the measures do not exceed that objective
3. there are no viable alternatives.

The proportionality requirement rules out measures that harbour the risk of escalation and that are not strictly necessary to end the attack or prevent attacks in the near future (CAVV, 2011).

5.6.3 Necessity

Necessity limits the amount of force a state can use against legitimate targets, to the amount necessary to accomplish a valid military objective[12], and that only actions necessary for the defeat of the opposing side are allowed (ICRC, 2005). Lawful targets are combatants[13], military objectives and civilians directly participating in hostilities. An attack that may be necessary, but is expected to cause collateral damage which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited (HPCR, 2009).

Because cyber targeting is difficult and the expected effects are not always certain, the principle of distinction is an aspect that seriously can hamper lawful meaning of the attack, and can affect

[12] "Military objectives", as far as objects are concerned, are those objects which by their nature, location, purpose or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. (Doswald-Beck & Henckaerts, 2005)

[13] Members of the armed forces of a Party to a conflict (other than medical personnel and chaplains covered by Article 33 of the Third Convention) are combatants, that is to say, they have the right to participate directly in hostilities. (ICRC, 1977, s. art. 43)

the principle of necessity. In the context of self-defence, necessity usually refers to the existence of an armed attack, or the imminent threat of attack. Even then, it is only relevant if there are no alternatives, there is sufficient certainty regarding the identity of the author of the attack (the attacker must be attributable) and the self-defence measures can be taken in a targeted and proportional manner (CAVV, 2011).

> Valid targets are limited to those that make a direct contribution to the enemy's war effort, or those whose damage or destruction would produce a military advantage because of their nature, location, purpose, or use. Thus, enemy military forces (and their equipment and stores) may be attacked at will, as is also true for civilians and civilian property that make a direct contribution to the war effort. Assets that do not contribute to the war effort or whose destruction would provide no significant military advantage may not be deliberately targeted by cyber or kinetic means. LoAC also provides for a category of specially and (in theory) universally protected facilities such as hospitals and religious facilities (Dam et al., 2009, s. 246).

The difficulty in the principle of necessity is, as with the principle of proportionality, the judgement and targeting of dual-use targets, which makes it risky and uncertain to predict the outcome, assess the damage and judge the military advantage in relation to the damage occurred.

5.6.4 Distinction

Distinction is the requirement that "*parties to the conflict shall at all times distinguish between the civilian population and combatants and shall direct their operations only against military objectives"* (Doswald-Beck & Henckaerts, 2005, s. 25). However, distinction does not protect civilians who directly participate in hostilities (ICRC, 2005).

The IHL rule of distinction is particularly hard to apply in today's interconnected computer networks, which render the line distinguishing between civilian and military targets particularly blurred. The reason for that is that military objectives which can be attacked, and civilian objects which must be respected are often dual-use targets and often based on SCADA[14] (Supervisory Control and Data Acquisition) systems. While the legality of potential cyber attacks may often be clear, the non-lethal potential of cyber warfare may lead to more frequent

[14] These systems are designed for real-time data collection, control and monitoring of critical infrastructure including power plants, oil/gas pipelines, refineries or water systems (Shakarian, 2011, s. 2).

violations of the principle of distinction than in conventional warfare. Naturally, this civilian-military intermingling raises a further problem associated with modern warfare, as it further worsen the difficulty in dealing with dual-use targets (Hathaway et al., 2011; Papanastasiou, 2010). Papanastasiou believes: "[…] nevertheless, it has to be admitted that the NATO bombardment in April 1999 of the Serbian media station RTS in Kosovo resulting in 16 casualties, could have been bloodless had it been effectuated via a cyber attack" (Papanastasiou, 2010, s. 25).

The principle of distinction also means that our own forces must adhere to the LoAC. On the modern battlefield as part of the LoAC, legitimate war fighting agents must wear the uniform of the country for which they fight. In the cyberspace domain, no equivalent practice exists. The practice which most nearly serves the same purpose would be for the military to always operate from the same set of IP addresses, intentionally never faking its identity. Cyber attacks than can easily be attributed. However, this practice would severely cripple the capabilities of cyber operations. The strength of the cyber domain comes from its fluidity and uncertainty. If cyber forces removed their cloaks of secrecy, they would effectively remove themselves from the battle, because enemy network operators would simply block all traffic from the known IP addresses, essentially immunising their systems against compromise from government systems (Mulligan & Growden, 2009).

In addition to the question of who may be targeted in a cyber-attack, the principle of distinction restricts how states constitute their cyber-fighting forces. A state that sponsors use of force by individuals not in the regular armed forces, may be breaching the law of war (Hathaway et al., 2011). This sponsoring or employment of civilians using similar tactics would potentially provide one of the answers some nations have been looking for. Civilian network operators would not be bound by the laws of LoAC like traditional military operators. They would be free to operate undercover, using the full potential of network operations for deception and surprise. This approach would be distasteful, because states are then recruiting and coordinating cyber citizens to attack foreign information systems in order to maintain government deniability. These organised civilian cyber operators are often called cyber militia (Ottis, 2011).

This distinction principle is therefore a problematic principle to deal with. At one side it's difficult to distinguish civilians, combatants, military and civilian objects through the internet. At

the other side the effect of cyber operations are severely hampered if attackers have to attribute their attacks, and so give the opponent the opportunity to organise its defence.

5.7 Subconclusion

Within the international environment there is no well-developed policy or legal framework for cyber operations. The fundamental framework for cyber operations should be based on terms relevant to the Charter of the United Nations, such as ‘use of force’ and ‘armed attack’. One option to prevent a global arms race in cyber space is the approach of arms control to cyber warfare. This approach seems far away. Like the lack of a legal framework, nations have not reached consensus on how to tackle this new modern phenomenon of cyber operations. Until such an internationally accepted cyber legal framework is introduced, the existing international laws are still applicable, and must be met and respected. It is not easy to judge modern cyber operations according to, on kinetic based operations, existing framework of international law.

Globally, cyber operations should be judged according to the principles of the Laws of War, LoAC and the UN Charter, which includes both jus ad bellum and jus i bello. In addition, new analytical work is needed to understand what these principles do and how they should apply to cyber weapons. Although the principles of the LoAC still apply, the specifics of applying the principles are sometimes uncertain and difficult.

The three principles of proportionality, necessity and distinction form the parameters for the case study in the next chapter. These three parameters have their own challenges in the cyber operations discussion.

6 Case Study

6.1 Introduction

In this chapter four cases will be analysed on the use of offensive cyber. All four are of a different kind, and have some similarities, and differences. All four cases did occur in the near past and are therefore interesting and suitable for analysis. This paper will introduce every case in a different section. Then it will analyse whether the three main principles proportionality, necessity and distinction of the LoAC, as described in the previous chapter, are applicable to these cases. This paper will finish every case by answering the question if the case could be used by modern, sophisticated countries, as a scenario for future offensive operations.

The four cases are:

1. Estonia 2007: This was the first proclaimed cyber war by the media. This case was a cyber attack on civilian, economical and governmental targets, disrupting daily life in Estonia, without a clear military objective.
2. Georgia 2008: This case was among the first cases in which an international political and military conflict was accompanied, or even preceded, by a coordinated cyber offensive. This case is on the timeline of the short Russian-Georgian war in 2008.
3. Stuxnet 2010: This case represents the first case in which industrial equipment was targeted with a cyber weapon and caused physical damage.
4. Libya 2011: This is a case that was considered, but never happened. In March 2011 the US seriously discussed and considered the use of offensive cyber in Libya. The arguments why the cyber operations were not used and executed, and the case itself, are interesting to analyse. This case might be the perfect example of a cyber operation, fitting within the international legal framework. But than other arguments show up that must be taken into consideration in future situations as well.

6.2 Estonia 2007

6.2.1 The Case

6.2.1.1 General

Over three weeks, in the spring of 2007, Estonia was hit by a series of politically motivated cyber attacks. Web defacements carrying political messages targeted websites of political parties and governmental and commercial organisations suffered from different forms of (D)DoS attacks. Among the targets were Estonian governmental agencies and services, schools, banks, Internet Service Providers (ISPs) as well as media channels and private web sites (Czosseck et al., 2010, s. 57).

Estonian government's decision to move a Soviet memorial of World War II from its previous location in central Tallinn to a military cemetery triggered street riots in Estonia, violence against the Estonian Ambassador in Moscow, indirect economic sanctions by Russia, as well as a campaign of politically motivated cyber attacks against Estonia (Czosseck et al., 2010, s. 57).

Soon the cyber attacks against Estonia were officially recognised as more than just random criminal acts.

The methods used in this incident were not really new. However, considering Estonia's small size and high reliance on information systems, the attacks posed a significant threat. Estonia did not consider the event as an armed attack and thus refrained from requesting NATO's support under Art. 5 of the NATO Treaty. Instead, the attacks were simply regarded as individual cyber crimes or hacktivism[15]. The incident quickly drew worldwide attention, and media labelled the attacks the first 'Cyber War' (Czosseck et al., 2010, s. 57).

6.2.1.2 Phases and Timeline of the Attacks

Cyber attacks started in parallel to rioting on streets in the late hours of April 27, when web pages of Estonian government institutions and news portals came under a wave of cyber attacks.

[15] Hacktivism: uses cyber attacks based on political motivations, who use cyber sabotage to promote a specific cause. As opposed to the hacking industry intent on data theft, hacktivism is not motivated by money, and high visibility is key. Hacktivisms are motivated by revenge, politics, ideology, protest and a desire to humiliate victims. Profit is not a factor (Imperva, 2012). See also Annex A (A2 cyber terror)

Estonian e-services and information infrastructure were hit, in varying degrees of intensity until the end of May, when the political tensions between Estonia and Russia over the Bronze Soldier issue finally started to calm down (Tikk, Kaska, & Vihul, 2010, s. 18).

A wide array of offensive techniques was used (see Figure 3).

The attacks had two distinctly different phases, each consisting of several waves of elevated intensity. The first phase took place from April 27 to 29 and was assessed to have been emotionally motivated, as the attacks were relatively simple and any coordination mainly occurred on an ad hoc basis. The second phase was a co-ordinated attack phase lasting from April 30 to May 18 and was much more sophisticated. Here was the use of large botnets and professional coordination was obvious. Notably, clear correlation was observed between politically significant dates and intensification of attacks (Tikk et al., 2010, s. 18).

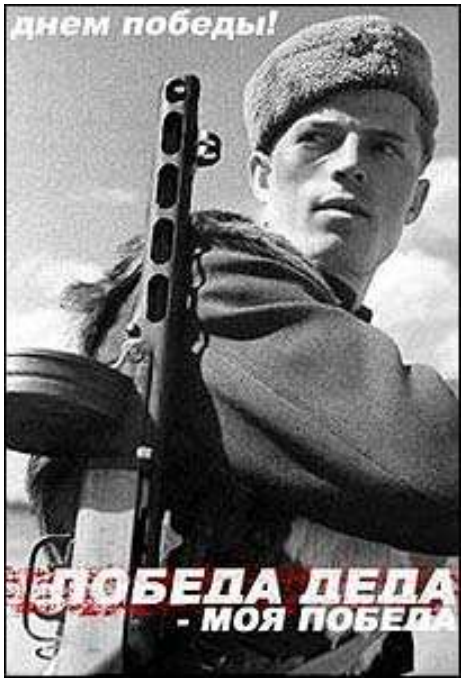

Figure 3: A defaced Estonian website: It shows a Soviet soldier

6.2.1.3 Effects of the Attacks

The cyber effects had both a direct economic and a wider societal effect. As many sectors of commerce and industry rely on ICT infrastructure and electronic communication channels in their daily conduct of business, the overload of e-mail servers, network devices and web servers of internet service providers not only affected large entities but also small and medium size

> enterprises whose daily business activities were seriously impaired […] The attacks also had a societal effect. Because of the unavailability of government websites and the excessive spamming of official e-mail addresses, normal communication with government was impossible for citizens. Cyber attacks against online public services provided via the State Portal had a discernible effect for certain segments of the population, since these services are widely used for filing tax reports, applying for state benefits and for other communication with the government, there was a direct practical or monetary significance for the person involved […] Last but not least, the attacks also affected the nation's information flow to the outside world. The receipt and dissemination of first-hand information about the Bronze Soldier riots, the siege of the Estonian embassy in Moscow and the cyber attacks was impossible. In fact, local media web outlets and the Estonian government's online briefing room were among the first sites to come under cyber attack (Tikk et al., 2010, s. 24-25).

6.2.2 Analysis

The Estonian case is not covered by the LoAC, because an armed conflict is out of the question. This case will be used however to consider if this could be a possible scenario of an offensive cyber operation.

6.2.2.1 Proportionality

This case of Estonia rationally exceeds every form of proportional reaction. The cause of the cyber attacks originates when the bronze soldier statue was replaced in Tallinn. Furthermore there were not any disputes or frictions between Estonia and Russia or any other country. That single decision by the Estonian government was followed by the three weeks of cyber attacks that paralysed the internet traffic in Estonia.

The hackers and attackers reacted emotionally on the movement of the statue. The decision taken by the Estonian government was not according their wishes. The hackers and attackers used all necessary cyber means to disrupt the country that in their eyes made that decision. Their intent is still unknown, but at least they desired and received attention for their cause. These types of hackers are called Patriotic hackers[16] in literature (which are not the same as the earlier described

[16] Patriot hacking is performed by a group of people who take action "pro patria" in cases where they believe that this is the right thing for their government to do or where they perceive the government as unable to do "the right thing" (Tikk et al., 2010, s. 31)

cyber militia)(Tikk et al., 2008). The emotional reactions on Estonia's decision were shown especially during the first, uncoordinated phase of the cyber attacks.

The disproportional side of these attacks lies in the fact that the government took the decision to replace the statue, but the whole nation was a victim of the cyber attacks. Especially the populations' high dependence on the internet and its services, and the high internet connectivity in Estonia, made almost every (innocent) citizen a victim. The attacks generated much intended and unintended collateral damage. It is a fact, that the higher the density of internet connectivity and dependency in a country is, the more the direct and indirect effects, and chance of collateral damage, will be.

> While some Estonian politicians initially uttered emotional statements comparing the attacks to conventional military activity, it was clear to the Estonian authorities that the cyber attacks could, and should, be treated as cyber crime under the applicable Penal Code and investigated in accordance with national law and relevant international agreements (Tikk et al., 2008, s. 25).

Looking back, the Estonian state was not seriously affected, because to a larger extent, state functions and objects of critical information infrastructure were not interrupted or disturbed. A cyber attack that impacts civil or military computer systems and only results in the modification or destruction of non-essential data, similar to what happened in Estonia, would not rise to the threshold of an armed conflict, even if an attack had clear political, financial or economic consequences.

6.2.2.2 Necessity

Looking at the definition of necessity not all factors that meet that definition were filled.
At first, necessity limits the amount of force a state can use against legitimate targets to the amount necessary to accomplish a valid military objective. It states that only actions necessary for the defeat of the opposing side are allowed. In the Estonian case, there was not a state that initiated the attacks, but more or less patriotic hackers who attacked the Estonian Internet structures. Patriot hacking is often used as response against a country's political decision that the country, where the particular hacker, or group of hackers originates from, openly or presumably disapproves (Tikk et al., 2010). In this Estonian case, the political activists expressed their

protest by engaging in coordinated and uncoordinated cyber attacks against the online presence and, to a smaller degree, the Internet infrastructure of Estonia. In no way can these hackers be seen as part of a state that attacks another state. When drawing the line further, it can also be stated that there were no legitimate targets, and no military objective that these actions approved for execution or initiation. Also there was no legal reason of speaking about using actions and force against a possible defeat of the Estonian government. So analysing the definition of necessity and applying it on the Estonian case, it can be said that the principle of necessity was absolutely not met. Even pretending this was a case within the scope of the LoAC and in a jus i bello situation, this cyber attacks were not complied with the necessity principle, because the hackers attacked more than only legitimate (if any) targets and they had no clear objective to be reached.

Secondly, the principle of necessity can only be discussed if a settlement through peaceful means could not be reached. So if the necessity principle is discussed, than we can assume the (political) negotiations prior to the attacks were unsatisfactory. In this Estonian case it could not be analysed whether and how the negotiations for a peaceful settlement went, because there were none. It was known that the Russian government did not like the decision taken by the Estonian government.

6.2.2.3 Distinction

Distinction requires armed forces to make reasonable efforts to distinguish between military and civilian assets. Pretending this case was executed by armed forces, which it was not, the distinction principle was not met at all. The aim of the attackers was not purely to attack political and military objectives, but civilian objectives were struck as well. The attacks originated from computers from 178 countries altogether, and mainly all attacks came from outside of Estonia. In fact Estonia was one big cyber target area.

> While patriot hacking may be perceived as more ‘noble’ compared to other types of hacking, it has hazardous effects both toward its target and point of origin. Patriot hacking is understandably harmful against the target jurisdiction, as it is intended to achieve a political goal by pressuring the authorities or influencing the public. But it also has a hazardous effect towards the jurisdiction of its’ origin, because patriotic hackers assume on their own accord, a role on behalf of their

> governments, by attacking the position of another sovereign nation, thereby raising the question of state attribution (Tikk et al., 2008, s. 31-32).

This attribution problem is also applicable in this case. Today it is still not exactly clear who attacked Estonia and who ordered those attacks. Although the attacks were largely carried out by nationalistically/politically motivated individuals, who followed instructions provided on Russian language Internet forums and websites, the Russian authorities have always denied any involvement. After the attacks, the Estonians delivered a letter to Russia which included specific IP addresses and references to web forum users of the attackers, who were likely located on the Russian territory and whom Russia was asked to assist to identify. In a reply the Russian Federation refused to grant the request, stating that the procedural act requested in the letter was not foreseen by the mutual legal assistance treaty (Tikk et al., 2008, s. 27). In other words: Russia refused to chase after the attackers who allegedly were in the Russian Federation, which raises the suspicion that Russia in one way or the other knew, initiated, supported or approved the attacks.

6.2.3 Can this Estonia 2007 Scenario be used?

This case of Estonia is an interesting case because it is seen as the first real cyber war. But is it a cyber war according to the definition stated in chapter 2? No, it is not. This is not a case in which a nation state cyber attacks another nation state. So this case does not meet the jus i bello criteria and the LoAC is not applicable.

It is interesting however to look at this case and pretend that this array of cyber attacks, that happened in Estonia in 2007, is a scenario modern sophisticated countries, which act according the LoAC, could use as an offensive cyber opportunity within a jus i bello situation. Is this a scenario that could happen and is it allowed according the LoAC? Looking at the three principles analysed in this case the answer for this scenario is a clear: NO (see Figure 4). As well as the proportionality principle as the necessity principle are not met and respected. There is not even a grey area, open for discussion in this case. Another main principle that is breached is the distinction principle. Especially the attribution problem is of huge importance. As long as the attacks are not attributable, the attacks are unlawful. This case should not be considered as a possible line of operation, solely or in combination with a kinetic operation.

Case / *Principle of LoAC*	**Estonia 2007**	Georgia 2008	Stuxnet 2010	Libya 2011
Proportionality	No			
Necessity	No			
Distinction	No			
Does this case apply to LoAC?	No			
Can this case be usable for cyber operations (with adjustments)?	No			

Figure 4: The applicability of the Estonia case within the LoAC

6.3 Georgia 2008

6.3.1 The Case

6.3.1.1 General

"The conflict in this case, falls within the timeframe and context of the broader armed conflict that broke out in August 2008 between the Russian Federation and Georgia over South Ossetia, an autonomous and demilitarised Georgian region on the border of Georgia and Russia"(Tikk et al., 2008, s. 67).

> On August 7, Georgian forces launched a surprise attack against the separatist forces in South Ossetia. On August 8, Russia responded to Georgia's act by initiating military operations into Georgian territory, which the Georgian authorities viewed as Russia's military aggression against Georgia. By late August 7, before the Russian invasion into Georgia commenced, cyber attacks were already being launched against a large number of Georgian governmental websites, making it among the first cases in which an international political and military conflict was accompanied by a coordinated cyber offensive (Tikk et al., 2008, s. 67-68).

6.3.1.2 Methods of Cyber Attacks

The methods of cyber attacks against Georgia primarily included defacement of public websites (see Figure 5) directed at political/governmental and financial sites, and launch of DDoS attacks against numerous targets, such as the Parliament, Supreme Court and Ministry of Foreign Affairs of Georgia, several news and media resources and numerous other sites. The methods were similar to those used in attacks against Estonia in 2007. Several Russian blogs, forums and websites spread a Microsoft Windows batch script that was designed to attack the Georgian websites. The conclusions leave little doubt that the Georgian cyber attacks were largely coordinated and not simply an ad hoc reaction of individual cyber-activists sympathetic to the Russian cause. This constitutes a new development compared to the incidents in Estonia, where coordination was recognised only in the second phase of the cyber attacks (Tikk et al., 2008, s. 71-74).

As was the case with Estonia, there is no conclusive proof of who is behind the cyber attacks, even though finger pointing at Russia is prevalent. The attacks are either state sponsored or acts of hacktivism.

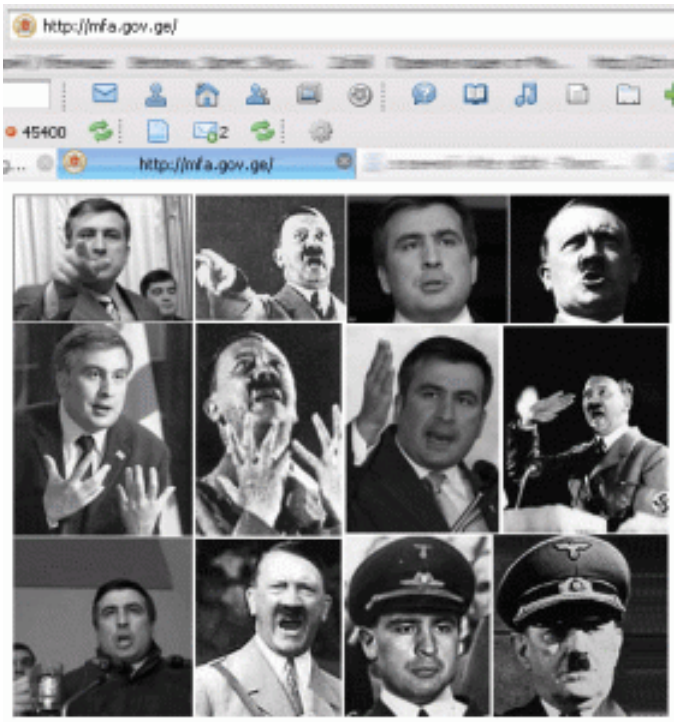

Figure 5: Web defacement on the Georgian parliament website.

6.3.1.3 Effects

> The unavailability of crucial websites to the Georgian government caused by the attacks, severed communication from the Georgian government in the early days of the Georgian-Russian conflict. This period was doubtless the most critical in the events, where the Georgian government had a vital interest in keeping the information flowing to both the international public and to its own residents […] The unavailability of the core state institutions' websites can additionally be seen as serving a discouraging effect on Georgian nationals […] Given the different context of the Georgian cyber event compared to the Estonian cyber attacks, the damage is manifested in different categories as well. In Estonia, the core of the damage consisted of obstructed access to socially vital electronic services, provided by both the public and private sector. In Georgia, the heart of the damage lied in limiting the nation's options to distribute their point of view about the ongoing military conflict, in 'making its voice heard' to the world and Georgian citizens (Tikk et al., 2008, s. 77-78).

The cyber incidents also had a reflection on the provision of public services. As a consequence of the attacks, on August 9, the National Bank of Georgia ordered all banks to stop offering electronic services. Ten days later, the National Bank reported that all commercial banks in Georgia were back to operating business as usual, which, meant that electronic banking services

were out all the time. In Georgia's case, the significance of service disruption is different compared to the importance that cyber attacks had in Estonia, as the scale of the two countries' ICT dependence is rather different. Generally, countries with a higher degree of ICT development are more exposed to cyber attacks and consequently face greater damage (Tikk et al., 2008, s. 78).

6.3.1.4 Georgia's 'Left Hook'

When the Georgian government found itself cyber-locked and barely able to communicate on the Internet, they responded by taking the unorthodox step of seeking cyber refuge in the United States. Without first obtaining US government approval, Georgia relocated critical and strategic IP-based cyber capabilities to the United States, Estonia and Poland. Georgia thereby ensured continued wartime communication with Georgian citizens and military forces. So the Georgian government partially defeated the cyber attack by flowing a portion of its strategic C2 through the United States, the so called 'Left Hook'.

Georgia's 'cyber left hook' manoeuvre is seen as a new precedent in strategic cyber operations. On the other hand, there is a reason to be concerned. A nations' cyber neutrality could be questioned (Korns & Kastenberg, 2009). This neutrality issue is outside this papers scope.

6.3.2 Analysis

6.3.2.1 Proportionality

Analysing this case means the cyber attack must be seen from the Russian point of view, the country that in one way or the other was involved in the attacks. The cyber attacks on Georgia were simultaneously executed with kinetic operations from Russia. The kinetic and non-kinetic attacks seemed like an orchestrated and integrated operation which indicates a large preparation and synchronisation period.

Purely focussing on the cyber attacks, they had influence on the military and governmental information infrastructure, as well, to a lesser extent, on civilian and economic computer networks. A cyber attack that impacts civil or military computer systems and only results in the modification or destruction of non-essential data, which happened at the civilian targets in

Georgia, would not rise to the threshold of an armed conflict. However, if an organised cyber attack (or series of attacks) leads to the destruction of, or substantial or long-lasting damage to computer systems managing critical military or civil infrastructure, it could conceivably be considered an armed conflict, and LoAC would apply. The same is true of a cyber attack that seriously damages the state's ability to perform essential tasks, causing serious and lasting harm to the economic or financial stability of that state and its people, as it was the case in Georgia concerning military and governmental network infrastructures.

While the direct effect of the Georgian cyber attacks is difficult to estimate, the low overall dependence of the Georgian population on online services indicates that the effect of cyber attacks was not serious enough to amount to severe economic damage or significant human suffering (Tikk et al., 2008, s. 77-79). The government and military however, were severely hampered by the attack. This does not mean that the proportionality principle was met correctly. The civilian targets were not correct to attack.

Seen from the Russian point of view, they considered the kinetic attack on Georgia as legitimate, as the Georgians attacked 'their Russian population' in South Ossetia a day earlier. The Russians wanted to protect their people, they said. The cyber attacks on Georgia were perfectly timed and the damage inflicted on the military and governmental infrastructure was well targeted. Looking at the proportionality principle the chosen methods of (temporarily) hampering and disturbing the Georgian governmental and military C2 structures and communications by cyber attacks, were much more effective and less more destructive than if this was executed by kinetic means.

The principle of proportionality is therefore partly met. If the attack was attributable and the Russian government acknowledged its involvement, and the civilian targets were not attacked, the principle was far more applicable.

6.3.2.2 Necessity

The involvement of armed forces in the conflict is an important prerequisite for the applicability of LoAC. In the Georgia scenario this was the case as Georgian and Russian armed forces were involved. A lot of the targets attacked by cyber means were military in nature (e.g. the Georgian Ministry of Defence website), but not all. Thereby, the simultaneous timing between the cyber attacks and Russian military operations into Georgian territory caused, at least initially,

allegations by some of a state-on-state cyber attack. As the necessity principle demands that force only may be used to gain a military advantage, it can be concluded that if this cyber attack was a state-on-state attack, the principle was met because the goal was to hamper the Georgian C2 to their military forces and population. The attacks however also struck the civilian and economic heart of Georgia, which was not necessary to obtain their goal, but was of big inconvenience for the population and economy. As written before, the overall internet connectivity in Georgia was, at that point, not to a level that this inconvenience had a huge and decisive effect. It can be concluded that the gravity of the attacks was not purely on military and governmental targets.

The necessity principle is also applicable if negotiations prior to the attacks can not reach a satisfying settlement and solution. Thereby could Russia interpret the Russian reaction on Georgia's surprise attack in South Ossetia, as an act of self defence, which as described in chapter 5, is a legitimate reason to attack.

This concludes that the necessity principle is partly met. Purely based on strict rules the necessity principle failed because the targets that were attacked were more than the lawful military objectives and combatants and were more than only necessary to accomplish a military advantage.

6.3.2.3 Distinction

In the case of this Georgian incident, the Russian Federation denied any state involvement in the cyber attacks, and data traffic analyses conducted by independent parties failed to draw a direct connection between the cyber attacks and Russian authorities. The orchestrated and coordinated kinetic and non-kinetic operations on Georgia, the timings of the attacks and the picked targets hint to something else. This hits the attribution problem in its heart, as we will also see in the next case. Logically analysing the attacks there can only be one conclusion of where these attacks originate, but as long as the alleged source keeps on denying its involvement, there is no basis to formally accuse a government, or in this case Russia.

Another infliction on the principle of distinction is that the armed forces (cyber attacks) did not distinguish between military and civilian assets. Economic and civilian sites were attacked and

severely hampered as well, although on the civilian side the effect was not that big. This quickly reveals that the distinction principle, in this case, is clearly not met.

6.3.3 Can this Georgia 2008 Scenario be used?

A case closest to the application of LoAC is shown with the Georgian case, where cyber attacks against Georgian governmental websites fell into the timeframe of a nationally declared state of war. We have concluded in the previous analysis that it would be highly problematic to apply LoAC to the Georgian cyber attacks. The objective evidence of the case is too vague to meet the necessary criteria of both state involvement and gravity of effect. Yet, when looking at the context of when these attacks occurred and how well the desired effect was achieved, if state attribution would be possible, the applicability of LoAC would be much more likely (see Figure 6). This case is a scenario that can possibly be used as a suitable scenario after some adjustments. The proportionality and necessity principles can be met in this case, to exclude the civilian and economic targets from attacking, and to avoid collateral damage and unintended effects. These are principles that can be met, but require a solid and intensive intelligence preparation and coordination.

The principle of distinction can be met by solely attacking the military objectives, avoiding civilians and making the attacks attributable. However, making the attacks attributable limits the attackers' effectiveness and makes defending the attacks easier after the first surprise attacks.

Case / *Principle of LoAC*	Estonia 2007	**Georgia 2008**	Stuxnet 2010	Libya 2011
Proportionality	No	Partly		
Necessity	No	Partly		
Distinction	No	No		
Does this case apply to LoAC?	No	No		
Can this case be usable for cyber operations (with adjustments)?	No	**Yes**		

Figure 6: The applicability of the Georgian case within the LoAC

6.4 Stuxnet 2010

6.4.1 The Case

6.4.1.1 General

On June 17th, 2010, security researchers in Belarus identified malicious software (malware). In the months that followed it was revealed that this discovery identified only one component of a new computer worm known as Stuxnet. This software was designed to specifically target industrial equipment.

> The type of industrial equipment Stuxnet infects is known as SCADA systems. These systems are designed for real-time data collection, control and monitoring of critical infrastructure including power plants, oil/gas pipelines, refineries or water systems. SCADA systems often use Programmable Logic Controllers (PLCs) (Shakarian, 2011, s. 2).

> Once it was revealed that the majority of infections were discovered in Iran, along with an unexplained decommissioning of centrifuges at the Iranian fuel (uranium) enrichment plant (FEP) at Natanz, many speculated that the ultimate goal of Stuxnet was to target Iranian nuclear facilities. In November of 2010 some of these suspicions were validated when Iranian President Mahmoud Ahmadinejad publically acknowledged that a computer worm created problems for a "limited number of our nuclear centrifuges" (Shakarian, 2011, s. 1).

Although no entity has acknowledged being the source of the poisonous code, some evidence suggests that the virus was an American-Israeli project. Iran's announcement that a computer worm called Stuxnet had infected computers that controlled one of its nuclear processing facilities, marked a signal event in cyber attacks. Stuxnet represents the first case in which industrial equipment was targeted with a cyber weapon and caused physical damage (Shakarian, 2011). The sophisticated nature of the worm and the resources that would have been required to design, produce and implant it strongly suggest a state-sponsored attack (Porche et al., 2011).

The ultimate goal of Stuxnet is to sabotage the facility, by reprogramming PLCs to operate as how the attackers intend them to, and to hide those changes from the operator of the equipment. Stuxnet was discovered in June 2010, but it is confirmed that it existed at least one year prior and likely even before. The majority of infections were found in Iran (Falliere, Murchu, & Chien,

2011). But there were also “reports of the worm on SCADA equipment in Germany, Finland and China. None of these infections resulted in damage to the industrial systems. This could be due to the specific configuration of the PLC, as Stuxnet only launches the attacks on certain setups” (Shakarian, 2011, s. 6).

6.4.1.2 Effects in Natanz

Stuxnet is a large, complex piece of self-replicating malware with many different components and functionalities, and among others making use of Zero-day exploits. It was designed to attack two models of PLCs controlled by the Siemens’ Step 7 software. Security experts have determined that Stuxnet only launches attacks if the PLC is attached to devices configured in a very specific manner (see Figure 7). In the case of the Iranian nuclear facility, the worm’s target appears to have been the gas centrifuges, which are critical to the uranium enrichment process. According to reports, the worm subtly changed the motor-control frequencies that drive the centrifuges, thus affecting their spin rate and accelerating them to the point where they became unstable and failed. According to a report by the Institute for Science and International Security, between November 2009 and January 2010 Iran replaced 1,000 IR-1 centrifuges at its Natanz FEP (Albright, Brannan, & Walrond, 2010). It is said that Iran’s nuclear developmental efforts had been ‘set back by several years’ by this attack (Broad, Markoff, & Sanger, 2011; Katz, 2010)

6.4.1.3 Infection

How the worm infected the FEP is still not exactly known. One version is that although the network targeted by Stuxnet was likely closed (i.e., not connected to the Internet), it was still ‘sucked into cyberspace’ because the computers that accessed it also accessed open networks. These computers were laptops used by technicians who plugged into the facility’s PLCs, which are on the closed network, to maintain and diagnose equipment. These same laptops could also be used by the technicians to access email, which would connect them to an open network (Porche et al., 2011). A second, more recent version states that the Stuxnet virus that damaged Iran’s nuclear program was implanted by an Israeli proxy, an Iranian, who used a corrupt ‘memory stick.32’ to infect the machines there (Sale, 2012). Using a person on the ground would greatly increase the probability of computer infection, as opposed to passively waiting for the software to spread through the computer facility, as described earlier in chapter 3.

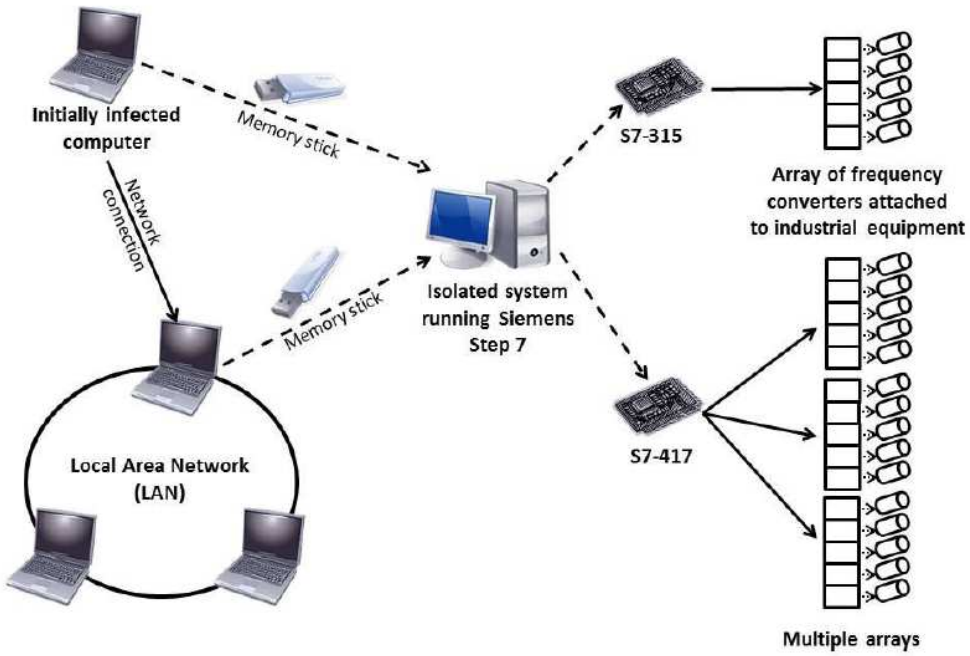

Figure 7: The propagation of the Stuxnet worm (Shakarian, 2011, s. 3)

6.4.2 Analysis

Although Iran and some other countries, as the US and Israel, are accusing each other for many reasons, but especially on military and nuclear issues, there is no situation of war or armed conflict. So the LoAC is not applicable on this situation. To decide whether this case is a scenario that modern sophisticated democratic countries can use as a possible cyber operation scenario, this case will be analysed as if LoAC is applicable.

6.4.2.1 Proportionality

The proportionality principle limits the use of force to situations in which the expected military advantage outweighs the expected collateral damage to civilians and their property. In the Stuxnet case the injection of the Stuxnet worm is seen as the attack. This Stuxnet worm has infected the global internet and ten-thousands, or even more, of Windows computers worldwide. This can be seen as collateral damage. On internet, anti-virus software to disinfect the Stuxnet worm was distributed freely. The production of anti-virus software, which costs a lot of money,

is also a side effect. On the other hand it can be said that this attack did not cost any human life as a direct effect, and the collateral damage has no huge economic or human consequences, except some inconvenience.

Take into account that the attack was aimed against the huge threat and possible consequences of the uranium enrichment capability in the FEP, it must be said that the cyber attack was of a proportionate character. The soft non-kinetic and non-harmful method used was only disrupting the FEP and resulted in a serious set-back of the plant, which was exactly the aim of the attack. No civilians were injured or lost. Top German computer consultant Ralph Langer even stated: '*This was nearly as effective as a military strike, but even better since there are no fatalities and no full-blown war. From a military perspective, this was a huge success*' (Katz, 2010).
So purely analysing the proportionality principle, as if it was a jus i bello situation, the principle was met. As a case on its own, the proportionality principle and LoAC is not applicable.

6.4.2.2 Necessity

If this case is considered as a jus i bello situation, the necessity of attacking this FEP could eventually be a possibility. The political, military and nuclear importance of Iran enriching uranium for possible nuclear attack capabilities is considered a global threat to all, and makes this FEP a lawful military objective to attack, to eliminate or severely damage, or delays its processes. Seen in this light the attack was successful. The necessity principle seen in the light of momentum is not that clear. Although the FEP could be a threat to the world in enriching uranium for possible nuclear capabilities and military use, the diplomatic discussion were still ongoing. The International Atomic Energy Agency[17] (IAEA) was still investigating and inspecting the FEP locations in Natanz and other locations. The corporation with Iran did not go very fluently and without problems (IAEA, 2010), but there was not (yet) an alarming situation that needed direct military intervention. So seen in the light of momentum, the necessity principle was not met.

[17] The IAEA is the world's centre of cooperation in the nuclear field. It was set up as the world's "Atoms for Peace" organisation in 1957 within the United Nations family. The Agency works with its Member States and multiple partners worldwide to promote safe, secure and peaceful nuclear technologies. As an independent international organisation related to the United Nations system, the IAEA´s relationship with the UN is regulated by special agreement. In terms of its Statute, the IAEA reports annually to the UN General Assembly and, when appropriate, to the Security Council regarding non-compliance by States with their safeguards obligations as well as on matters relating to international peace and security (www.IAEA.org)

Furthermore there was not a situation that the Iranian government attacked another nation, which could explain an act of self defence, or a situation that the UNSC pronounced a resolution to act as such.
Because there was no armed conflict altogether, the cyber attack was not necessary at all to achieve a military advantage, and so the principle of necessity in general was not met.

6.4.2.3 Distinction

In the Stuxnet case the main problem is the same as in the Georgia and Estonia case. This is the attribution problem. Again, this cyber attack was not attributed, although the attack was very thoroughly prepared, and is concluded that the sophisticated nature of the worm and the resources that would have been required to design, produce and implant it, strongly suggest a state-sponsored attack. Many scientists and analysts are convinced the Stuxnet cyber attack is an American-Israeli corporation, but the US as Israel both deny state involvement in the attacks. This makes this distinction principle not met, if this were a LoAC situation.

If the distinction principle focuses on the distinguishing between military objectives, civilian population and combatants, it can be said that the real effectiveness of the Stuxnet worm, and so the gravity of the attack, was only within the FEP Natanz. However the worm also infected other computers worldwide, the worm is now latent and ineffective.

6.4.3 Can this Stuxnet 2010 Scenario be used?

It was clear that this Stuxnet case did not fit into the LoAC and did not meet with the three analysed principles. More important and interesting is to see whether and how this case can be used as a scenario, which is usable as a cyber operations model for modern, sophisticated, acting according LoAC countries. The scenario would be a cyber attack on a SCADA-like system or industrial equipment to inflict physical damage or delay. A big side effect of SCADA systems is that a lot of them are dual-use systems. So attacking the system as a military objective can have an unintended collateral damage effect. This kind of attack therefore requires a huge intelligence effort, to exclude as much as possible the collateral damage effects, and distinguish between the military objectives, combatants and civilian population.

.

It is thinkable to cyber attack a SCADA system in close corporation with synchronous kinetic operations in a jus i bello situation (see Figure 8). This cyber attack can have the purpose to, for example, temporary disrupt a system or destroy a system to avoid possible use in future. As in this case the objective is a FEP, this could easily be a legitimate cyber target, as part of an overarching operation and plan. The necessity principle can be met in this way.

The proportionality principle can be met almost in the same conjunction as in this case. It is important to avoid collateral damage. In this case the collateral damage could be minimised by not infecting the Stuxnet worm via internet, but by executing a close-access attack, and penetrate such a closed system by, for example, a portable memory card (such as USB-stick). Such as is suspected in how Stuxnet infected the FEP in Natanz. Important and difficult in this case is minimising or avoiding collateral damage.

The principle of distinction must, in the first place, be met by finding a solution and seeking for an optimum between attributing the cyber attacks and gaining as much effectiveness as possible. As stated before in this paper, attributing cyber operations makes defence at the opposing side easier. After a first surprise attack is executed, the opposing side is expecting a next phase or wave of cyber attacks, and is able to prepare for and defend against those attacks. This necessitates an attack that inflicts all the damage and achieves all the goals in the first attack.

The distinction principle requires distinguishing between military objectives, combatants and civil population, and this scenario makes this possible. A thorough intelligence phase and preparation phase must be made prior to the actual attacks and execution phase to meet these principles. This makes this kind of attacks pre-planned or part of a fast changing manoeuvre operation.

It can be concluded that this scenario, if thoroughly prepared, is an option to consider, without or in combination with kinetic attacks.

Case / *Principle of LoAC*	Estonia 2007	Georgia 2008	**Stuxnet 2010**	Libya 2011
Proportionality	No	Partly	No	
Necessity	No	Partly	No	
Distinction	No	No	No	
Does this case apply to LoAC?	No	No	No	
Can this case be usable for cyber operations (with adjustments)?	No	**Yes**	**Yes**	

Figure 8: The applicability of the Stuxnet case within the LoAC

6.5 Libya 2011

6.5.1 The Case

6.5.1.1 General

> Just before the American-led strikes against Libya in March 2011, the Obama administration debated whether to open the mission with a new kind of warfare: a cyber offensive to disrupt and even disable the Ghaddafi government's air-defence system, which threatened allied warplanes. While the exact techniques under consideration remain classified, the goal would have been to break through the firewalls of the Libyan government's computer networks to sever military communications links, and prevent the early-warning radars from gathering information and relaying it to missile batteries aiming at NATO warplanes (Schmitt & Shanker, 2011).

At the decisive moment there were six dilemmas on the use of a cyber attack:

1. Precedent: The US feared that it might set a precedent for other nations, in particular Russia or China, to carry out such offensives of their own. This is the dilemma of the first use strike.
2. Time: It was questioned whether the attack could be mounted on such short notice. It takes significant intelligence to identify potential entry points (vulnerabilities) and susceptible nodes in a linked network of communications systems, radars and missiles, like that operated by the Libyan government. After that it takes time to write and insert the proper poisonous codes. Another aspect, as it was said, was that Libyan government forces, led by Ghaddafi, were at the time close to overrunning Benghazi, a rebel stronghold where US officials feared massacre might occur without fast intervention.
3. Domestic law: The US was unable to resolve whether the president had the power to proceed with such an attack without informing Congress.
4. Necessity of revealing methods: Some officials expressed their concern about revealing American technological capabilities to potential enemies for what seemed like a relatively minor security threat to the United States. Libya's air-defence network was dangerous but not exceptionally robust (Schmitt & Shanker, 2011).
5. Collateral damage: The Americans were not sure whether the intended targets were connected or used as dual-use systems. So the consequences for the civilian population or hospitals could not be foreseen and the indirect and unintended effects

and collateral damage could not be estimated.

6. Uncertain effect: There was the possibility of any damage inflicted by a cyber weapon being temporary, allowing the Libyan government to potentially restore its air defences quickly, and as a result the US fighter being vulnerable to Libyan attacks.

In the end, American officials rejected cyber warfare and used conventional aircraft, cruise missiles and drones to strike the Libyan air-defence missiles and radars used by Ghaddafi's government (Schmitt & Shanker, 2011).

The rejection of this cyber operation was covered by two metaphors: "We don't want to be the ones who break the glass on this new kind of warfare" said James Andrew Lewis, a senior fellow at the Centre for Strategic and International Studies. An Obama administration official briefed on the discussions said "These cyber capabilities are still like the Ferrari that you keep in the garage and only take out for the big race and not just for a run around town, unless nothing else can get you there" (Schmitt & Shanker, 2011).

6.5.1.2 Pakistan

The discussion on whether or not to use offensive cyber during planning for the opening salvos of the Libya mission, was repeated on a smaller scale several weeks later. Military planners suggested a far narrower computer-network attack to prevent Pakistani radars from spotting helicopters carrying Navy Seal commandos on the raid that killed Osama bin Laden on May 2 2011. Again, officials decided against it. Instead, specially modified, radar-evading Black Hawk helicopters ferried the strike team (Schmitt & Shanker, 2011).

6.5.2 Analysis

The specialty about this case is that the cyber attacks in this case never occurred. However, the discussions prior to the possible attacks, the considerations and the decision not to use cyber attacks are interesting to analyse and can form a firm basis to future discussions on the use of offensive cyber operations. The whole Libya operation was initiated by the Americans as 'Operation Odyssey Dawn' (Rønneberg, 2011), and later taken over by NATO. The operations conducted were covered by the UNSC resolution 1973 (UNSC, 2011). This case is, therefore, an example of a jus i bello situation and the LoAC is applicable. This chapter will analyse the three principles of proportionality, necessity and distinction as if this case happened or can happen.

6.5.2.1 Proportionality

Thinking at the proportionality principle and discussing whether to use a non-kinetic cyber operation to (temporary) eliminate enemy radar and anti-aircraft installations, or using kinetic methods as fighters to bomb those facilities, could express a preference for the cyber operations. The cyber operation will not kill people directly, has the potential to temporary eliminate the systems at one side, but on the other hand has the potential to reverse the systems back to normal after the attack is over. The kinetic attacks are risky for the fighter pilots as they could be under attack, and there is a chance for physical collateral damage on the ground is big. Besides that, if the Libya dispute ends, it would be much more difficult to rebuild its defence system if the current systems are physically eliminated. These arguments would support the use of cyber operations in this situation.

In 2011 the Americans used two strong arguments that could make the outcome of proportionality uncertain: Time and collateral damage. In fact, the intelligence process was a key in this. Attacking and eliminating enemy radar and anti-aircraft installations demands a thorough intelligence and reconnaissance process. This takes time. Time the Americans, at that moment, did not have, at least not enough. The Americans were able, and had the means to conduct cyber operations on the alleged targets, but did not have enough time and/or intelligence to judge whether the risks for unintended collateral damage was at a minimum. Besides, the Americans had more arguments not to cyber attack the Libyan targets, these time and collateral damage arguments, in the light of proportionality, were valid reasons not to attack with cyber. The alternative however was kinetic, irreversible, and full of risk on collateral damage too, but it was known by experience, what and how these attacks would result in the desired outcome, orchestrated in the whole operation.

It can be concluded that this case, in the light of proportionality, was a perfect scenario for a cyber attack on the Libyan targets, if the result could be predicted more precisely, if the collateral damage could be minimised, and if time for reconnaissance and intelligence was sufficient.

6.5.2.2 Necessity

Necessity means that the force only may be used if it is essential to achieve the military objective. In this case the military objectives were the Libyan radar and anti-aircraft installations (air-defence systems). These targets were within the LoAC valid and legitimate. Elimination of these targets by cyber operations were meant to pave the way to conduct kinetic surprise air-attacks on Libya's strategic C2, communication, leadership, military airbases and other military objectives. It can be concluded that eliminating these air-defence installations would have a clear military advantage, independently of the question how to obtain this advantage. Whether the attacks would be kinetic by air-strikes or non-kinetic cyber operations does not question the principle of necessity. One aspect within this principle is that the risk for collateral damage should not be excessive in relation to the concrete and direct military advantage. This supported the choice for a kinetic attack, as the possible collateral damage could be more easily assessed than if the attack was executed by cyber attacks, as already discussed earlier in this case. This is due to the Americans lacking accurate intelligence and time to prepare the cyber attacks.

6.5.2.3 Distinction

Distinction requires armed forces to make reasonable efforts to distinguish between military and civilian assets, and between military personnel and civilians, and to refrain from deliberately attacking civilians or civilian assets. Concerning the air-defence systems, the targets were well chosen. The initial targets were purely military and therefore there was a good distinction between military and civilian. As was also mentioned in the proportionality section of this case, the unknown consequences of attacking the air-defence network was of primary concern and one of the reasons not to attack. The UNSC resolution 1973 was pronounced at the 17th of March 2011, while the coordinating conference, where the international community in Paris on the 19th of March decided to take actions. The first American attacks began that very same day, showing that the time to prepare proper cyber operations determines whether the networks were dual-use systems and assessing and waging possible collateral damage, was way too short. The possibility of dual-use of these systems with civilian vital installations is present, which concludes that the distinction principle can not be guaranteed.

The collateral damage and time aspect were not the most important of the reasons why, in the end, the cyber operations were not conducted. They were however valid and important enough to determine and wage the risk of cyber operations, and to decide not to use it.

6.5.3 Can this Libya 2011 Scenario be used?

This case shows that cyber operations can be a force multiplier, a better alternative and a legitimate option as part of an overall campaign or operation. Of all cases analysed in this study, this is probably the most clear and usable scenario for planners; executing cyber operations in close orchestration with kinetic operations. The main condition for the usability of this scenario is that it must fully comply within the international legal framework. This case can, with some adjustments, comply with the three main principles within the LoAC, which means these types of cyber operations are technically and (international) legally working options. The adjustments that have to be made are merely in the field of intelligence, time and collateral damage. To fully comply with these principles of proportionality, necessity and distinction, the collateral damage and guaranteed distinction of civilian population and assets on one side, and military objectives and combatants on the other, must be subject to accurate intelligence work. The intelligence work is more intensive and harder to accomplish in cyber space than in the realm of kinetic operations. As the intelligence work before an operation is harder, so is the battle damage assessment after an action harder to execute in cyber space. This is a factor that must not be forgotten.

This concludes that the first phases of a cyber attack, the exploit and reconnaissance phase, are very time consuming and require thorough preparation. This means that cyber operations has to be planned thoroughly and must be part of a bigger campaign, to pursue maximum efficiency and effectiveness in use of man power, risk, damage, manoeuvre and goals to be achieved. It can therefore also be said that cyber operations are not very suitable in combination with kinetic operations if involved in situations with quick changing plans and manoeuvre warfare, where time is for short to conduct proper intelligence work to comply fully with the three principles in the LoAC. Knowing this can imply that offensive cyber operations can be best incorporated in the military planning and decision making processes at the strategic and operational level, as intelligence sources are more equipped at those levels than the tactical and technical level. At the strategic and operational level they have more time to prepare a campaign in which the offensive cyber operations' risks and threats are carefully waged and assessed.

So this Libya case is a case that with some adjustments can be a usable scenario, seen from the technically and international legal side (see Figure 9). There can be cases where all the technical

and legal requirements are filled in, but the operation still cannot continue. It may be other motives that are considered, whether an operation can be executed or not. These are arguments that the planners of offensive cyber operations will have to handle with in the future.

1. **Dilemma of the first use strike**: This Libya case showed that the US did not execute the cyber attacks on moral and ethical grounds. Not because of the Libyan population, but because of the fear of reprisals when the US overtly initiates a cyber attack in a war situation, which would set a precedent to other countries to do the same against the US. The (political, military) cost-benefit analysis did not lean to the benefit side. Libya was not special enough to risk that first use strike. This dilemma is, besides the legal and technical aspects, an argument that seriously has to be taken into account in future. This feeds also the cyber arms control discussion, as described in the previous chapter.
2. **Secrecy**: Libya was not important enough to reveal the US's cyber methods and secrets to the world. This is a very plausible consideration not to use offensive cyber. Techniques develop daily and, once revealed, cyber methods can allow the opponent to quickly adapt its cyber security and neutralise the attack methods for future use. This will make the deployment of offensive cyber a case of specially picked moments and circumstances. Revealing secrets and methods must be worthwhile in relation with the benefit and goals to be achieved.
3. **Domestic law**: Besides the international framework of Laws, nations often themselves have their own legal and political laws, procedures and regulations they have to go through, before the nation is allowed and entitled to use methods, such as offensive cyber.

This analysis demonstrates that if technical and international legal principles are met, and the prerequisites are filled in, there are overarching arguments that can have a huge effect, and influence on the use of offensive cyber. The question that modern, sophisticated countries, acting according the international legal framework face is, whether and when to cross the threshold into overt cyber attacks.

Case / *Principle of LoAC*	Estonia 2007	Georgia 2008	Stuxnet 2010	**Libya 2011**
Proportionality	No	Partly	No	Likely
Necessity	No	Partly	No	Yes
Distinction	No	No	No	Likely
Does this case apply to LoAC?	No	No	No	Likely
Can this case be usable for cyber operations (with adjustments)?	No	**Yes**	**Yes**	**Yes**

Figure 9: The applicability of the Libya case within the LoAC

6.6 Subconclusion

This case study showed the difficulty of simultaneously conducting cyber attacks at an efficient and effective manner on one hand and executing these attacks within the existing international legal framework, the LoAC, on the other hand. Within the first three cases, none of the three analysed principles of the LoAC, proportionality, necessity and distinction, were met, pretending the cases were applicable to the LoAC (see Figure 10). The main reasons the cases do not meet the principles are:

1. The attribution problem. The cyber attacks were not attributable to a government or nation state.
2. Collateral damage. The effects of the attacks were bigger than strictly necessary, and possibly intended.
3. Distinction between military and civilian objectives: The cyber attacks did not distinguish enough to exclude innocent civilians from the attacks.

The Libya 2011 case would probably be the case that comes closest in meeting the three principles, but the case did never occur.

If the case study analyses the scenarios, and determines whether the scenarios can be used by modern sophisticated countries within the existing international legal framework, it must be concluded that it is difficult to meet those principles. The primary reason is that making the scenarios attributable goes at the expense of the power, efficiency and effectiveness of the cyber attacks. Furthermore it is difficult, more difficult than in conventional attacks, to minimise collateral damage and distinguish between the military and civilian objectives. This may lead to the conclusion that, however the offensive cyber is physically humane and has many advantages above kinetic attacks; it is less effective and less easy to use. This is the case if the use of offensive cyber must apply to the principles of the LoAC. The LoAC limits the optimum use of offensive cyber severely.

Offensive cyber operations must be planned on forehand to assure minimum of collateral damage and maximum of distinction. This takes time, needed for intelligence gathering, and will not secure the use of the specific planned cyber operation. One should note that in cyberspace the world can change in seconds.

Case / *Principle of LoAC*	Estonia 2007	Georgia 2008	Stuxnet 2010	Libya 2011
Proportionality	No	Partly	No	Likely
Necessity	No	Partly	No	Yes
Distinction	No	No	No	Likely
Does this case apply to LoAC?	No	No	No	Likely
Can this case be usable for cyber operations (with adjustments)?	No	**Yes**	**Yes**	**Yes**

Figure 10: Overview of the applicability of all four cases within the LoAC

7 Conclusions and Food for Thought

7.1 Conclusions

This paper has explained and analysed all kinds of aspects concerning offensive cyber, with the restriction that these cyber assets are only deployed as capabilities between two or more nation-states, by their military forces.

This paper was written answering two sub questions, which together answers the main thesis question. The first sub question explained what offensive cyber is and what its possibilities and capabilities are. This was necessary as basis for the second part of the study, which analysed the use of offensive cyber within the existing international legal framework (the LoAC). This second part considered four case studies (Estonia 2007, Georgia 2008, Stuxnet 2010 and Libya 2011), and analysed the applicability of these four cases as an offensive cyber scenario, on the principles of proportionality, necessity and distinction within the LoAC.

The first part explained cyber attack and offensive cyber. There are several characteristics of cyber attack that are important to emphasize. The most important are:

1. The indirect effects of weapons for cyber attack are almost always more consequential than the direct effects of the attack.
2. The outcomes of a cyber attack are often highly uncertain. One consequence can be that collateral damage and damage assessment of a cyber attack may be very difficult to estimate.
3. Cyber attacks are often very complex to plan and execute, because they can involve a much larger range of options than most traditional military operations, and need more accurate intelligence.
4. Compared to traditional military operations, cyber attacks are relatively inexpensive.
5. Most sophisticated cyber attack weapons are only usable once or a few times. The victim will adapt its defence once an attack has occurred.
6. The identity of the originating party behind a significant cyber attack can be concealed with relative ease compared to that of a significant kinetic attack (the attribution problem).

The different offensive scenarios show that offensive cyber can be used in the full spectrum of (cyber)war. Offensive cyber can on one side of the spectrum be deployed in small covert operations, and on the other end of the spectrum in full overt offensive cyber operations. However offensive cyber operations can be conducted independently, it makes them less influential. The main objectives in an overarching operation will be reached not only with cyber operations, but often in combination with kinetic operations.

Important dilemmas that constantly must be considered during decision-making processes and during the offensive cyber operations are the dilemmas of first use, preparation of the battlefield, ambiguity of intent, and escalation of a global war and collateral damage. Another important part in the use of offensive cyber is deterrence. While offensive and defensive cyber capabilities are critical to deterring aggression, employing these capabilities depends on robust international norms for state behaviour in cyberspace. International law is the first line of deterrence in cyberspace.

The second part of the thesis analysed the position of offensive cyber within the existing international legal framework. Within the international environment there is no well-developed policy or legal framework for cyber operations. Until such an internationally accepted cyber legal framework is introduced, the existing international laws are still applicable, and must be met and respected. However, it is not easy to judge modern cyber operations on the existing framework of international law, which is based on conservative kinetic based operations. It is working with new capabilities, under old rules.

In addition, to prevent a global arms race in cyber space it can be necessary to develop an approach of arms control to cyber warfare. This approach is yet far away because of lack of international consensus.

Globally, cyber operations should be judged according to the principles of the Laws of War, LoAC and the UN Charter, which includes both jus ad bellum and jus i bello. Although the main principles of the LoAC still apply, the specifics of applying these principles on cyber operations are difficult. The case studies showed the difficulty of simultaneously conducting cyber attacks at an efficient and effective manner on one hand and executing these attacks within the existing international legal framework, the LoAC, on the other hand. In the Estonia, Georgia and Stuxnet cases, none of the three main principles of the LoAC, proportionality, necessity and distinction,

were met, pretending the cases were applicable to the LoAC. The main reasons the cases do not meet the principles are the attribution problem, collateral damage and distinction between military and civilian objectives.

Analysing the Estonia, Georgia and Stuxnet cases concludes that those cases are problematic to use as an offensive cyber scenario within a jus i bello situation. Only if specific adjustments are made in the scenarios on attribution, avoiding collateral damage and securing distinction, the scenarios may comply with the LoAC. However, making the scenarios attributable goes at the expense of the power, efficiency and effectiveness of the cyber attacks. Furthermore it is difficult to minimise collateral damage and distinguish between the military and civilian objectives. In general, the LoAC limits the optimum use of offensive cyber. Offensive cyber operations must be planned thoroughly on forehand, to assure minimum of collateral damage and maximum of distinction. This takes time, needed for constant intelligence gathering. However, the constant changing cyber space is the reason that carefully planned cyber operations will not assure the execution of that specific planned cyber operation on that specific needed occasion.

The Libya case has taught us, that when all three principles of the LoAC seem applicable, and the cyber operation is international legally covered, other factors rise that can hamper the use of offensive cyber operations. These factors are the dilemma of the first use strike, secrecy and the domestic law of the originator. These dilemmas will play and important role in future offensive cyber planning.

Offensive cyber has a lot of potential. Offensive cyber can really increase the overall offensive capability, and multiply the offensive options for military planners and leadership. However, as long as there is no consensus on international accepted cyber law that sets the boundaries for the use of offensive cyber, the existing international legal framework is applicable. Today, the on kinetic operations based rules and laws, are not fully suitable for cyber operations, which creates grey areas and lack of clarity in the use of offensive cyber. A new international accepted legal cyber framework should limit, and set boundaries for the use of offensive cyber. On the other hand, developing a new international accepted legal framework, in which offensive cyber is appointed, is also an opportunity to exploit the optimum use of offensive cyber, within that framework. Uniformity in definitions, approach and interpretation is a prerequisite.
Until that moment, there exists the possibility of a long Cyber Cold War.

7.2 Food for Thought

Studying offensive cyber and analysing the cases, answers a lot of questions within the scope of this study, but also raises new dilemmas, questions or conclusions that are worthwhile for future research. Some of these thoughts are:

1. This paper has looked at the use of offensive cyber in a jus i bello situation. Offensive cyber can also be analysed and researched if used in a jus ad bellum situation. Can offensive cyber be used in the phase that political and diplomatic negotiations come to a fruitless end, economic embargoes are not effective, and military kinetic operations should be the first logical step? Offensive cyber can be a way to persuade or pressure another government.
2. A big challenge in conducting offensive cyber operations is to use state of the art cyber techniques, to make sure that your attack methods will not be outdated, and to have the personnel that take care of that. How does an armed force recruit state of the art personnel, and how do they keep them state of the art, how do they train them, and how do they educate them? Can the armed forces pay those people or is there another construction? How do other countries like China and Russia solve this challenge?
3. The comprehensive approach can be very useful in addressing the national and international cyber security challenges. Military, diplomatic and economic departments can work together, because cyber knows no boundaries. Also international corporation in cyber security is recommended. But when it comes to cyber offence, every single nation works in splendid isolation on its offensive cyber capability, preferably as covert as possible. How do other countries look at the use of offensive cyber, is corporation on the offensive side due to fail, or are there common opportunities and chances that can be addressed together?
4. Stating that offensive cyber asks for a new international legal framework will automatically raise the question how this framework should look like, and what items should and should not be addressed and discussed in the new to develop Cyber Law. Neutrality, for instance, should be one of those subjects.

Annex A: Cyber Crime & Cyber Terror

A.1 Cyber Crime

Cyber crime can be defined as "**any criminal offense that is committed or facilitated through the use of the communication capabilities (cyberspace) of computers and computer systems"** (Schröfl, Rajaee, & Muhr, 2011, s. 10). It can consist out of the following 6 categories:

1. Interference with lawful use of a computer (which includes such crimes as cyber-vandalism, cyber terrorism and the spread of viruses, worms and other forms of malicious code)
2. Dissemination of offensive materials (which includes child pornography, other forms of illegal material, racist/hate-group material, illegal online gambling and treasonous content)
3. Threatening communication (which includes extortion and cyber stalking)
4. Forgery and Counterfeiting (which includes identity theft, phishing, IP offenses, various kinds of software and entertainment piracy and copyright violations)
5. Fraud (which includes credit card fraud, e-funds transfer fraud, theft on internet or telephone services, online securities fraud and other types of Internet fraud)
6. And other types of cyber-crime (which includes interception of communications, commercial and corporate espionage, communications used in criminal conspiracy and electronic money laundering)(Schröfl et al., 2011).

> Cybercrime is one of the most pressing security concerns in today's networked world. This is not only because of the sheer scale of cyber crime, but also because the ambiguous nature of actors in cyber space means that cyber criminals can really be (state-backed) cyber warriors, and vice versa. Many of the attack techniques used are largely the same. Addressing and combating cybercrime therefore address many of the operational issues potentially associated with cyber warfare; thus it has become a focus for national security policies in many countries (Klimburg & Tirmaa-Klaar, 2011, s. 9).

Cybercrime is increasingly considered to be the most advanced and profitable of all criminal enterprises and it has long since overtaken the drug trade in terms of business volume (Geers, 2011).

There is significant evidence that implicates non-state groups (possibly definable as cyber crime groups) in serious cyber espionage cases directed against Western governments. Due to the difficulty of actor attribution, as well as legal consequences in categorising an attack as 'warfare', it can be presumed that many of the anti-cyber crime security measures European governments seek to implement are at least equally directed at state-directed cyber attacks (Klimburg & Tirmaa-Klaar, 2011, s. 10).

A.2 Cyber Terror

The concept of 'cyber terrorism' is highly contentious. The term has been used in a wide range of contexts. The FBI has reportedly defined cyber terrorism in terms very similar to their conventional terrorism definition. The US Army developed two definitions of cyber terrorism, namely "**activities carried out in support of conventional terrorism"** (e.g. 'content', such as propaganda, recruitment, or planning) and "**actual cyber attacks for terrorist purposes"**. The 'content' interpretation of cyber terrorism raises many obvious concerns, as it can quickly cross over into civil-rights and freedom of expression issues. The category 'direct cyber terrorist attacks' is not undisputed either, as this also includes a wide range of behaviour, not all of which can be considered as serious attacks. There have certainly been a number of politically-motivated non-state attacks on the Internet, ranging from website defacement operations to attacks on entire countries. […] The production of computer viruses for ideological reasons or for purely disruptive, nonfinancial gain could be termed a cyber terror attack. Overall, a strong concern exists that applying the term cyber terrorism loosely (or in any form at all) would allow draconian security legislation to be applied to relatively minor misdemeanours. A number of critics have therefore sought to completely replace the term cyber terrorism with terms such as 'hacktivism'. Sometimes it is argued that attacking a website, or a network, can never be considered terrorism, as direct casualties hardly ever result. In other words, if there are no direct casualties it cannot be considered terrorism. This argument ignores, however, the fact that mass disruptions on their own can be extraordinarily expensive to a society or an organisation, potentially crippling a country's economy or destroying a company (Klimburg & Tirmaa-Klaar, 2011, s. 10).

At present the hackers group Anonymous is gathering a lot of media attention, as they out of an ideological point of view, cyber attack huge companies and organisations. Those companies were in one way or the other involved in the WikiLeaks documents case (VISA, Mastercard, FBI, etc). The latest hacking activity, at the time of writing this paper, is the tapping of the FBI talking to Scotland Yard, early 2012 (Cornish et al., 2010). Anonymous is not after gaining

financial profit, but are ideological (see Figure 11). Therefore they fit more in the cyber terror definition. Illegal it is anyhow.

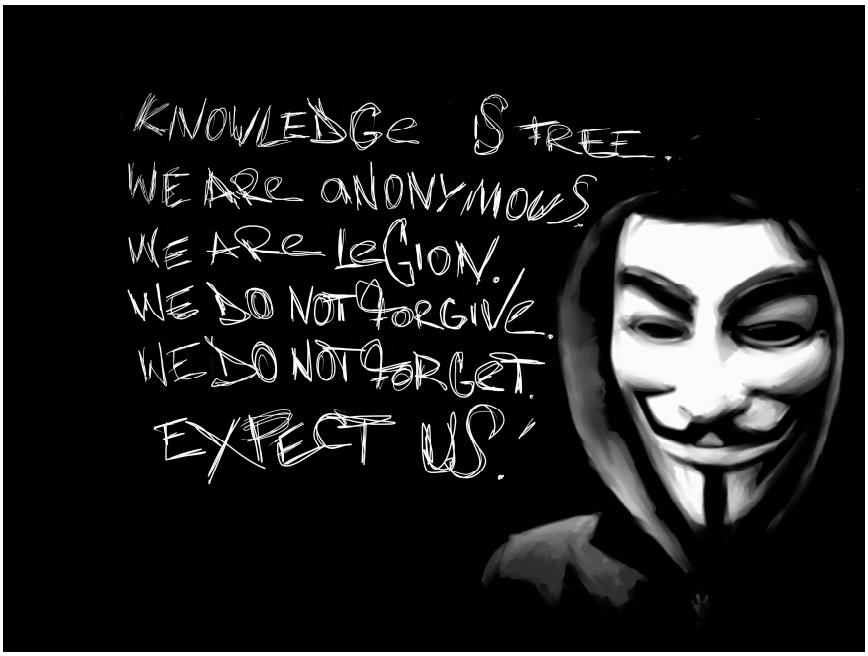

Figure 11: Hackers group Anonymous' self description

Annex B: Techniques

Most of the cyber threats, vulnerabilities and attacks can be categorised into the following different types with different types of techniques:

1. Deliberate logical attacks. These kinds of attack refer to software failures, using so called malware (malicious software) designed to secretly access a computer system without the owner's informed consent, and they are aimed at syntactic and semantic layers. There are different sorts:
    a. **Logic Bomb**. This is the earliest and simplest form of malware. It is a concealed program that triggers a result, which the designers of a system did not expect. The result of a logic bomb detonation can range from a jokey on-screen message to complete system shutdown or a complex sequence of events.
    b. **Spyware programs**. It is a collective term for programs that are commercially produced for the purpose of gathering information about computer users, showing them pop-up ads, or altering web-browser behaviour for the benefit of the spyware creator. Spyware programs are sometimes installed as Trojan horses of one sort or another.
    c. **Trojan horse**. It is a program that creates a back-door into a computer (A back-door is a method of bypassing normal authentication procedures). The program invites the user to run it, concealing a harmful or malicious payload. The payload may take effect immediately and can lead to many undesirable effects, such as deleting the user's files or further installing malicious or undesirable software.
    d. **Virus**. A virus is a self-replicating program that often has a logic bomb or a Trojan as a payload. It can also infect some executable software, followed by, when run, the spread of the virus to other executables. The term 'virus' is also commonly but erroneously used to refer to other types of malware.
    e. **Worm**. A computer worm is also a self-duplicating malware computer program. It uses a computer network to send copies of itself to other nodes, and it may do so without any user intervention due to security shortcomings on the target computer. A virus requires user intervention to spread, whereas a worm spreads itself automatically.
    f. **Key logger**. This is a program, which monitors and records the keystrokes on a computer; it can be regarded as a special form of payload.

g. **Root-kit**. The term originally referred to a program that took over an entire computer and gave the perpetrator total, or ‘root’, privileges. Today root-kit tends to mean a piece of malware that is very well hidden within the operating system of a computer and hence difficult to detect and remove.

h. **Web based malware**. Malware can also be embedded in web pages. Web pages often contain code in languages, such as JavaScript. This may be used for such innocent purposes as triggering a moving display or validating the input to an on-screen form. However, it can also be exploited to install malware. Another technique is the use of single pixels on a web page, which would normally be invisible to the user but which contains a hyperlink to destructive malware.

2. Cyber vulnerabilities. It is a form of weakness that allows an attacker to reduce a system’s information assurance. There are many different cyber vulnerability types, but the two best-known are:

a. **Social engineering**, which is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques.

b. **Zero-Day Exploits**. A zero-day exploit is one that uses hitherto unknown technical vulnerability for its effect.

3. Threats:

a. **Information overload**. In abnormal circumstance, if resources are insufficient, systems will cease to work, either shutting themselves down in an orderly fashion or going into an error state. Because of the interconnectivity, a fault or overload in one system that does not close down ‘gracefully’, may result in cascading errors. Many computers will already shut down e-mail spam, also known as junk e-mail or unsolicited bulk e-mail (UBE), which is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. Botnets, networks of virus-infected computers, are used to send about 80% of spam.

b. **Hackers**. In common usage, a ‘hacker’ is a stereotypical person who breaks into computers and computer networks, motivated by the challenge, profits or a political drive. Hackers can use different types of techniques:

i. **Spoofing** attack. A ‘spoofing attack’ is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. There are different forms, but the two best-known are:

1. **Man-in-the-middle**. The man-in-the-middle attack creates a situation in which an attacker spoofs Alice into believing the attacker is Bob, and spoofs Bob into believing the attacker is Alice, thus gaining access to all messages in both directions without the trouble of any cryptanalytic effort.
2. **Phishing**. In this kind of attack, also known as ‘webpage spoofing’, a legitimate web page such as a bank's site is reproduced in ‘look and feel’ on another server under control of the attacker. The main intent is to fool the users into thinking that they are connected to a trusted site, for instance to harvest usernames and passwords.

ii. **Defacement**. ‘Website defacement’ is an attack on a website that changes the visual appearance of the site (as in the Georgia and Estonia cases). These are typically the work of crackers, who break into a web server and replace the hosted website with one of their own messages. Defacement is generally meant as a kind of electronic graffiti, although recently it has become a means to spread by motivated ‘cyber protesters’.

4. **Denial of Service (DoS) attacks**. A DoS attack focuses on consuming scare resources so that legitimate work cannot be done. An example is cutting of power to a data centre. Most DoS-attacks are known as Distributed Denial of Service attacks (DDoS-attacks), which overwhelms Internet-connected systems and their networks by sending a large quantity of network traffic to a specific machine. An attack from a single computer can easily be managed, and so attackers use large numbers of compromised (with malware) machines, the so-called ‘bots’ (bots organised in a botnet is also called a ‘zombie army’), which can be connected together into ‘botnets’, and which can carry out a DDoS-attack.

Annex C: Features of Offensive Cyber Operations

As this paper has shown, offensive cyber operations have their utility, but at the same time their dilemmas. Planners must be constantly aware of these dilemmas. For using offensive cyber correctly, it's important to know of the features of offensive cyber operations. There is a list of 12 features belonging to offensive operations, which is used to categorise offensive cyber operations and cyber conflicts. It is also a list to take into consideration, in order to explain different offensive cyber operations more in detail. The list includes the following features:

1. **Nature of opponents**. Are the offensive operations carried out by nation-states on one-side, both, or neither?
2. **Nature of targets**. Is the offensive cyber operation against a military or a civilian target or a dual use target somewhere in between?
3. **Target physicality**. Is the offensive cyber operation targeting the logical (such as disrupt a software service), the cognitive (such as disrupt the opponents using false information), or the physical (such as breaking a generator).
4. **Integration with kinetic operations**. Is it a stand alone attack? Or is the offensive cyber operation intended to be integrated or simply coincident with kinetic attacks?
5. **Scope of effect**. Is the offensive cyber operation meant for a narrow tactical or technical purpose, such as disabling a botnet, achieving strategic gains, such as coercing a nation to stay out of a conflict, or something operational in between?
6. **Intended duration**. Is the attack meant to have temporary effects, such as distracting an opponent's radar system for a few minutes, or instead be persistent, such as disrupting electrical transmission for the duration of a months-long conflict?
7. **Openness**. Will the offensive cyber operation be overt or covert?
8. **Context**. Is the offensive cyber operation being conducted as part of a wider increase in tension between opponents, or is the operation truly an 'out-of-the-blue' pre-emptive or surprise attack?
9. **Campaign use**. Is the offensive cyber operation meant as part of a larger campaign? This point is a connection with feature 4, but point 4 is focusing on the mixture of kinetic and cyber operations, whereas this feature is more used at the operational, considering cyber as a separate line of operation.
10. **Initiation responsibility**. Who is going to initiate the 'first use' of offensive cyber operations?

11. **Timing and nature of attack**. Is the use of offensive cyber operations meant as a surprise, a pre-emption to an expected incoming attack, or a counter-attack to a previous cyber-attack (a so-called ‘hack back’) or kinetic attack?
12. **Intensity of attack**. If part of a campaign, are the offensive operations characterised by a massive initial set of strikes with many separate attacks? Or do the offensive operations build over time? (Rattray & Healey, 2010)

The list gives a good insight into the different kinds of features and characteristics of offensive cyber operations. It can also be used by planners and operators when considering to plan and execute offensive cyber operations (Rattray & Healey, 2010).

List of Abbreviations

C4ISR	Command Control Communications Computers Intelligence Surveillance and Reconnaissance
C2	Command and Control
CCD CoE	Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
DoD	Department of Defence
DoS	Denial of Service
DDoS	Distributed Denial of Service
FEP	Fuel Enrichment Plant
HQ	Head Quarters
IAEA	International Atomic Energy Agency
ICT	Information and Computer Technology
IHL	International Humanitarian Law
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
JP	Joint Publication
LoAC	Law of Armed Conflicts
MC	Military Committee
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organisation
PLC	Programmable Logic Controller
RoE	Rules of Engagement
SCADA	Supervisory Control and Data Acquisition
UBE	Unsolicited Bulk E-mail
UK	United Kingdom
UN	United Nations

UNSC	United Nations Security Council
US	United States
US DoD	United States Department of Defence
WiFi	Wireless Fidelity (Wireless Local Area Network (WLAN))
WMD	Weapons of Mass Destruction

List of Figures

Literature

Albright, D., Brannan, P., & Walrond, C. (2010). *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Washington DC: Institute for Science and International Security (ISIS). Hentet fra http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

Andreassen, T. A. (2011, 17 July 2011). Norges nye forsvarsgren (translated: Norways new defence domain). *Aftenposten*. Hentet fra http://www.aftenposten.no/nyheter/iriks/Norges-nye-forsvarsgren-5014194.html

Assembly, U. G. (1974). *Resolution 3314 (XXIX) Definition of Agression*. Hentet fra http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement

Beidleman, L. U. W. (2009). *Defining and Deterring Cyberwar*. Philadelphia: U.S. Army War College.

Bernier, M., & Treurniet, J. (2010). *Understanding Cyber Operations in a Canadian Strategic context: More than C4ISR, more than CNO* (Conference on Cyber Conflict Proceedings 2010). Tallinn: CCD COE.

Boivin, A. (2006). *The Legal Regime Applicable to Targeting Military Objectives in the Context of Contemporary Warfare*. Geneva (Switzerland) University Centre for International Humanitarian Law.

Broad, W. J., Markoff, J., & Sanger, D. E. (2011, January 17, 2011). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *The New York Times*. Hentet fra http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&pagewanted=all

Bush, G. W. (2003). *National Strategy to Secure Cyberspace*. Washington DC: The White House. Hentet fra http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

Carr, J., & Shepherd, L. (2010). *Inside cyber warfare*. Sebastopol, Calif.: O'Reilly Media.

CAVV (2011). *Digitale Oorlogsvoering (translated: Cyber Warfare)* (Adviesraad Internationale Vraagstukken (AIV)

(translated: Advisory Council on International Affairs). Hentet fra http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf

Clarke, R. A., & Knake, R. (2010). *Cyber war: the next threat to national security and what to do aboutit*. New York: Ecco.

Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). *On Cyber Warfare*. London: Chatham House. Hentet fra http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2010). *Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security*. Tallinn: Cooperative Cyber Defence Centre of Excellence. Hentet fra http://www.ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_After_the_2007_Cyber_Attacks.PDF

Dam, K. W., Lin, H., & Owens, W. A. (2009). *Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities*. Washington, DC: National Academies Press.

Defensiestaf, N. (2005). *Nederlandse Defensie Doctrine (translated: Netherlands Defence Doctrine)*. (10: 90808440920). Den Haag: Netherlands Defence Staff

DoD, U. (2006). *JP 3-13 Joint Doctrine for Information Operations*. Washington: US DoD

DoD, U. (2011). *JP 1-02 Dictionary of Military and Associated Terms*. Washington: US DoD

Dorffa, R. H., & Ceramib, J. R. (2001). Deterrence and competitive strategies: A new look at an old concept. I M. G. Manwaring (Red.), *Deterrence in the 21st century* (s. 109 - 123). London: Routledge.

Doswald-Beck, L., & Henckaerts, J.-M. (2005). *Customary International Humanitarian Law. Volume1: Rules*. Cambridge: Cambridge University Press.

Economist, T. (2010). The threat from the internet; Cyberwar. It is time for countries to start talking about arms control on the internet. *The Economist*. Hentet fra http://www.economist.com/node/16481504

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier*. Cupertino, CA, USA: Symantec Corporation World Headquarters. Hentet fra http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Ferguson, A. J. (2005). Fostering Email Security Awareness: The West Point Carronade. *EDUCAUSE Quarterly, Volume 28* (No. 1), 4.

Forsvardepartementet. (2012). Proposisjon til Stortinget (forslag til stortingsvedtak): Et forsvar for vår tid (translated: Proposition to Parliament: A Defence of our Time). Hentet fra http://www.regjeringen.no/nb/dep/fd/dok/regpubl/prop/2011-2012/prop-73-s-20112012.html?id=676029

Freeman, C. W. J. (1997). *Arts of Power: Statecraft and Diplomacy*. Washington DC: US Institute of Peace.

Fritz, J. (2008). How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness. *Culture Mandala, Volume 08* (No. 1), 28-80.

GAO, G. A. O. (1996). *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. Hentet fra http://www.fas.org/irp/gao/aim96084.htm

Geers, K. (2011, 21 September 2011). Heading off Hackers. *per Concordiam, 2*, 23-27.

Gray, C. S. (2000). Deterrence and the Nature of Strategy. *Small Wars & Insurgencies, Volume 11* (no. 2), 17-26. doi: 10.1080/09592310008423274

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., et al. (2011). The Law Of Cyber Attack. *California Law Review 2012*, 76.

HPCR (2009). *HPCR Manual on International Law Applicable to Air and Missile Warfare*. Bern: Harvard University.

Hunker, J. (2010). *Cyber war and cyber power, Issues for NATO doctrine* (NATO Research Paper No. 62). Rome (Italy): NATO Defence College, Research Division,. Hentet fra http://www.ndc.nato.int/research/series.php?icode=1

IAEA. (2010). *Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions 1737 (2006), 1747 (2007), 1803 (2008) and 1835 (2008) in the Islamic Republic of Iran*. (GOV/2010/10). Vieanna (AUT): IAEA. Hentet fra http://www.iaea.org/Publications/Documents/Board/2010/gov2010-10.pdf

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 (1977).

ICRC. (2005). *Rules of International Humanitarian Law and other Rules relating to the Conduct of Hostilities* (revised and updated from 1989. utg.). Geneve, Suisse: International Committee of the Red Cross.

Imperva. (2012). *Hacktivism (Definition, Examples, and Video's)*. Hentet fra http://www.imperva.com/resources/glossary/hacktivism.html

Janczewski, L., & Colarik, A. M. (2008). *Cyber warfare and cyber terrorism*. Hershey, Penn.: Information Science Reference.

Kaminski, R. T. (2010). Escaping the Cyber State of Nature: Cyber deterrence and International Institutions. In C. Czosseck & K. Podins (Eds.), *Conference on Cyber Conflict Proceedings 2010* (pp. 79-94). Tallinn: CCD COE Publications.

Katz, Y. (2010). Stuxnet virus set back Iran's nuclear program by 2 years. *The Jerusalem Post, 15 Dec 2010*. Hentet fra http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475

Klimburg, A., & Tirmaa-Klaar, H. (2011). *Cybersecurity and Cyberpower: concepts, conditions and capabilities for cooperation for action within the EU* (nr. ref: EP/EXPO/B/SEDE/FWC/2009-01/Lot6/09. (PE 433.828)). Brussels: European Parliament.

Korns, S. W., & Kastenberg, J. E. (2009). Georgia's Cyber Left Hook. *US Army War College: Parameters, Volume XXXVIII* (Winter 2008-09), p. 60-76.

Kuehl, D. D. (2008). *From Cyberspace to Cyberpower: Defining the Problem* (United States National Defense University. Hentet fra http://www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl%20Final.doc

Kugler, R. L. (2009). Deterrence of Cyber Attacks. I F. D. Kramer, S. H. Starr & L. K. Wentz (Red.), *Cyberpower and National Security* (s. 642). Wahington DC: Center for Technology and National Security Policy & National Defense University & Potomac Books.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, Calif.: RAND.

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy, Volume 4*(63), 24.

Lynn, W. I. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs, Volume 89* (Nr. 5), 97-108.

Marshall, M. S. M. (2010). *Offensive Cyber Capability: Can it Reduce Cyberterrorism?* , United States Army Command and General Staff College, Fort Leavenworth, Kansas.

Minkwitz, O. (2003). *Ohne Hemmungen in den Krieg? Cyberwar und die Folgen (translated: Waging War Without Restraints? Cyber War and Its Consequences)*. Frankfurt am Main (DEU): Hessische Stiftung Friedens- und Konfliktforschung (translated: Peace Research Institute Frankfurt).

Mulligan, B., & Growden, C. (2009). *The Role of Just War Theory in Cyberwarfare* (Hentet fra http://www.amplionitor.com/papers/Philosophy-CyberEthicsintheMilitaryEnvironment.doc

NATO. (2010a). *AJP-01(D) Allied Joint Doctrine. Ratification Draft* Brussel.

NATO. (2010b). NATO in the Cyber Commons, ACT Workshop Report. Tallinn (Estonia): Cooperative Cyber Defence Centre of Excellence (CCD CoE).

NATO. (2011). HQ SACT Point Paper: Information update on cyber defence activity within ACT (pp. 2). Norfolk, USA: NATO ACT.

Nazario, J. (2009). Politically Motivated Denial of Service Attacks. I C. Czosseck & K. Geers (Red.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (s. 163-181). Amsterdam: IOS Press.

Ottis, R. (2011). Theoretical Offensive Cyber Militia Models *Proceedings of the 6th International Conference on Information Warfare and Security* (pp. p 307-313). Washington DC: Academic Publishing Limited.

Ottis, R., & Lorents, P. (2010). *Cyberspace: Definition and Implications*. Tallinn: Cooperative Cyber Defence Centre of Excellence, CCD CoE.

Pace, G. P. (2006). *National Military Strategy for Cyberspace Operations*. Washington DC: US DoD. Hentet fra http://www.bits.de/NRANEU/others/strategy/07-F-2105doc1.pdf

Palojärvi, P. (2009). *A battle in bits and bytes: computer network attacks and the law of armed conflicts*. Helsinki: Erik Castrén Institute of International Law and Human Rights.

Papanastasiou, A. (2010). Application of International Law in Cyber Warfare Operations. *SSRN eLibrary*. doi: 10.2139/ssrn.1673785

Porche, I. R. I., Sollinger, J. M., & McKay, S. (2011). *A Cyberworm that Knows no Boundaries*. Santa Monica: RAND National Defense Research Institute. Hentet fra http://www.rand.org/content/dam/rand/pubs/occasional_papers/2011/RAND_OP342.pdf

Rattray, G., & Healey, J. (2010). Categorizing and Understanding Offensive Cyber Capabilities and Their Use. I *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (s. 23): National Academy of Sciences. Hentet fra http://sites.nationalacademies.org/xpedio/groups/cstbsite/documents/webpage/cstb_059437.pdf

Rowe, N. C. (2008). Ethics of Cyber War Attacks. I L. Janczewski & A. M. Colarik (Red.), *Cyber Warfare and Cyber Terrorism* (s. 105 - 111). Hershey, Penn.: Information Science Reference.

Rønneberg, K. (2011, 19 March 2011). «Operation Odyssey Dawn», USA leder an i et massivt angrep på flybaser og andre militære mål i Libya. Tripoli er nå under angrep (translated: USA leads a massive attack on Airbases and other military objectives in Libya. Tripoli is under attack now). *Aftenposten*. Hentet fra http://www.aftenposten.no/nyheter/uriks/article4066369.ece

Sale, R. (2012). Stuxnet Loaded by Iran Double Agents. *Industrial Safety and Security Source (ISS Source)*. Hentet fra http://www.isssource.com/stuxnet-loaded-by-iran-double-agents/

Schjølberg, S. (2010). Wanted: A United Nations Cyberspace Treaty. In A. Nagorski (Ed.), *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway* (pp. 28). New York: The EastWest Institute.

Schmitt, E., & Shanker, T. (2011, October 17, 2011). U.S. Debated Cyberwarfare in Attack Plan on Libya. *The New York Times*. Hentet fra http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1

Schröfl, J., Rajaee, B. M., & Muhr, D. (2011). *Hybrid and cyber war as consequences of the asymmetry: a comprehensive approach answering hybrid actors and activities in cyberspace ; political, social and military respones*. Frankfurt am Main: Peter Lang Verlag.

Shakarian, P. (2011). Stuxnet: Cyberwar Revolution in Military Affairs. *Small Wars Journal, 14 April 2011*, 10 pages.

Solon, O. (2010, 15 October 2010). Do we need a Geneva convention for cyber warfare? *Wired.co.uk*. Hentet fra http://www.wired.co.uk/news/archive/2010-10/15/cyber-warfare-ethics

Sundseth, G. R. (2012). Cyber og Cybersikkerhet - Voksende trusler og nye utfordringer (translated: Cyber and Cybersecurity - Increasing threats and new challenges). *Norsk Militært Tidsskrift (translated: Norwegian Military Journal)*(Årsgang 182, nr. 1/2012), 36-40.

Tettero, M., & Graaf, P. d. (2010). Het Vijfde Domein voor de Krijgsmacht: Naar een Integrale Strategie voor Digitale Defensie (translated: 'The Fifth Domain for the Armed Forces: Heading for an Comprehensive Strategy for a Digital Defence'). *Militaire Spectator (translated: Military Spectator), Volume 179, ,* (Nr. 5).

Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A.-M., & Vihul, L. (2008). *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn: CCD CoE.

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents: Legal Consideations*. Tallinn (EST): Cooperative Cyber Defence Centre of Excellence (CCD COE).

UN. (1945, 24 September 1973). *The Charter of the United Nations*. Hentet fra http://www.un.org/en/documents/charter/index.shtml

UNSC. (2011). *Resolution 1973 (2011): resolution on Lybia*. (S/RES/1973 (2011)). United Nations Security Council. Hentet fra http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N11/268/39/PDF/N1126839.pdf?OpenElement

US Strategic Command, D. P. a. P. (2006). *Deterrence Operations Joint Operating Concept. Version 2.0*. Washington. Hentet fra http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA490279