NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NORWEGIAN CYBER DEFENSE

by

Karl Birger Stensboel

December 2013

Thesis Advisor: Dorothy E. Denning
Second Reader: Kristen Tsolis

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE NORWEGIAN CYBER DEFENSE

5. FUNDING NUMBERS

6. AUTHOR(S) Karl Birger Stensboel

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

This thesis postulates the need for a more proactive approach to cyber defense in Norway and offers recommendations about how Norway can be better prepared to counter cyber threats. It finds that Norway's strategic infrastructure is vulnerable to cyber attacks and that Norway has no coherent strategy for meeting this challenge. The thesis argues that an effective cyber defense requires a wide range of offensive and defensive measures as well as a central authority for command and control. Norway must increasingly be perceived as a serious and tough player in cyberspace; this requires proactive thinking and offensive capabilities. An important first step would be to make the Ministry of Defense responsible for the nation's cyber defense.

14. SUBJECT TERMS Cyberspace, Cyber warfare, Cyber strategy, Chinese cyber warfare, Norwegian cyber defense policy, Norwegian Armed Forces.

15. NUMBER OF PAGES 101

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

NORWEGIAN CYBER DEFENSE

Karl Birger Stensboel
Major, Royal Norwegian Army
Norwegian Military Academy, 1989

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL

December 2013

Author: Karl Birger Stensboel

Approved by: Dorothy E. Denning
Thesis Advisor

Kristen Tsolis
Second Reader

John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis postulates the need for a more proactive approach to cyber defense in Norway and offers recommendations about how Norway can be better prepared to counter cyber threats. It finds that Norway's strategic infrastructure is vulnerable to cyber attacks and that Norway has no coherent strategy for meeting this challenge. The thesis argues that an effective cyber defense requires a wide range of offensive and defensive measures as well as a central authority for command and control. Norway must increasingly be perceived as a serious and tough player in cyberspace; this requires proactive thinking and offensive capabilities. An important first step would be to make the Ministry of Defense responsible for the nation's cyber defense.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACD	Active Cyber Defense
ARPA	The Advanced Research Project Agency
BGP	Border Gateway Protocol Poisoning
Botnet	Collection of Internet Connected Programs
CI	Critical Infrastructure
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNI	Critical National Infrastructure
CNO	Computer Network Operations
DCS	Distributed Control Systems
DDos	Distributed Denial of Service
DoD	Department of Defense
DSB	Norwegian Directorate for Civil Protection
DT	The Norwegian Data Protection Authority
EU	European Union
EW	Electronic Warfare
FFI	The Norwegian Defense Research Establishment
GSD	General Staff Department
HTTP	Hyper Text Transfer Protocol
HUMINT	Human Intelligence
ICS	Industrial Control System
ICS-CERT	The Industrial Control Systems Cyber Emergency Response
ICT	Information and Communications Technology
IDS	Intrusion Detection System Team
INEW	Integrated Network Electronic Warfare
ISP	Internet Service Providers

IW	Information Warfare
KRIPOS	(Norwegian) National Criminal Investigation Service
MRB	Master Boot Record
NIS	Norwegian Intelligence Service
NorCERT	Norway's National Center for the Management of Serious Cyber Attacks Against Critical Infrastructure and Information
NorSIS	The Norwegian Centre for Information Security
MuCD	Military Unit Cover Designator
NIS	Norwegian Intelligence Service
NRI	Networked Readiness Index
NSM	Norwegian National Security Authority
NTSB	The National Transportation Safety Board
PIN	Personal Identification Number
PLA	Peoples Liberation Army
PLC	Programmable Logic Controllers
PRC	People's Republic of China
PST	Norwegian Police Security Service
PSYOPS	Psychological Operations
PT	The Norwegian Post and Telecommunications Authority
SCADA	The Supervisory Control and Data Acquisition
TNT	Trinitrotoluene, Explosives
UN	United Nations
URL	Uniform Resource Locator
USB	Universal Serial Bus

ACKNOWLEDGMENTS

The author would like to thank his supervisor, Dr. Dorothy E. Denning, for her thorough knowledge of cyber warfare and support throughout this project. This thesis would not have been possible without her support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> "We must try to identify which threats the nation will face in ten, fifteen years."
>
> Head of Norwegian Cyber Defence,
> Major General Roar Sundseth, Aug 13, 2013

A. INTRODUCTION

This thesis will analyze the cyber threat environment confronting Norway's Critical National Infrastructure (CNI). The intention is to assess whether Norway utilizes cyber defense resources in an optimal manner. The thesis will suggest ways to improve and enhance effectiveness in cyber defenses to better meet the rapid changes in cyberspace.

Recognition of future challenges related to electronic threats was mentioned in official documents as early as 13 years ago. Since then, developments have been significant with respect to both the rapid expansion of technology and to the growing importance of the Internet and cyberspace. In Norway, the so-called Vulnerability Committee report from 2000 describes with foresight an upcoming change in technology: Especially interesting is the possibility of the use of new methods that can be given the paradoxical term "soft terrorism," namely electronic means aimed at information and communication systems.[1] The Committee report continues: "The risks of a devastating online attack are in many ways just as real as a more conventional military attack. There have been no reports of organized attacks carried out on a large scale, although there have been incidents in connection with the tense international

1 Norges offentlige utredninger, (NOU) [Norwegian Official Reports] 2000:24, Et sårbart samfunn, Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet, 4 juli 2000 [A Vulnerable Society: Challenges for Norwegian Security and Preparedness, July 4, 2000], 7, http://www.regjeringen.no/Rpub/NOU/20002000/024/PDFA/NOU200020000024000DDDPDFA.pdf.

situation."[2] A more up-to-date parliamentary bill from 2012 describes the cyber threat as:

> Norwegian society and state security are challenged by threats related to the use of digital technology and the ability to spread and control information. Attack in the digital space, also referred to as "cyberspace," is one of the fastest growing threats to individuals, businesses and public institutions. The attacks can come from both state and non-state actors, such as from other countries' military defense, intelligence services, organized crime, terrorist and extremist groups, competing businesses and individual hackers. The most serious threat comes from states.[3]

The Norwegian Intelligence Service 2012 annual report, "Focus," envisions that cyberspace may become an arena that acquires an important role for crisis and conflict management. Several states are developing modern cyber capabilities to attack critical areas of society. Targets can be infrastructure, social activities or decision-making and information processes. The Great Powers have many instruments in their toolbox, operations in the cyber domain being one.[4]

Despite knowledge and understanding of the threat in cyberspace, the assessment of the data security department, NorCERT (a part of the Norwegian National Security Authority (NSM)), is that the security status for 2012 is unsatisfactory.[5]

---

[2] Ibid., 39.

3 Forsvarsdepartementet [Norwegian Ministry of Defence], St.prp. Nr 73 S (2011–2012) Et Forsvar for vår tid [The Ministry of Defence: A defence for our time, Parliamentary Bill no. 73 S (2011–2012)], 24, http://www.regjeringen.no/pages/37583840/PDFS/PRP201120120073000DDDPDFS.pdf.

4 Norwegian Intelligence Service, Focus 2012, 43. http://forsvaret.no/om-forsvaret/organisasjon/felles/etjenesten/Documents/etj_lo-res.pdf.

5 Nasjonal sikkerhetsmyndighet [National Security Authority], Rapport om sikkerhetstilstanden 2012, 3, [Security conditions 2012], https://www.nsm.stat.no/Documents/Risikovurdering/Ugradert%20rapport%20om%20sikkerhetstilstanden%202012.pdf.

B. PURPOSE AND SCOPE

The purpose of this thesis is to critically evaluate Norwegian cyber security. First, the thesis examines developments in cyberspace, including developments in espionage and warfare capabilities, to show what type of actors use cyberspace as an arena of conflict. It also shows which technology is most commonly used for both offensive and defensive operations in cyberspace to provide an understanding of cyberspace as a venue that is distinct from other more traditional arenas of conflict. Because cyberspace has become a unique arena with unique threats, traditional thinking about defense in cyberspace is hardly appropriate.

Second, to give an idea of the current threat, and how it is likely to develop in the future, this thesis focuses on China. China is the leading nation with respect to cyber espionage, a current and highly relevant threat to Norwegian high tech enterprises and critical infrastructure. A study of China's cyber capabilities will also give an indication of how other individuals, groups or nations may be able to develop their own capabilities in the future.

Third, open sources are studied to find how responsibility and preparedness in cyber defense is delegated in Norway. The findings indicate that Norway's defense organization is fragmented with many actors without overarching or coordinating management.

The cyber activities of criminals and organized crime gangs motivated by financial or material gain are excluded from this thesis.

C. BACKGROUND

To understand the extent and seriousness of what cyber war is, it is important to remember what such a war *can* be and how seriously the threat is perceived. In a speech in July 2012 at Intrepid Sea, Air and Space Museum in New York, U.S. Defense Secretary Panetta warned that the United States faces the possibility of a "Cyber Pearl Harbor" and is increasingly vulnerable to foreign computer hackers who can dismantle the nation's power grid, transportation

system, financial networks, and government.[6] Reports from the Department of Homeland Security show that in a one-year period, 2010 to 2011, the number of attempted and successful cyber attacks against U.S. critical infrastructure—such as dams and energy and water systems—rose more than 383 percent.[7]

Although the above is an assessment of the threat to the United States and not Norway, it is important to remember that the infrastructure in the two countries have many common features. Computers, Internet and network constitute a common denominator regardless of whether you are an American or a Norwegian. A variety of actors, some private, some state-sponsored, execute cyber exploitation and attacks on a daily basis against numerous targets around the world. Evidence from the last 10 years shows that nations like China, Russia and the United States have the capacity to conduct cyber war with significant results. The Russian cyber attacks on both Estonia and Georgia, for example, demonstrates emphatically that nations with such capability can be quite successful. The attack against Iran with Stuxnet[8] shows how targeted actions against industrial control systems could have serious consequences for the nations that are exposed to them. Both the ability and the intent to attack in cyberspace form the basis for what we refer to as the cyber threat.

D. THE THREAT TO NORWAY

The questions are: Is there any cyber threat to Norwegian infrastructure? Is it conceivable that strategic interest in future conflicts will leave Norway caught between the great powers' interests? While there are no certain answers to these

6 Elisabeth Bumiller and Tom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," The New York Times, October 11, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.

7 Nicole Blake Johnson, "Report: Cyber attacks on critical infrastructure jump 383% in 2011," Federal Times, July 3, 2012, http://www.federaltimes.com/article/20120703/IT01/307030004/Report-Cyber-attacks-critical-infrastructure-jump-383–2011.

8 STUXNET is a computer worm discovered in 2010, created to attack Iranian nuclear productions systems.

questions, it is important to analyze nations' ability and willingness to facilitate cyber attacks or to gather intelligence. In many cases, we see that cyberspace is an important supplement to traditional arenas of both war and intelligence collection. To give an idea of the complexity and scope of cyberspace, it may be interesting to study some different actors' assessment of the challenges related to it:

The McAfee Virtual Criminology Report 2009 Virtually Here: The Age of Cyber Warfare asserts:[9]

> If a major cyber conflict between nation states were to erupt, it is very likely that the private sector would get caught in the crossfire. Most experts agree that critical infrastructure systems—such as the electrical grid, banking and finance, and oil and gas sectors—are vulnerable to cyber attack in many countries.
>
> Some nation states are actively doing reconnaissance to identify specific vulnerabilities in these networks. In the words of one expert, nation states are "laying the electronic battlefield and preparing to use it."

In the case of Norway, the Norwegian Intelligence Service (NIS) writes in the 2012 "Focus" publication: "Chinese authorities are using digital operations to a large degree as a replacement for human collection and often use proxies for obtaining information."[10] Both examples show a traditional conflict-orientated approach to the use of cyberspace. However, cyberspace can also be used for other purposes**;** in "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," Danish scientist Magnus Hjortdal claims:"[11]

> China's military strategists describe cyber capabilities as a powerful asymmetric opportunity in a deterrence strategy. Analysts consider

9 McAfee, Virtual Criminology Report 2009 Virtually Here: "The Age of Cyber Warfare,," 3, http://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf.

10 Norwegian Intelligence Service, Focus 2012, 44. http://forsvaret.no/om-forsvaret/organisasjon/felles/etjenesten/Documents/etj_lo-res.pdf.

11 Magnus Hjortdal, Journal of Strategic Security, Volume 4, Number 2, Summer 2011: Strategic Security in Article 2 the Cyber Age, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," 5, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss.

> that an “important theme in Chinese writings on computer network operations (CNO) is the use of computer-network attack (CNA) as the spear point of deterrence.” CNA increases the enemy’s costs to become too great to engage in warfare in the first place.

Hjortdal puts cyber warfare in a context where the goal is not necessarily conflict, but conflict prevention through deterrence. Deterrence in cyberspace is an opportunity for nations that have well-developed cyber skills to openly let it be known that they have and will make use of these capabilities. In a later chapter it will be shown that a nation`s military capacity enhances its deterrence in cyberspace, but it is not essential.

In a modern society where many challenges, contexts and interests are more closely intertwined than ever, Norway may be affected by peripheral conflicts. The fact that Norway—besides being a NATO member—is supplying the European powers with natural gas, could make Norway a target for groups or nations that are in conflict far away from its borders. This does not mean that the Norwegian infrastructure will be attacked or destroyed, but the threat alone can have a great effect if ample protection is unavailable.

The extent to which a nation will use force will always be unclear; although military doctrines may provide some insight, they do not tell the whole and complete truth. It may, therefore, be interesting to see what Chinese officers write about warfare. In the book “Unrestricted Warfare” colonels Liang and Xiangsui write:[12]

> In terms of beyond-limits warfare, there is no longer any distinction between what is or is not the battlefield. Spaces in nature including the ground, the seas, the air, and outer space are battlefields, but social spaces such as the military, politics, economics, culture, and the psyche are also battlefields…. Warfare can be military, or it canbe quasi-military, or it can be non-military…. These characteristics of beyond-limits war are the watershed between it and traditional warfare, as well as the starting line for new types of warfare.

12 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China’s Master Plan to Destroy America* (Pan American Publishing Company (August 22, 2002), 206.

China's capabilities and doctrines could provide an important indication of the progress in cyber warfare that can be expected in the future.

For Norway, the challenges remain unchanged, regardless of who constitutes the threat, or in what form it materializes.

E. RESEARCH QUESTION

How can Norway best counter threats in cyberspace?

F. METHODOLOGY

To answer the research question, the thesis explores the following claims:

- Cyberspace has become an arena of warfare at tactical, operational and strategical level.
- Cyberspace is a venue that will have a substantial role in crisis and conflict.
- The major powers are preparing to use digital operations as a tool in conflict resolution, primarily alongside other more traditional measures.
- Threats in cyberspace have changed, and Norway is not prepared.
- The primary state actors behind threats in cyberspace are foreign intelligence and security services.
- Cyber power can be used to produce preferred outcomes within cyberspace.[13]
- China has the most extensive cyber-espionage capability in the world.
- China currently conducts extensive cyber operations worldwide.
- Several communities are acquiring expertise in intrusion and influence of the overall electronic control systems (SCADA) of the critical infrastructure.
- Norway's CNI could be a potential target as a part on a beyond-limits warfare approach.
- Norwegian cyber defense lacks central management and one responsible ministry.
- Norway's role as supplier of natural gas is vulnerable to cyber attacks.

13 Joseph S. Nye Jr., *The Future of Power* (New York: Public Affairs, 2011), 113.

- A defensive posture is not necessarily the best way of protecting a country in cyberspace.

The five remaining chapters of the thesis are designed to substantiate these claims and answer the research question. The analysis is based on qualitative research of both empirical and conceptual literature on cyber warfare and related topics.

As background for the understanding of how cyberspace has developed, Chapter II describes the essential elements of cyberspace. The discussion assumes that security is a prerequisite for all work in cyberspace, either as an individual who sends email or as a nation that will defend vital infrastructure. The chapter builds the theoretical foundation for later understanding of the complexities of cyber both in terms of attack and defense, cyber threat and cyber power.

Chapter III describes how states perceive cyber power, why states invest in cyber technology and how cyber power can be used. The chapter also describes the various theories of cyber power and how cyber can be used to support military operations.

Chapter IV deals with China's growing cyber capabilities, including the rate of its cyber operations. China's capacity and capabilities in the cyber domain are discussed and put into a frame that can give insight into how the cyber domain is likely to be developed in the future.

Chapter V describes Norway's cyber strategy, cyber defenses and distribution of labor.

Chapter VI summarizes the preceding analyses and discussions and argues for changes in the cyber defenses.

II. CYBERSPACE: DEVELOPMENT OF A NEW DOMAIN

A. INTRODUCTION

This chapter aims to provide an understanding of what cyberspace is. Some argue: "After land, sea, air and space, warfare has entered the fifth domain: cyberspace."[14] The chapter provides an overview of cyber security, the role of cyberspace in conflict, and how cyberspace is both a target and a tool of conflict. The chapter continues with a description of offensive and defensive technologies before it ends with a description and role of infrastructure. To show the severity of a planned cyber attack against a state, the chapter ends with a presentation of how Estonia was the victim of a major cyber attack in 2007.

There are several definitions of cyberspace, but I have chosen to apply Daniel T. Kuehl's definition:

> [A] global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.[15]

Cyberspace also includes telecommunications, radio waves and other types of networks that process information. We are all part of this network, either as individuals or as employees. Computers, digital technology and cyberspace are all established terminology, and this thesis has as a premise that the reader has the basic knowledge of computers and networks. Regardless of location or reason for use, ever since the Internet and PCs came into common use, individuals have had to deal with one prominent challenge: hostile actors and cyber security.

---

14 *The Economist*, "War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?," The Economist, July 1, 2010, http://www.economist.com/node/16478792.

15 Daniel T. Kuehl, "From Cyberspace to Cyberpower," Ch 2 in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 28.

B. CYBER SECURITY AND THREAT SOURCES

Actors who consciously decide to conduct cyber attacks can potentially cause problems for any client who directly or indirectly is connected to the Internet. In addition to deliberately implemented and planned attacks, cyber systems may be vulnerable to accidents and natural disasters, as shown in Figure 1.

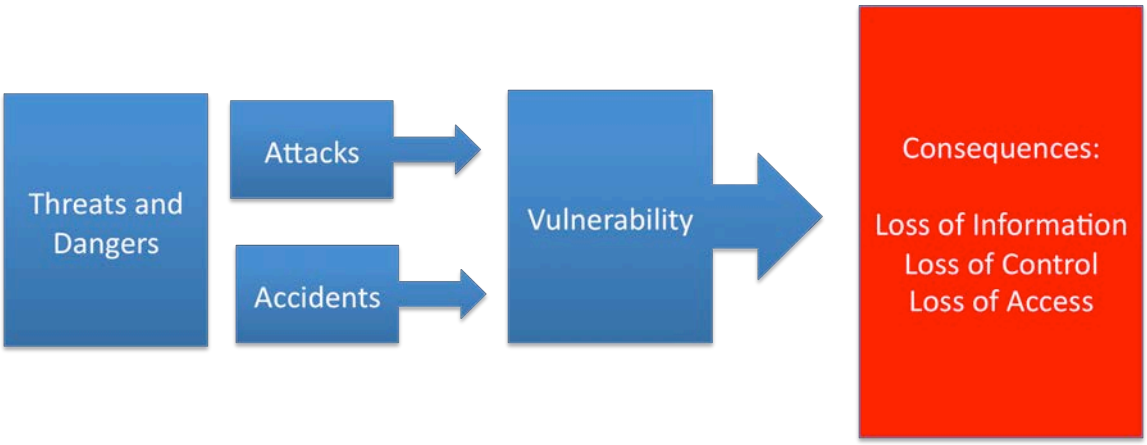

Figure 1. Threats and dangers.[16]

Accidents and unintentional events are a major source of problems; an incident may be power outage, lack of cooling or inadequate maintenance of the networks. While these types of events may have serious consequences, they are not discussed in this thesis; the focus is on desired and planned attacks.

An important factor is the number of potential attackers; in practice, anyone with an IP address is a potential attacker or target. This means that any person with harmful intent can carry out an attack against anybody with Internet access. The consequence is that the likelihood of being a target of an attack is very high, and it applies to both individuals and organizations. Technological development, distribution, and dependence on cyberspace form the backdrop for why this domain has developed multiple sources of threats.

16 John Thuv, Ron Windvik, Kjell Olav Nystuen and Tormod Sivertsen, "Vulnerabilities in Internet,," 21, has given me ideas to the figure, http://rapporter.ffi.no/rapporter/2007/00903.pdf.

Groups or individuals may intentionally deploy cyber exploits targeting a specific cyber asset or attack through the Internet using a virus, worm, or malware with no specific target. Different types of cyber threats can use various cyber exploits that may adversely affect computers, software, or a network.[17] The U.S. Accountability Office provides the following definitions:

1. Botnet Operators

Botnet operators use a network, or botnet, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial of service attack or servers to relay spam or phishing attacks).[18]

2. Criminal Groups

Criminal groups seek to attack systems for financial gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and criminal organizations also pose a threat through their ability to conduct industrial espionage and large-scale economic theft and by hiring or developing hacker talent.[19]

3. Hackers

Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, protest, revenge, stalking others, and monetary gain, as well as other reasons. Hackers can download attack scripts and protocols from the Internet and launch attacks against victim sites. Attack tools have become more sophisticated over time; in addition, they have become easier to

17 U.S. Government Accountability Office, “Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance” (Washington, D.C., 2010), 4–5, http://gao.gov/assets/310/308401.pdf.

18 Ibid., 4.

19 Ibid.

use. According to the Central Intelligence Agency (CIA), the large majority of hackers do not have the requisite expertise to threaten complicated targets, such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.[20]

4. Insiders

The disgruntled insider of an organization is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of the target system often allows them to gain unrestricted access, thereby causing damage to the system or stealing system data. The insider threat includes contractors hired by the organization, as well as employees who accidentally introduce malware into systems.[21]

5. Nations

Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop IW doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures, thereby affecting the daily lives of citizens across the country.[22]

Each actor has different motivations, abilities and finances to pose a threat. Common to all is their potential to be dangerous. An insider with a USB stick can cause just as much damage as a nation that has vast resources at its disposal. The potential of damage and conflict is considerable; small resources that are inserted in the right place can have major consequences. Cyberspace is

[20] Ibid.

[21] Ibid.

[22] Ibid.

therefore an arena where those who want to produce effects have great opportunities, both positive and negative.

C. WHAT IS THE ROLE OF CYBERSPACE IN CONFLICT?

Cyber technology is greatly altering the nature of warfare as we enter the twenty-first century. Thinking of cyberspace as an arena of conflict goes as far back as 1976 when Thomas P. Rona published the paper, "Weapon Systems and Information War."[23] Some analysts claim that this early work was only focused on information flow in military operations, but it helped to define cyberspace at an early stage.

John Arquilla and David Ronfeldt published "Cyber War is Coming!" in 1993, in which they advocated that warfare was no longer reserved for those who used the most capital, labor and technology on the battlefield, but also those who had the best information.[24]

From 1988 until the present, the tremendous development of the Internet has also resulted in a growth in cyber attacks and cyber crime. Some consider the cyber attacks on Estonia that started April 27, 2007 to be the first major cyber attack on a nation state. Even though Morris's worm in 1988 took systems down for days, it posed no great threat or damage; however, the attack on Estonia was of a completely different magnitude.

Cyber incidents in recent years have aroused great concern among governments in many countries, including Norway. The potential threat is substantial. The greatest concern, however, is that which has not yet happened. Because cyberspace is a relatively new phenomenon, nobody can accurately predict the potential threats and vulnerabilities.

---

[23] Thomas P. Rona, "Weapon Systems and Information War" (Office of the Secretary of Defense, July 1, 1976).

[24] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" (RAND Corporation 1993).

Cyberspace can have multiple roles and may be used as a tool for military operations. Gregory Rattray and Jason Healey explain a few key aspects relevant to the role of cyberspace as a war fighting domain:[25]

> First, logical but physical: Though a war fighting domain, cyberspace has some striking differences from the other domains. "Unlike the land, sea, air and space where the laws of physics do not change, cyberspace is a man-made creation that continually changes and evolves."[26]
>
> Second, usually used, owned, and controlled predominantly by the private sector: Future conflicts in cyberspace are very likely to be won or lost in the private sector, which runs, owns, and depends on the underlying networks and information, at least in the most advanced economies.[27]
>
> Third, tactically fast but operationally slow: Cyberspace, where the computer is the battlefield, is widely considered to be an operational environment through which an attacker can strike with minimal investment while yielding potentially large-scale effects with great speed.[28]
>
> Fourth, fraught with uncertainty: Cyberspace is an extremely complex environment, characterized by rapid change and adaption, whose direction is difficult to predict.[29]

A common denominator is that cyberspace cuts across boundaries between the civil and the military and between the public and the private. Anyone who has the will to use cyberspace can affect the government, the military, businesses or private persons. An attack may have a number of secondary consequences on other peripherally involved actors. This means that cyber attacks can have accidental and unpredictable consequences.

---

[25] Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council, (The National academics Press 2010), 77.

[26] Ibid., 78.

[27] Ibid., 79.

[28] Ibid.

[29] Ibid.

D. OFFENSIVE CYBER TECHNOLOGIES AND METHODS

In digital space, some claim that the attackers always have an advantage. They only need to find one hole to penetrate a system, while those who defend the system must locate and seal all holes.[30] Both offensive and defensive technologies have their own characteristics and methods. This section gives an overview of technologies and methods for cyber offensive operations, including network intrusions, malware, botnets, and denial-of-service (DoS) attacks. It also gives an overview of technologies and methods of defense, including cryptography, access controls, and intrusion/malware detection/prevention.

1. Systems Penetration

Systems penetration could be an attack on servers, routers, PCs, smart phones or any device with processor and memory. Attackers can gain entry through a variety of means, such as logging into a user or system account with a password or PIN. The attacker might exploit a vulnerability in software (e.g., web services) or find backdoors into the system. The attacker might join the target's wireless network where it may be possible to read traffic, alter it, and get access to other devices on the network.

2. Phishing Attacks

Another trend in attacks involves "phishing" email: the aim is revealing sensitive information or getting malicious software installed, by an attacker pretending to be a trusted organization or individual. When the unsuspecting user enters account information, the attacker harvests this data, using it for identity theft. Recent phishing attacks include so-called spear phishing attacks that target a particular organization or even individuals. Such phishing email may appear to come from a trusted individual, such as a government, corporate executive or

30 Norwegian Intelligence Service, Focus 2012, 26, http://forsvaret.no/om-forsvaret/organisasjon/felles/etjenesten/Documents/etj_lo-res.pdf.

manager and exhorts the recipient to take some action. By clicking on a link in a spear-phishing email could allow the attacker to exploit the victim's browser.[31]

3. Denial-of-Service (DoS) Attacks

A Denial-of-Service attack aims to disrupt the normal operation of a computer system (e.g., web server or email server). A common method used in DoS attacks is to deluge a system or site with messages that drastically slow down its response time or to overwhelm its data handling capacity, resulting in a system crash. In many countries a DoS attack is a criminal offense even if intended as a prank.[32]

In a Distributed Denial-of-Service (DDoS) attack a network of computers sends attack packets all at once. This kind of attack typically generates more traffic than do single-source DoS attacks and often renders the target system unavailable to its intended users.

4. Malware (Malicious Software)

Malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses, and spyware. Viruses, for example, can wreak havoc on a computer's hard drive by deleting files or directory information. Unknown to the user, spyware can gather data such as web pages visited or credit card information from a user's system.[33] Remote access Trojans can give the attacker full control over a compromised machine.

---

31 Edvard Skoudis, "Evolutionary Trends in Cyberspace," Ch 6 in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 165.

32 Business Dictionary, http://www.businessdictionary.com/definition/denial-of-service-DOS-attack.html.

33 Techterms definitions, http://www.techterms.com/definition/malware.

Malware may be propagated in many ways, including emails with attachments and websites. Malware is often installed in stages until the adversary has full control of the target system.[34]

5. Botnets

An attack technology of particular power and significance is the botnet. Botnets are networks of compromised computers that are remotely controlled by the attacker. On a compromised computer, an individual bot is connected to the Internet and runs software clandestinely introduced by the attacker. The attack value of a botnet arises from the sheer number of computers that an attacker can control, often tens or hundreds of thousands and perhaps as many as a million. Since all of these computers are under one attacker's control, the botnet can act as a powerful amplifier. Botnets are ideally suited for conducting Distributed Denial-of-Service (DDoS) attacks against computer systems.[35]

E. DEFENSE TECHNOLOGIES AND METHODS

With so many methods of conducting cyber attacks, a huge market for technology that protects the network from unauthorized access has grown. Anti-virus programs for personal computers are prevalent; however, defense technology must be more than just anti-virus.

1. Cryptography

Cryptography is the science of principles and techniques to hide information so that only the authorized agent has the opportunity to reveal the contents. The wide spread development of computer communications has led to that new forms of cryptography are developed. In data and telecommunications, cryptography is necessary for communication over any untrusted medium, which includes just about any network, particularly the Internet. Within the context of

34 William A. Owens, Kenneth W. Dam, and Herbert S. Lin (eds.), Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities, National Research Council, (The National Academies Press, 2009), 97–98.

35 Ibid., 92.

any application-to-application communication, some specific security requirements include: Authentication: 1) Proof of a person's identity and the source of a message, 2) Privacy/confidentiality: Contributes to that it's only recipient of a message can read it, 3) Integrity: Retains the original message content, and 4) Non-repudiation: Prove that the sender is the one who sent the message.[36]

Cryptography supports all of these functions. It not only protects data from theft or alteration, but it also provides user and source authentication and non-repudiation.

Three types of cryptographic schemes are used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions.[37]

2. Identification and Authentication

Identification is the process whereby a network element recognizes a valid actor's identity. Authentication is the process of verifying the claimed identity of an actor who may be a person, a process, or a system (e.g., another network element) that access a network element to perform tasks or process a call. Information used to verify the claimed identity of a user can be based on a password, Personal Identification Number (PIN), smart card, biometric, token, exchange of keys, or other similar devices.[38]

3. Intrusion and Malware Detection and Blockage

An intrusion detection system (IDS) inspects inbound and outbound network activity and Identifies suspicious patterns that may indicate a network or

36 An overview of Cryptography, Ch 2, http://www.garykessler.net/library/crypto.html#purpose.

37 Ibid., Ch 2.

38 National Institute of Standards and Technology, Computer Security Division, "Identification and Authentication of Users," http://csrc.nist.gov/publications/nistpubs/800–11/node26.html.

system attack.[39] Malware detection screens incoming data (files, web pages, etc.) for malware, Trojan horses and phishing attempts. Both block packets and data that match the signatures of known threats.[40]

Both offensive and defensive technologies are under constant development and exist in a competitive relationship. The following section discusses a series of spectacular attacks against critical infrastructure and the resulting effects.

F. CRITICAL INFRASTRUCTURE, VULNERABILITIES AND ATTACKS

Critical infrastructure (CI), which comprises systems that are essential to maintain society's critical functions, is the backbone of a nation's economy, security and health. Examples are roads, water, and power. In case of failure in these systems, the society is not able to maintain the supply of goods and services upon which the population is dependent. The critical infrastructure supports national security and the country's vital national interests.[41]

Serious failures in critical systems could rapidly lead to massive disruption in society. To a greater or lesser extent, the different systems are interdependent, and the effects of failure in one of them can have cascading effects on others.

Critical infrastructure (CI) is familiar to most people as the power used in our homes, heating, water, roads, bridges, the means of communication both the physical as well as telephones, radios, networks, computers and TV. These systems are all networks of computers and other devices being monitored or

39 Webopedia, is a free online dictionary for words phrases and abbreviations that are related to computer and Internet technology, http://www.webopedia.com/TERM/I/intrusion_detection_system.html.

40 Cisco, Security Flirting, Definitions, https://docs.meraki.com/display/MX/Security+filtering.

41 Norges offentlige utredninger (NOU), [Norwegian Official Reports] 2006:6, Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner, 5 japril 2006 [When security is important: Protecting the nation's critical infrastructures and critical societal functions, April 5, 2006, 11, http://www.regjeringen.no/nb/dep/jd/dok/nouer/2006/nou-2006–6/5/1.html?id=157439.

controlled by them. Supervisory Control and Data Acquisition (SCADA) systems, which provide centralized control over the other components, perform key functions for many critical services, including power generation and distribution, oil and gas distribution, and water treatment and distribution. CI are the heart and brain of systems and networks, whether physical or virtual, so vital that their incapacitation or destruction would have a devastating effect on national security, economic security and national public safety.[42] Historically, with their reliance on proprietary networks and hardware, SCADA systems were considered safe from cyber attacks and were not designed for security. The situation has changed, but security is still inadequate in many of these systems, making them vulnerable to disruption of service or manipulation of operational data that could result in public safety concerns.[43] In 2013 Norwegian newspaper Dagbladet found over 2,500 SCADA systems in Norway used for example in defense, health, oil industry and the public transportation. Some were protected by a username and password, others were as open as any website.[44] Cyber attacks on SCADA systems, especially in energy production and distribution systems, could endanger public health and safety as well as invoke serious environmental damage

G. ATTACKS–A HISTORICAL REVIEW

Infrastructure attack is a story as old as war. Since time immemorial attackers have sought to cut off their target's water supply and transportation, often with decisive results. Starting in the nineteenth century, the rise of modern infrastructure systems brought heightened concerns about vulnerability.[45]

---

42 U.S. Department of Homeland Security, "National Infrastructure protection Plan," 7, http://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf.

43 Arne Roar Nygård, "Risk management in SCADA system,," Master's Thesis, Royal Institute of Technology, Sweden, July 2004, p iii, http://brage.bibsys.no/hig/handle/URN:NBN:no-bibsys_brage_4310.

44 Linn Kongsli Hillestad, Espen Sandli and Ola Strømman, "In the worst case, people can die," Dagbladet, October 17, 2013, http://www.dagbladet.no/2013/10/17/nyheter/innenriks/datasikkerhet/nullctrl/28572676/.

45 William D. O'Neil, "Cyberspace and Infrastructure" Ch 5 in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 113.

Attacks against single critical targets became a reality after 1982 and showed that these were vulnerable to cyber attacks. Even greater attention was given to the cyber attacks against Estonia in 2007 and Georgia in 2008; the last section describes the events in Estonia.

1. Attacks on Infrastructure

In "A Survey of SCADA and Critical Infrastructure Incidents," Bill Miller and Dale C. Rowe have listed examples of attacks targeting critical infrastructure and the effects they have had. A selection of these attacks is provided in the following subsection.[46]

a. Siberian Pipeline Explosion (1982)

In 1982, intruders planted a Trojan horse in the SCADA system that controls the Siberian Pipeline. This is the first known cyber-security incident involving critical infrastructure and caused an explosion equivalent to three kilotons of TNT.[47]

b. Chevron Emergency Alert System (1992)

In 1992 a fired Chevron employee hacked into the company's emergency alert network and reconfiguring them so they would crash. It was first discovered when an emergency arose at the Chevron refinery in Richmond, California. During the ten-hour period in 1992 when the system was down, thousands of people in twenty-two states and six unspecified areas of Canada were put at risk.[48]

46 Bill Miller and Dale C. Rowe, "A Survey of SCADA and Critical Infrastructure Incidents,"Brigham Young University Information Technology Program Provo, Utah, 2, http://sigite2012.sigite.org/wp-content/uploads/2012/08/session17-paper01.pdf.

47 Ibid., 2.

48 Ibid.

c. Gazprom (1999)

"In 1999, hackers broke into Gazprom, a gas company in Russia. The attack was collaborated with a Gazprom insider. The hackers were said to have used a Trojan horse to gain control of the central switchboard that controls gas flow in pipelines."[49]

d. Bellingham (1999)

In June 1999, after database development work on the SCADA system, 237,000 gallons of gasoline was leaked into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. The accident caused three deaths and eight documented injuries. "While the incident was an accident rather than an attack, the loss of human life illustrates the dangers of any kind of failure in a critical infrastructure system."[50]

e. Stuxnet (2010)

In June 2010, a worm named Stuxnet attacked the Iranian nuclear facility at Natanz. Stuxnet who used four 'zero-day vulnerabilities' and attacked drives were used to power centrifuges used in the concentration of the uranium-235 isotope. The worm accessed and altered Windows operating systems and frequency-converter drives. Stuxnet caused the centrifuges to switch between high and low speeds, making them useless.[51]

f. Night Dragon (2011)

In February 2011, 'Night Dragon' a combination of social engineering, Trojan horses and Windows-based exploits where used to attack five global energy and oil firms. The attacks were confirmed to have been

[49] Ibid., 2.

[50] ibid., 3.

[51] Ibid.

ongoing for over two years using Chinese tools and compromised Chinese computers, maybe in order to mask their identity.[52]

g. Shamoon (2012)

In August 2012, Saudi Arabia's Saudi Aramco and Qatar's RAS Gas, reported infection by a Trojan horse resulting in corruption of numerous workstations. Data was overwritten, lost and it was not possible to recover any data. "Due to the highly destructive functionality of the Shamoon "Wiper" module, organizations infected with the malware could experience operational impacts including loss of intellectual property and disruption of critical systems."[53]

A recent report from the Department of Homeland Security revealed that cyber criminals have targeted the oil and gas sector more than any other industry in the United States. "Over the six months leading to May 2013 there were 111 cyber incidents reported by the energy sector, accounting for 53% of all reported cyber attacks to industrial control systems."[54] Developing technology has made great strides forward, while protective measures have not received the same attention.

In the first half of fiscal year 2013, (October 1, 2012–May 2013), ICS-CERT responded to over 200 incidents across all critical infrastructure sectors.[55] The effect of an attack would be even greater if it were directed against several basic services in a society. While the examples of attacks on oil and gas had a serious impact, the attacks against Estonia in 2008 gave a warning of what is possible.

---

52 Ibid., 4.

53 U.S. Department of Energy, Technical Lessons Learned from the Shamoon Malware Attacks, CIP Awareness Bulletin – Joint Product October 2012, "Shamoon Malware Targets Oil and Natural Gas Critical Infrastructure Systems," http://www.nwppa.org/CWT/EXTERNAL/WCPAGES/WCMEDIA/DOCUMENTS/_NEWSLETTERS/CIP%20AWARENESS%20BULLETIN-SHAMOON%20TECHNICAL%20LESSONS%20LEARNED.PDF.

54 U.S. Department of Homeland Security, "ICS-CERT Monitor," 2, http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf.

55 Ibid., 2.

2. Attacks on a Nation State – Estonia

Since 2001, Estonia has been one of the countries in Europe with the most developed digital network. All the inhabitants have a digital ID-card. Estonia was the first country in the world to introduce election over the Internet for the local elections in 2005.[56]

On April 27, 2007, Estonian authorities decided to move the monument "Bronze Soldier" from the center of the capital Tallinn to a war cemetery on the outskirts of the city. The move was very unpopular with the Russian minority and with the Russian authorities. This resulted in extensive cyber attacks in the following months.[57]

The first cyber attacks were against Estonia's government and private Internet Service Providers (ISP). These attacks included Distributed Denial-of - Service (DDoS) attacks. The main targets were the websites of the Parliament, the President and the Prime Minister. Several news stations were also attacked. The first attacks were simple in their form, uncoordinated and easily averted.[58] The next attack consisted of millions of emails sent to Estonia's members of Parliament with the text "Congratulations on the Victory Day" and caused large numbers of errors and problems with mail servers. The result was that the government and other government institutions were without communication capabilities for several days. Some leading newspapers' websites were also attacked and closed from the outside. The attacks were more sophisticated than normal DDoS attacks; they were better coordinated and much more extensive.

The third attack targeted the President, Prime Minister, banks, political parties, major news agency, government, private Internet Service Providers and

56 eEstonia, The Digital Society, http://e-estonia.com/components/x-road.

57 Heather A. Conley and Theodore P. Gerber, "Soft Power in the 21st Century, an examination of Russian compatriot policy in Estonia," a report of the CSIS Europe program, August 2011, 1–7, http://csis.org/files/publication/110826_Conley_RussianSoftPower_Web.pdf.

58 Cooperative Cyber Defence Centre of Excellence, International Cyber Incidents, Tallinn, Estland 2010, 18, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf.

telephone companies vulnerable to DDoS attacks.[59] Sites and services were heavily affected with economic losses. Estonia was said to be very close to a digital collapse on May 10, 2007.[60]

The last major attack was a massive DDoS attack carried out by a bot network with 85,000 "zombie computers" against the Computer Emergency Response Team Estonia.[61]

It seems clear that most of the cyber attacks originated from Russian nationalist hacker groups.[62] Russian authorities had called for sanctions against Estonia and did little to stop riots outside the Estonian embassy. Russian authorities did not help the Estonian government in finding the responsible hackers and alleged perpetrators of the cyber attack. The fact that these attacks were well received in the Kremlin, however, does not mean that the government was behind them. The lack of follow-up afterwards speaks a clearer language, but proves little.

H. SUMMARY

Technological development, distribution and dependence of cyberspace allows almost anyone with an IP address to be a potential attacker or target, this means that the chance of being a target of an attack from botnet operators, criminal groups, hackers or nations is very high.

In conflict, the role of cyberspace is in constant change, more and more available technology challenges any cyber defense. Several nations are aggressively working to develop IW doctrine, programs, and capabilities in cyberspace since opportunities to inflict damage are significant for an attacker. Many actors have greater opportunity than ever before to direct cyber attacks

59 Ibid., 21.

60 Scott Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," Berkeley Journal of International Law nr. 27:1 2008, 205.

61 Cooperative Cyber Defence Centre of Excellence, International Cyber Incidents, 20.

62 David J. Smith, "How Russia Harnesses Cyberwarfare," 8–9, Defense Dossier, Issue 4, August 2012, http://www.afpc.org/files/august2012.pdf.

against critical infrastructure, while cyberspace cuts across boundaries between the civil and the military and between the public and the private.

Modern society is connected to many networks and some are particularly vulnerable to attacks. SCADA systems are an example of such especially vulnerable systems. Infrastructure attacks, either on specific individual targets or on larger targets as in the Estonian case, serve as a reminder of how advanced attacks might be. Just as important, however, is the recognition of the difficulty in tracking and revealing an attacker.

The most important recognition of cyberspace is the size, complexity and speed. This means that techniques, tactics and strategies in cyberspace will evolve, as we have seen it in the other domains: land, sea, air and space, but with a different speed. In cyberspace change will probably go even faster than in any other domain, and those who have developed holistic concepts are likely to dominate others. After the Second World War, the world was divided between the superpowers; it would not be inconceivable that it will be divided between those who have cyber power in the future.

III. CYBER POWER–THREATS OF STATES

A. BACKGROUND

Opinions differ over the definition of cyber power. In simple terms, it can be said as follows: "Cyber power is the capability to apply or project force in or through the cyber domain, a tool for both attack and defense."[63] This chapter aims to provide an understanding of what cyber power is. It provides a definition of cyber power, the role of cyber power in conflict, and how different scholars assess cyber power. A discussion of how deterrence might be conducted in cyberspace and how cyber deterrence can be an opportunity for Norway follows. The chapter concludes with an overview of how cyber operations can support other types of military operations.

B. WHAT IS CYBER POWER?

Daniel T. Kuehl defines cyberspace as "an operational space where humans and our organizations use the necessary technologies to act and create effects...In this sense it is no different from any of the other four physical domains—air, land, sea and outer space—in which we operate..."[64]

Kuehl claims that "the analogy among the domains of air-land-sea and outer space and cyberspace, and those same analogies hold true for a concept of cyber power as drawn from sea power or airpower."[65] According to Kuehl, this leads to the definition of cyber power as "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[66] Kuehl claims that cyber power is shaped by multiple

63 Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, Committee on Deterring Cyber attacks: Informing Strategies and Developing Options; National Research Council, (The National academics Press 2010), 57.

64 Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem" Ch. 2 in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 29.

65 Ibid., 37.

66 Ibid.

factors: first, technology, because the ability to "enter" cyberspace is what makes it possible to use it; and second, organizational mission, be it military, economic, or political.[67] Kuehl concludes, "All of these different factors shape how we employ cyber power to impact and influence the elements of power. Cyber power creates synergies across the other elements and instruments of power and connects them in ways that improve all of them."[68]

Another scholar who has defined cyber power is Joseph Nye, Jr. He argues that "cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain."[69]

Nye argues that there are two types of power shifts in this century. Historically the power has transitioned from one dominant state to another, but more recently the information revolution has changed the nature of power and increased its diffusion. With this he means that although the state will remain the dominant actor, it will face increased competition from non-state actors, which will make it more difficult for the state to control society.[70] The traditional concepts of international security and international relations may, therefore, change and new concepts must be developed. Nye also states that "cyber power can be used to produce preferred outcomes within cyberspace, or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace."[71]

From Joseph Nye's point of view, a concept of complex interdependence describes the world politics. From his perspective, cyberspace is not a neutral environment where everybody can act as if belonging to the same family. This idea leads to the perception that cyberspace is divided between the strong and the weak, the rich and the poor, the digital and the analog. With regard to

67 Ibid., 40.

68 Ibid.E

69 Joseph S. Nye Jr., Cyber Power, (Harvard Kennedy School, May 2010), 3.

70 Joseph S. Nye Jr., The Future of Power (New York: Public Affairs, 2011),113.

71 Ibid, 123.

security, this means that non-neutral cyberspace needs different kind of security both in a technological and in a social sense.[72]

Both Kuehl and Nye's definitions contain "the influence of others" with slightly different words. The possibility that cyber power creates cross-border synergies and improves other instruments of power makes it into a unique force multiplier, of interest for Norway. This means that a nation's ability to have success in, for example, conventional war, could increase if the nation has a well-developed cyber capability. Such a scenario opens up many considerations regarding the acquisition of cyber capabilities. While Kuehl and Nye both suggest that we need to think of cyber power in a new way where non-state actors play a bigger role, other scholars have a different view.

C. CYBER WAR–DIFFERENT VIEWS

Two other academic schools of thought regarding cyber power exist as suggested by Hans-Inge Langø in the paper, "Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security."[73] These are the revolutionists and traditionalists:

1. The Revolutionists

The first school of thought that Langø describes is the revolutionists.[74] Their thoughts about cyber power are, according to him, the oldest and go as far back as 1976 when Thomas P. Rona published the paper "Weapon Systems and

72 Jari Rantapelkonen & Harry Kantola, "Insights into Cyberspace, Cyber Security, and Cyberwar in the Nordic Countries" 32–33, in The Fog of Cyber Defence, ed. Jari Rantapelkonen & Mirva Salminen (Helsinki: National Defense University, 2013) http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf.

73 Hans-Inge Langø suggests three distinct approaches to cyber security and the question of strategic utility, these are: the Revolutionists, the Traditionalists, and the Environmentalists.

74 Hans-Inge Langø, "Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security" (Norwegian Institute of International Affairs, 2013), http://english.nupi.no/Publications/Working-Papers/2013/Slaying-Cyber-Dragons-Competing-Academic-Approaches-to-Cyber-Security.

Information War."[75] Although Rona focuses on military operations, Langø claims that this early work in the field helped to define cyber power and that some of the ideas presented are still relevant today.

These early thoughts on cyber power and cyber warfare were developed over time as technology became more accessible to the general public. John Arquilla and David Ronfeldt published "Cyber War Is Coming!" in 1993; in this work they asserted that wars would no longer be determined by who used the most capital, labor and technology on the battlefield, but who had the best information of the battlefield.[76]

The main claim by scholars with a revolutionist view is that they believe that new technology will change the very nature of warfare. Richard A. Clarke and Robert K. Knake in *Cyber War* make the same type of arguments regarding cyber war:[77] Cyber war is real, global and capable of occurring at the speed of light.

In response to these alarmist messages other academics are inherently skeptical of the potential of cyber power. Langø defines them as the traditionalists.

2. The Traditionalists

Langø underscores that the traditionalist thinkers do not reject that the technology has had an impact, but they are reluctant to throw away existing concepts, doctrines and policies prematurely.[78] One of the scholars that Langø defines as a traditionalist is Martin C. Libicki. In his early work, Libicki argues that the theoretical potential for cyber warfare exists, but it is unlikely at the present

75 Thomas P. Rona, "Weapon Systems and Information War" (Office of the Secretary of Defense, July 1, 1976).

76 John Arquilla and David Ronfeldt, "Cyberwar is Coming!,," 23.

77 Richard A. Clarke and Robert K. Knake, *Cyber War*, (Harper Collins Publisher: New York, 2010).

78 Hans-Inge Langø, "Slaying Cyber Dragons," 19.

time and in the immediate future.[79] Libicki's main argument is that the technology does not allow it, and there is a lack of empirical data that supports such warfare.

Many revolutionists argue that the entry cost of conducting cyber warfare is low compared to the other domains of warfare. A traditionalist response to this claim can be found in Dorothy E. Denning's work. She argues that while the cost of conducting cyber attacks, such as distributed denial-of-service (DDoS) attacks and webpage defacements, is low; the effects of these types of attacks are not equivalent to those of large-scale, costly military operations:

> The effects of cyber-attacks are relatively minor compared to what is achieved with armed forces, especially military operations that lead to the overthrow of governments, seizure of land, and human casualties. The discrepancy may narrow with more sophisticated cyber attacks that affect physical systems, but such attacks are likely to also have higher costs, raising the barriers to entry.[80]

Traditionalists acknowledge that technology has had a huge impact on society but that traditional instruments of national security are no less important. Instead of looking at cyberspace as a new way of warfare, they think it should be seen as a new tool in the state's toolbox for warfare.[81]

3. Assessments

Regardless of which school of thought they represent, the scholars have brought a great deal of clarity to the debate about cyber power. In short, revolutionists have shown the potential of cyber power; traditionalists have shown its limitations. Norway should recognize the potential of cyber power and that an effective national defense requires a combination of defensive and offensive capabilities.

---

79 Martin C. Libicki, "What Is Information Warfare?" (Washington, DC: National Defense University, 1995).

80 Dorothy E. Denning, "Barriers to Entry: Are They Lower for Cyber Warfare?," IO Journal 1, no. 1 (2009), 10.

81 Hans-Inge Langø, "Slaying Cyber Dragons," 26.

D. WHY KEEP CYBER CAPACITY?

Danish scientist Magnus Hjortedal argues that there are three reasons for states to maintain and utilize an aggressive cyber capability:

> To deter other states by infiltrating their critical infrastructure;
>
> To gain increased knowledge through espionage in cyberspace, which makes it possible for states to advance more quickly in their military development;
>
> To make economic gains where technological progress has been achieved—for example, through industrial espionage. This can be accomplished outside of official institutions.[82]

Hjortdal presents two primary effects of a nation's well-developed cyber capabilities: ability to deter and ability to conduct espionage. The capacity to carry out espionage for a variety of reasons and on different targets is an important manifestation of cyber power, which will be discussed in Chapter IV.

The following sections explain how cyber deterrence can be an effective tool that is not reserved for large nations.

1. Deterrence in Cyberspace

Denying benefits, imposing costs, and encouraging restraints to a potential attacker is the aim of deterrence. The U.S. Strategic Command defines deterrence as follows:

> "Deterrence seeks to convince adversaries not to take actions that threaten U.S. vital interests by means of decisive influence over their decision-making. Decisive influence is achieved by credibly threatening to deny benefits and/or impose costs, while encouraging restraint by convincing the actor that restraint will result in an acceptable outcome."[83]

---

82 Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," 3.

83 U.S. Joint Chiefs of Staff, Information Operations, Joint Publication 3-13, November 27, 2012, http://www.fas.org/irp/doddir/dod/jp3_13.pdf.

Adapted to cyberspace, deterrence seeks to prevent the potential threat of cyber attacks from states or groups by making the attacker realize that there is no chance of success or that the attacked nation has the ability to respond in a way that will be costly for the attacker. The assumption is that a state has the capability to threaten an opponent. One could deter a cyber attack by threatening some other action against the attacker. For non-state actors, the threat could be prison. For a state, it might be sanctions or a conventional military strike.

In analyzing deterrence of cyber attacks, Richard L. Kugler claims, "the goal of a cyber deterrence strategy would be to influence an adversary's decision-making calculus so decisively that it will not launch cyber attacks."[84] W. Earl Boebert mentions two factors that act to deter large scale disruptive cyber attacks from any source: "The first of these is the risk of an unintended consequence that the initiator, or allies of the initiator, are harmed by the attack." The second factor is: "a disruptive cyber attack is very unlikely to resemble a kinetic attack like a truck bomb."[85]

Boebert acknowledges uncertainty and the possibility that deterrence will not work unless it can be followed by kinetic methods. On the other hand, nations without military means may use the UN or international agreements to put pressure on an attacker. Diplomacy, bilateral agreements or membership in a union have an increasingly important role as an alternative or substitute for military power.

The development of the EU is one such example where military force has little or no role in relationships among nations. Conversely, economic agreements are very important and any threat of economic sanctions can have a huge impact. Another possibility is that the UN Security Council could take

84 Richard L. Kugler, "Deterrence of Cyber Attacks," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (Washington, DC: National Defense University Press 2009): 327.

85 W. Earl Boebert, "A Survey of Challenges in Attribution," in Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, Committee on Deterring Cyber attacks: Informing Strategies and Developing Options; National Research Council, (The National academics Press 2010), 50.

measures against an aggressive state under Article 39, assuming the aggressive action crossed the threshold for a response. A nation's cyber deterrence strategy may rest on such sanctions. This might be just as effective as threats of a military response. Another way might be to consistently pursue all cyber attackers and take them to court. For a country like Norway, both options should be considered. Norway is already a member of multiple international forums; Norway provides substantial sums to both EU countries and other nations. These are key areas that can back up future cyber deterrence. Prosecuting cyber attacks from non-state actors is probably an action the Norwegian government can take. A prerequisite is cooperation with other governments so that they can investigate, identify and arrest the attackers. In this way, the work of different scholars can be operationalized and may be developed to fit a small nation's cyber strategy.

E. CYBER ATTACK IN SUPPORT OF MILITARY OPERATIONS

Cyber attacks can support a variety of operations within the information operations sphere and also other military operations. In addition, cyber attacks can also be applied to missions that are not traditionally within the military domain.

1. Active Defense in Response to Adversary Probes/Attacks

Cyber attacks could be used defensively to eliminate a threat to government systems or networks. Active cyber defense (ACD) is a term that describes a wide range of proactive actions that engage the adversary before and during a cyber incident. ACD can dramatically improve efforts to prevent, detect and respond to sophisticated attacks.[86]

86 Center for a New American Security, Policy Brief, Active Cyber Defense, A Framework for Policymakers, February 2013, 1,http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf (accessed November 5, 2013).

2. Support for Information Operations

a. Psychological Operations

Key enemy personnel can be targeted in a cyber campaign by emails or telephone calls asking them to surrender or to escape. Another PSYOPS application might call for the launch of a small, but very visible cyber attack and then the announcement of the attack to an adversary in order to undermine confidence in their essential systems.[87]

b. Operations Security

Cyber attacks directed at systems for command and control, including specific adversary sensor systems that are intended to report on information related to the location of friendly forces will degrade operations security.[88]

c. Military Deception

Cyber attacks could be used to gain access to an adversary computer systems for identification, by assuming control of a computer used by a senior intelligence analyst, bogus email traffic or communications could be sent to that analyst's customers.[89] In this way, the enemy is given a wrong image of military build-up or maneuver.

d. Electronic Warfare (EW)

Cyber attacks could be used to disable an adversary's software-defined radios, thus preventing enemy wireless battlefield communications. In addition, EW could support cyber attacks.[90]

---

87 William A. Owens, Kenneth W. Dam, and Herbert S. Lin (eds.), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, (National Research Council, The National Academies Press 2009): 177.

88 Ibid., 177.

89 Ibid., 178.

90 Ibid.E

e. Support of Traditional Military Operations

Cyber attacks could also be used in connection with a variety of traditional military operations. Some examples are:

- Disruption of adversary command, control, and communications
- Suppression of adversary air defenses
- Degradation of adversary smart munitions and platforms
- Attacking adversary war fighting- or war making infrastructure[91]

f. Support to Nonmilitary Operations

Cyber attacks can support a variety of other operations as well, though these are not in the category of what are traditionally undertaken by military forces.[92] This may be cyber attack against the economic base of organized crime or some intelligence operations.

g. Covert Operations

Classic examples of covert action include providing weapons or funding to a favored party in a conflict, supporting agents to influence political affairs in another nation, engaging in psychological warfare, disseminating disinformation about a disfavored party, or deceiving a disfavored party. Specific actions that could be undertaken under the rubric of covert action include: Intelligence collection and disseminating of propaganda in order to create tensions between adversaries or groups. Other possibilities are to attack the economic system, creating fear in the population or disrupt vital infrastructure.93

These examples show how operations in cyberspace can support virtually any conceivable military operation. It is a reminder to the nations that have built a defensive doctrine; it will require significant resources to protect

---

[91] Ibid., 179–180.

[92] Ibid., 181.

[93] Ibid., 193–194.

against all these threats. It is also an important reminder that cyber power is created when a nation has some offensive capabilities and is willing to use it.

F. SUMMARY

This chapter started by asking whether cyberspace has opened up a new channel in which states can project power. The discussion has shown that there are many opinions about cyber power and what it represents. Kuehl and Nye offer views of cyber power that could provide a basis for a strategy that may be suitable for Norway's cyber defense. The premise is that one accepts the role of how power is distributed in cyberspace, and that there is no distinction between war and peace in cyberspace since states and individuals are constantly pursuing their own interests. Faced with this reality, Norway should, on the one hand, seek cooperation and, on the other hand, realize that offensive cyber capabilities are a complement to defensive capabilities.

The next key question was whether cyber power could deter another state. This research indicates that cyber power definitely has the power to hurt another state; however, cyber power has its clear limits in comparison to military power, and any cyber deterrence must be supported by diplomatic means. Based on that assumption, cyber deterrence cannot have a "stand-alone" strategic effect, but it will work best as an amplifier.

Cyber operations can support military operations in a variety of ways. For small countries, it is possible that the perception around warfare means that, by default, resources must concentrate on defense. This may explain why many nations seem to lack strategies for offensive operations in cyberspace. Others, however, have manifested a reputation as notorious cyber warriors. China is emerging as a nation with a very well-developed cyber capability, both defensively and offensively. China is thus helping to set the standard for future cyber powers.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CHINA'S CAPABILITIES IN CYBERSPACE

A. BACKGROUND

The 2013 annual report to the U.S. Congress on Military and Security Developments Involving the People's Republic of China states: "The People's Republic of China (PRC) continues to pursue a long-term, comprehensive military modernization program designed to improve the capacity of its armed forces to fight and win short- duration, high-intensity regional military conflict."[94]

This chapter describes how China has built up a significant capacity in cyberspace. It illustrates how a government can plan for cyber war, develop capabilities and use cyberspace as an arena of influence. China is an important example, because Chinese doctrine and technology will emerge as attractive for other nations with cyber ambitions. Insights into China's capabilities in cyberspace can provide an indication of how other nations are likely to develop their own capacities. It should also be noted that the U.S. has a significant cyber capacity and U.S. Cyber Command is probably the largest of its kind. However, the focus here is on China, as its capabilities and intentions are more relevant to Norwegian challenges.

Developing cyber capabilities for warfare is consistent with authoritative People's Liberation Army (PLA) military writings. Cyber warfare capabilities could serve the PRC's military operations in three key areas:

> First and foremost, they allow data collection through ex-filtration.
>
> Second, they can be employed to constrain an adversary's actions or slow response time by targeting network-based logistics, communications, and commercial activities.

94 U.S. Department of Defense, Annual Report To Congress, "Military and Security Developments Involving the People's Republic of China 2013," Executive Summary, i, http://www.defense.gov/pubs/2013_china_report_final.pdf.

> Third, they can serve as a force multiplier when coupled with military and security developments involving kinetic attacks by the People's Republic of China during times of crisis or conflict.[95]

In 2012, numerous computer systems around the world continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military. These intrusions were focused on exfiltrating information.[96] A Chinese military hacker group connected to the government is believed to be behind cyber attacks against sensitive targets in Norway. The Norwegian National Security Authority (NSM) said Norwegian companies have probably lost contracts because of computer espionage. According to NSM, at least 20 serious cyber attacks can be traced back to China.[97] The relationship between Norway and China has been at a low point since the Nobel Peace Prize was awarded to a Chinese dissident in 2010.[98]

B. THE ROLE OF THE PEOPLE'S LIBERATION ARMY

The PLA is the overall military organization of all land, sea and air forces of the People's Republic of China. The Army was created on August 1, 1927 as the military part of the Chinese Communist Party. The PLA now consists of a multidimensional force structure capable of conducting military operations across a realm incorporating land, sea, air, space, and finally, cyberspace.[99]

The PLA has several distinct entities that operate in the cyber domain, including elements of the headquarters staff and potentially each military branch, some combination of which would execute cyber attacks during wartime. Several

---

95 Ibid., 36.

96 Ibid., 36.

97 The Nordic Page, "China is Behind more than 20 Serious Cyber Attacks against Norway," http://www.tnp.no/norway/politics/3580-china-is-behind-more-than-20-serious-cyber-attacks-against-norway.

98 The Official website of the Nobel Prize, The Nobel Peace Prize 2010, Liu Xiaobo, "Liu Xiaobo–Facts," http://www.nobelprize.org/nobel_prizes/peace/laureates/2010/xiaobo-facts.html.

99 Paul H.B. Godwin, "PLA Doctrine and Strategy: Mutual Apprehension in Sino-American Military Planning," in *The People's Liberation Army and China in Transition*, Institute for National Strategic Studies National Defense University, August 2003, 272–273, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA430961.

entities within China's intelligence and security services also have a cyber espionage mandate. Nominally independent groups may engage in state-sponsored exploitation, and certain corporate actors, such as Chinese information technology or telecommunications firms, may also operate in cyberspace on the state's behalf.[100] The following sections, describe the PLA and China's cyber capabilities.

1. China's Cyber Strategy

The PLA is investing heavily in the development of IW capabilities, especially in the areas of electronics and cyber warfare. It has established IW units and is also able to harness extensive civilian resources to conduct cyber-warfare operations, even during peacetime.[101]

PLA campaign doctrine identifies the necessity of early establishment of information dominance over an enemy as one of the highest operational priorities in a conflict.[102] For this purpose, China possesses sophisticated cyber capabilities and has demonstrated a striking level of perseverance, evidenced by the sheer number of attacks and acts of espionage that the country commits. Since cyber warfare is not directly addressed in unclassified Chinese government documents, it is useful to explore the PLA's approach to information warfare (IW).[103]

---

100 U.S.- China Economic and Security Review Commission, 2012 Report to Congress of the U.S.-China economic and Security Review Commission, "Executive Summary and Recommendations," November 2012, 11, http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress-Executive%20Summary.pdf.

101 Tai Ming Cheung, "Dragon on the Horizon: China's Defense Industrial Renaissance,," published online February 25, 2009, 34.http://www.tandfonline.com/doi/abs/10.1080/01402390802407418#.Uombo5FEhyg.

102 Bryan Krekel, Patton Adams, and George Bakos, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,," Prepared for The US-China Economic and Security Review Commission, Northrup Grumman Corp, October 9, 2009, 6–8.

103 Julia Yrani and William Handel, "Cyberwar and the Deterrence Calculus, Assessing a U.S.-China Balance in the Digital Realm 2012,," 12. http://www.scribd.com/doc/137608606/Cyberwar-and-the-Deterrence-Calculus-Assessing-a-U-S-China-Balance-in-the-Digital-Realm.

a. Information Confrontation Framework

Information is seen as a strategic resource, and the side that is best informed will win. Krekel, Adams and Bakos argue, "Authoritative PLA writings on computer network operations typically focus on issues such as the dominating the seizure of information during a campaign, shaping adversary perceptions for maximum strategic impact, operating or training under informationized conditions, or strengthening the PLA's network defenses."[104] China's aggressive collection efforts appear to be intended to amass data that will support the country's economic growth, scientific and technological capacities and military power. Their collection effort aims to secure China's strategic advantage in relation to competitor countries and adversaries well before any form of hostility has broken out. China is seeking a position where they simply have information superiority, an advantage that is reinforced by the fact that PLA has both a doctrine and a concept of operations.

b. Cyber Integrated into People's War Concept

A holistic approach to information superiority within the PLA leadership encompasses more than just operational active duty units. The priorities have resulted in transforming the PLA's traditional forms of mobilization and civil-military integration. It is named "People's War in a New Era." Consequently, the modernization of the militia and reserve forces is largely focused on recruiting new members with skills in essential high technology areas, in part to form new units but also to help transform existing militia or reserve units by incorporating recruits with advanced education and technical skills in mission critical areas.[105]

---

[104] Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Report prepared for the U.S.- China Economic and Security Review Commission by Northrop Grumman Corp, March 7, 2012, 25, http://www.uscc.gov/RFP/2012/USCC%20 http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

[105] Ibid., 51–52.

c. Cyber Operations Seen as Low-Cost Asymmetric Method

The Chinese main doctrine on cyber war strategy advocates for a combination of cyber and electronic warfare capabilities in the early stages of conflict to paralyze enemy control and command and intelligence centers. The PLA's view is that a highly developed IW capability can act as an asymmetric tool to neutralize the military capabilities of a technologically superior opponent.[106] Another interesting take on the use of cyber operations is the ability to settle a controversy without physically attacking the opponent. An important realization is that deterrence and offense can be conducted simultaneously in IW, staging an attack in an effort to induce the adversary to expend valuable resources during a crisis on difficult issues of determining attribution. It can be assumed that tactics used in coordination with other assets can contribute to a PLA bloodless victory using largely IW based tools.[107]

d. Espionage Considered Acceptable

China's cyber operations in support of espionage operations has opened a source of previously inaccessible information that can be mined both in support of national security concerns and, more significantly, for national economic development. Cyber operations has in many ways replaced human intelligence (HUMINT), the spy is digital.[108] China is believed to be one of the most aggressive actors in the world of cyber-espionage and is regularly accused of stealing industrial and technological secrets.[109] Parts of this "success" can be attributed to an overall strategy but also as importantly to central management.

---

[106] Julia Yrani and William Handel, "Cyberwar and the Deterrence Calculus," 13–14.

[107] Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 29.

[108] Ibid., 107.

[109] Mandiant, "APT1 Exposing One of China's Cyber Espionage Units,," 2, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

C. THE ROLE OF PLA GENERAL STAFF

The Chinese have adopted a formal IW strategy called "Integrated Network Electronic Warfare" (INEW), which consolidates the offensive mission for both computer network attack (CNA) and EW under PLA General Staff Department's (GSD) 4th Department (Electronic Countermeasures). The computer network defense (CND) and intelligence gathering responsibilities likely belong to the GSD 3rd Department (Signals Intelligence), and possibly to a variety of the PLA's specialized IW militia units.[110] An overview of the PLA military organization's structure is shown in Figure 2.

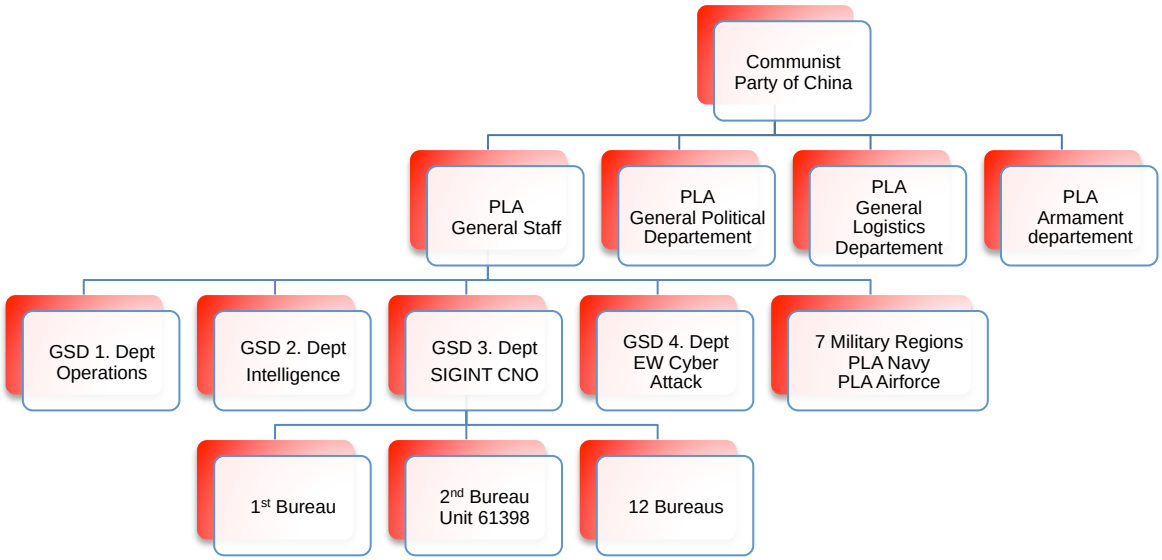

Figure 2. PLA military organization.[111]

[110] Bryan Krekel, Patton Adams, and George Bakos, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Prepared for The US-China Economic and Security Review Commission, (Northrup Grumman, October 9, 2009), 6-–8.

[111] Mandiant, APT 1 Report and Dorothy E. Denning, NPS class August 19, 2013.

Exercise and training in cyber operations occurs across all PLA service branches and is considered a core competence of all combat units. Field exercises include joint operations in "complex electromagnetic environments," and sources indicate the existence of a permanent "Blue Force" regiment, drilled in foreign IW tactics. Actions that confirm comprehensive planning, training and execution are only possible in an organization where responsibility and powers are clearly defined.[112]

a. PLA and Hackers

Government efforts to recruit and support individuals among the Chinese hacker community and evidence of consulting relationships between known elite freelance hackers and security services indicate some government willingness to draw from this pool of expertise and talent.[113]

According to an uncorroborated Taiwan media source referencing an article from a Sichuan University student newspaper, the PLA in 2005 reportedly held a series of regional or provincial hacker competitions to identify talented civilians who could support military cyber operations requirements.[114]

Another group of hackers are the "hacktivists," occasionally called ''patriotic hackers,'' who appear to act primarily on the basis of nationalistic sentiments, often engaging in Distributed Denial of Service/Denial of Service attacks or website defacements. Hacktivists often target decision-makers directly to express their dissatisfaction with various policies.[115]

---

112 Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," 11.

113 Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 34, 37, 97.

114 Bryan Krekel, Patton Adams, and George Bakos, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," 45–48.

115 Irving Lachow, "Cyber Terrorism: Menace or Myth" Ch 19 in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 439.

b. PLA's Sponsorship of Universities

It is a well-developed cooperation between government, military and commercial companies across the country, these technical programs, research, curricula and financial support helps to develop IW capabilities. The network of institutions and scholars funded to conduct research on IW techniques and technologies suggesting a continuing expansion of high-tech separate communities into niche areas of the national economy, such as finance, education, and law.[116]

2. Expenditure

In March 5, 2013, Beijing announced a 10.7 percent increase in its annual military budget to $114 billion, continuing more than two decades of sustained increases in annual defense spending. Estimating China's Actual Military Expenditures using 2012 prices and exchange rates, the DoD estimates that China's total actual military-related expenditure for 2012 falls between $135 billion and $215 billion.[117]

How much goes to the cyber is uncertain, and the numbers are not public. Defense Tech analyst Kevin Coleman estimated in 2008 that China spent $55 million on its cyber budget.[118]

3. Cyber Attacks and Espionage from China

China's desire for status has meant that they may have the most extensive and aggressive cyber warfare capability in the world. "Authoritative Chinese writings on the subject presented cyber warfare as an obvious asymmetric instrument for balancing overwhelming power, especially in case of

116 Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 58–59.

117 U.S. Department of Defense, Annual Report To Congress, "Military and Security Developments Involving the People's Republic of China 2013," 45, http://www.defense.gov/pubs/2013_china_report_final.pdf.

118 Kevin Coleman, "China's Cyber Forces," Defense Tech 2008, http://defensetech.org/2008/05/08/chinas-cyber-forces/.

open conflict, but also as a deterrent."[119] In contemporary Chinese thinking, IW is seen as a preemptive tool on equal basis with other combat arms. Doctrinal and strategic writings underline the importance of seizing information dominance at an early stage and thereby exploiting the use of IW tools for their potential deterrent effect.[120]

4. Cyber Operations Conducted by the PLA

China's development of its computer network operations capability extends beyond preparations for wartime operations. The PLA and state security organizations have begun employing this capability to mount a large-scale computer network exploitation effort for intelligence gathering purposes against the U.S. and many other countries around the world, according to statements by U.S. officials, accusations by targeted foreign governments, and a growing body of media reporting on these incidents.[121] The following two examples show both the scope and the objectives.

a. Titan Rain

In 2003, Department of Defense (DoD) and DoD contractor computers were attacked with aim to copy sensitive data files. The cyber espionage attack apparently went undetected for many months. The cyber espionage attacks apparently went undetected for many months. DoD suspected that this series of cyber attacks, later labeled Titan Rain, originated in China. Although no classified systems were breached, many files containing sensitive

119 Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," 6–7.

120 Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," 8, 29.

121 Bryan Krekel, Patton Adams, and George Bakos, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," 51.

information were copied.[122] In the case of Titan Rain, Chinese sources were estimated to have exfiltrated somewhere close to 10 terabits of data.[123]

b. APT 1

APT 1 is believed to be the Second Bureau of the People's Liberation Army General Staff Department's (GSD) Third Department, which is most commonly known by its Military unit Cover Designator (MuCD) as Unit 61398. The nature of Unit 61398's work is considered by China to be a state secret; however, the unit is believed to engage in cyber exploitation. Based on the size of Unit 61396's physical infrastructure, the staff is estimated to be hundreds, perhaps thousands, of people. APT 1 has systematically stolen hundreds of terabytes of data from at least 141 organizations and has demonstrated the capability and intent to steal from dozens of organizations simultaneously, including one victim in Norway.[124]

D. SUMMARY

Chinese leaders have shown foresight with regards to priorities, focus, and a desire to exploit new technology. China has a well-developed strategy combined with cyber resources across the government, including civilian IT companies and universities. China has had huge economic growth, and its budget reflects the overall growth in the state economy. Cyber power is a priority and the country's armed forces have a major role. Technology and development are other priority areas where the government supports an extensive espionage program in cyberspace. PLA appears to be a trendsetter in terms of how a government can organize its activities in cyberspace. In recent years, China has

122 Clay Wilson, "Cyber Crime," Ch 18 in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 424.

123 Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," Ch 3 in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), 85.

124 Mandiant, "APT1 Exposing One of China's Cyber Espionage Units," 3, 22, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

executed numerous advanced and effective cyber espionage programs. With ATP 1, China demonstrated its ability to exploit weaknesses in cyber defenses, thereby collecting large amounts of intelligence.

A nation that focuses on cyber weapons can thereby achieve deterrence in the cyber domain. Simply put, if any country challenges China in cyberspace, it must be prepared that China will strike back with great force.

THIS PAGE INTENTIONALLY LEFT BLANK

V. NORWEGIAN CYBER DEFENSES

A. INTRODUCTION

This chapter provides an understanding of how Norwegian cyber defenses are organized and their strategies and compares them to Finnish cyber security strategy. In many ways Finland is similar to Norway, especially in relation to resources and technology; however, Finland has developed a very ambitious cyber strategy, which can be seen as an innovative model.

Cyberspace is increasingly important for Norway and Finland. The Global Information Technology Report from 2012[125] confirms that the Nordic countries and the Asian economies are well ahead in adapting and implementing information and communication technology. Sweden ranked first on the worldwide Networked Readiness Index (NRI). Finland was third followed by Denmark as fourth, and Norway achieved the seventh place putting the four Nordic countries into the top ten on the NRI.[126]

Many states and organizations have begun to put money and research into their cyber security programs. Cyber weapons have become important tools of modern warfare. The attack on a cyber infrastructure as in Estonia has shown that cyberspace can be used to affect any nation. An important challenge for any cyber defense is the rapid changes in technologies, making it difficult for any state or organization to manage all developments in a timely manner. Attacks continue to affect operating systems, applications, communications protocols and networks.

125 World Economic Forum, The Global Information Technology Report 2012, "Living in a Hyperconnected World," 9, http://www3.weforum.org/docs/Global_IT_Report_2012.pdf.

126 Ibid., 12.

B. NORWEGIAN DEFENSE AND SECURITY THINKING

The experience gained by the swift Nazi occupation of Norway during WW2 led to a desire to form a total defense in 1946. The defense system included the nation's total resources, both military combat power and civil preparedness. The aim of this approach was two secure Norway's territory, independence and national values, and to safeguard the population. The concept responded to a need for ensuring a comprehensive effort by all sectors in the society in times of crisis and for avoiding unnecessary duplication of effort in such a small nation as Norway.[127]

Some nations have an organization that maintains cyber defense, and in countries such as the UK and France, cross-government institutions, like the cabinet office, are often preferred for coordinating cyber defense. In Norway, one of the challenges was the question of where to place responsibilities for cyber defense, as cyber threats by nature cut across different sectors. The organization of the government, as well as the formerly mentioned principle of responsibility, imply that all Ministers are responsible for their own sector – also in the realm of cyber defense.[128] This approach differs greatly from the one selected in China, where responsibilities and priorities seem much better coordinated. Although there are great differences between China and Norway, the challenges in relation to cyber defense are not so different.

C. CYBER SECURITY IN A SMALL COUNTRY

In relation to organizing a cyber defense, there is little point in comparing Norway with larger nations; however, Finland can provide a meaningful comparison. Finland has for many years been a leading country in telecommunications because of the presence of Nokia and has very ambitious

127 Kristin Hemmer Mørkestøl, "Norwegian Cyber Security: How to Build a Resilient Cyber Society in a Small Nation," in The Fog of Cyber Defence, ed. Jari Rantapelkonen & Mirva Salminen (Helsinki: National Defence University, 2013), 109.

128 Ibid., 112.

aspirations for its cyber defenses:[129] "Finland has high ambitions in terms of cyber security with the goal to become the leading country in this area by 2016.

Some of the principles in the national approach for Finland's cyber security management:

> The approach for the implementation of cyber security is based on efficient and wide-ranging information-collection, an analysis and gathering system as well as common and shared situation awareness, and national and international cooperation in preparedness. To succeed in this approach, the establishment of a Cyber Security Centre as well as the development of 24/7 information security arrangements for the entire society was required.
>
> Cyber security arrangements follow the division of duties between the authorities, businesses and organizations, in accordance with statutes and agreed cooperation. Rapid adaptability as well as the ability to seize new opportunities and react to unexpected situations demand strategic agility awareness and compliance from the actors as they keep developing and managing the measures, which are aimed at achieving cyber security.
>
> Cyber security is being constructed to meet its functional and technical requirements. In addition to national action, inputs are being made into international cooperation as well as participation in international R&D and exercises. The implementation of cyber security R&D and education at different levels does not only strengthen national expertise, but it also bolsters Finland as an information society.[130]

Finland's "level of readiness is first rate thanks to its world-class educational system, relatively inexpensive technologies, and excellent infrastructure."[131] The vision (of becoming leading country in the world by 2016) may sound optimistic, but the authors of the national document believe that Finland has a good chance of reaching the goal. Since WW2, security,

---

[129] Finland's Cyber Strategy, Government Resolution 24th of January 2013, 3, http://www.defmin.fi/en/publications/strategy_documents/finland_s_cyber_security_strategy.

[130] Ibid., 5.

[131] Jari Rantapelkonen & Harry Kantola, "Insights into Cyberspace, Cyber Security, and Cyberwar in the Nordic Countries," 29.

preparedness and self-sufficiency have been an important part of Finnish strategic priorities and national self-image.[132] Thus, it is not surprising that Finland has the same ambitions in cyber security. Among the many innovative ideas in this document, four areas of interest should be emphasized:

- Shared Situation Awareness
- Establishment of the Cyber Security Centre
- Strategic Agility
- Participation in International R & D and Exercises

These four areas could provide important improvements within the cyber defense of Norway if implemented; the challenge would be adapting the Norwegian model to such initiatives.

D. NORWEGIAN CYBER SECURITY STRATEGY

A number of documents describe the Norwegian cyber defense strategy and the types of threats that are considered serious. The recently released "*Strategy, Cyber Security Strategy for Norway"* (December 2012) provides background, status and plans. The document describes how information and communications technology (ICT) has caused major changes to society over the past decades. Technology is the foundation for all interaction across the society, making ICT a strategic security challenge. An increased use of ICT has made society more vulnerable. Threats to ICT systems are on the rise, and attacks are increasingly more sophisticated. Therefore, good preventive information security is increasingly important for national security. Information security means that information is protected against unauthorized access, that it is available when needed, and that it is protected against unauthorized changes.[133] Considerable

132 Anssi Kärkkäinen, "The Origins and the Future of Cyber Security in the Finnish Defence Forces," The Fog of Cyber Defence, ed. Jari Rantapelkonen & Mirva Salminen (Helsinki: National Defence University, 2013), 101.

133 The Ministry of Government Administration, Reform and Church Affairs [FAD] , "Cyber Security Strategy for Norway," December 17, 2012, 8, http://www.regjeringen.no/en/dep/fad/documents/Reports-and-plans/Plans/2012/cyber-security-strategy-for-norway.html?id=710469.

focus on information security and protection against unauthorized access might seem to be a narrow basis for a comprehensive approach to cyber security.

The strategy document describes the threats as follows:

> Espionage and sabotage - a growing threat. The tendency to be targeted by professional hacking against critical ICT systems is increasing. Targeted espionage attacks against the vital national security interests now constitute a significant challenge. Civilian agencies, military units and private companies are subject to espionage and sabotage. Many states are developing the ability to conduct intelligence and warfare against critical infrastructure. It must be noted that sophisticated tamper and impact attacks will be directed at socially critical information resources, including computer systems that control industrial processes and critical infrastructure.[134]

In another government document, a chart shows the number of ICT events in the period 2007–2011. These are cases that are handled by NSM Department, Norwegian Computer Emergency Response Team (NorCERT). More and more ICT events have been recorded in Norway, and the number of cases has tripled from 2007 to 2011.

[134] Ibid., 12.

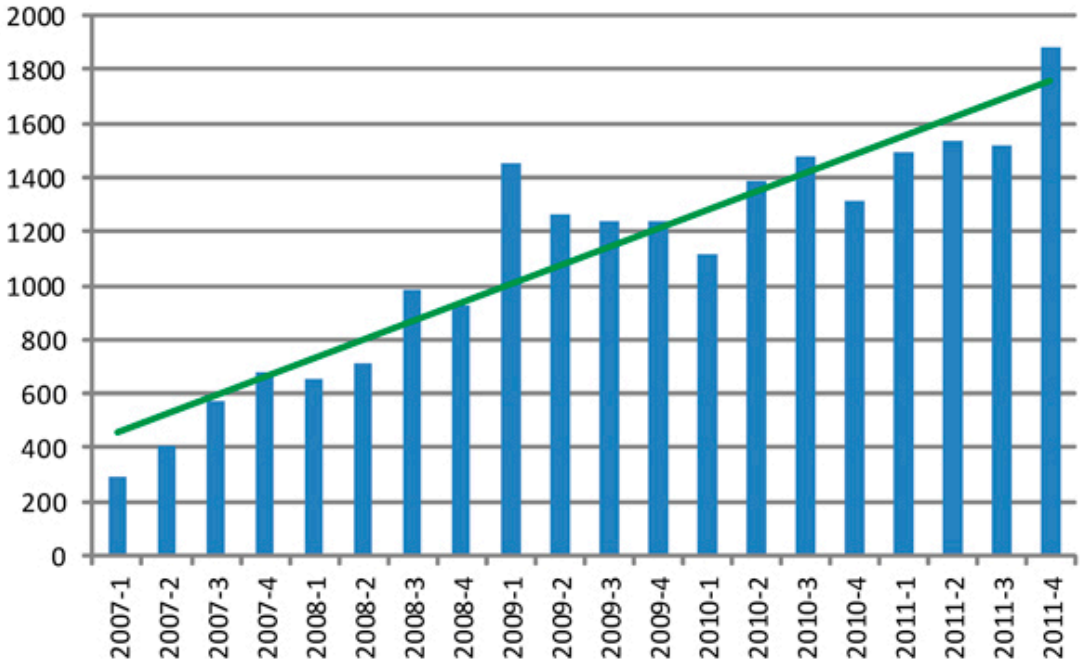

Figure 3. Number of handled ICT events.[135]

A more specific description of a possible threat is described in the Norwegian Intelligence Service' (NIS) annual unclassified threat assessment. NIS writes that the Chinese authorities are overusing digital operations to a large degree as a replacement for human collection and often use proxies for obtaining information. Educational institutions, firms, organizations and hacker circles provide a good cover for the activity.[136] This is an observation that matches well with the reality, as described in detail in Chapter IV.

A preliminary conclusion is that the strategy document is very accurate in describing the threat, but measures can be seen as defensive and not very ambitious. The document makes no introduction to the concept of the cyber

135 Justis- og Beredskapsdepartementet [Norwegian Ministry of Justice and Public Security], Meld. St. 29 (2011–2012) Samfunnssikkerhet [The Ministry of Justice and Public Security: Civil protection, White paper no. 29 (2011–2012)], 103, http://www.regjeringen.no/pages/37919076/PDFS/STM201120120029000DDDPDFS.pdf.

136 Norwegian Intelligence Service, FOCUS 2013, 44–45.

domain, an important component to create an understanding of the complexity and a comprehensive approach.

E. NORWEGIAN CYBER DEFENSE ORGANIZATIONS

1. Departmental Responsibilities

The Ministry of Justice and Public Security is responsible for coordinating civilian security. The Ministry acts as initiator and coordinator with respect to other sectoral authorities.

The Ministry of Government Administration, Reform and Church Affairs is responsible for coordinating government ICT policy. The Ministry has specific responsibility for promoting a stronger and more comprehensive approach to information security in the public administration. The Ministry is also responsible for improving coordination of work on information security by agencies and for contributing to coordinated solutions.

The Ministry of Transport and Communications is, by virtue of its responsibility for the Norwegian Post and Telecommunications Authority, responsible for ICT security related to electronic communication networks and services.

The Ministry of Defense is responsible for cyber security in the military sector, including preventive measures. The Ministry of Defense has management responsibility for the Norwegian National Security Authority (NSM) and administrative responsibility for the National Security Act.

The defense sector comprises the Ministry of Defense and all subordinate agencies: the Armed Forces, the Norwegian Defense Estates Agency, the Norwegian Defense Research Establishment (FFI) and the Norwegian National Security Authority (NSM).[137]

137 Norwegian Ministry of Government Administration, Reform and Church Affairs [FAD], Meld. St. 23 (2012–2013) Digital Agenda for Norge, IKT for vekst og verdiskaping, [Ministry of Government Administration, Reform and Church Affairs: Digital Agenda for Norway, ICT for Growth and Value, White paper no. 23 (2012–2013)], 105–106. http://www.regjeringen.no/pages/38354256/PDFS/STM201220130023000EN_PDFS.pdf.

2. Organizations and Responsibilities

Despite the fact that Norway is a small country with limited resources, a number of organizations are responsible for cyber security. The following agencies have a responsibility to protect Norway against cyber threats:

a. The Norwegian National Security Authority (NSM)

NSM is the central directorate for the protection of information and infrastructure crucial for critical societal functions. It protects information, information systems and other assets against espionage, sabotage, and terrorism through inspections in accordance with the Security Act; it develops security initiatives, provides advice and guidance, and detects and manages countermeasures for serious cyber attacks (see NorCERT later in this chapter). It is the driving force for improving security conditions.[138]

The Norwegian National Security Authority (NSM) is the executive body for preventive security in the civil and military sectors on behalf of the Ministry of Justice and the Police and the Ministry of Defense. The NSM counters threats to the independence and security of the realm and other vital national security interests, primarily espionage, sabotage or acts of terrorism. The NSM is a directorate that is administratively subordinated to the Ministry of Defense.[139]

b. NorCERT

NorCERT, a department under the NSM, is the national center for notification and countermeasure coordination for serious cyber attacks and other ICT security incidents targeting important ICT infrastructure for critical societal functions.[140] NorCERT is Norway's national center for issuing alerts on and

138 FAD, "Cyber Security Strategy for Norway," December 17, 2012, 31.

139 Forsvarsdepartementet [Norwegian Ministry of Defence], Meld. St. 14 (2012–2013) Kompetanse for en ny tid [The Ministry of Defence: Competence for a new era, White paper no. 14 (2012–2013)], 12, http://www.regjeringen.no/pages/38247066/PDFS/STM201220130014000DDDPDFS.pdf (accessed September 13, 2012).

140 FAD, "Cyber Security Strategy for Norway," December 17, 2012, 30.

coordinating responses to serious cyber attacks. The Norwegian Alert and Early Warning System for Digital Infrastructure gives authorities capabilities to verify and issue alerts on serious and coordinated attacks on critical ICT infrastructure. NorCERT participates in the Nordic CERT (Computer Emergency Response Team) partnership and cooperates closely with counterparts in other countries.

c. The Norwegian Post and Telecommunications Authority (PT)

PT monitors companies providing electronic communications services, electronic communications networks and postal services, and issuers of official eSignature certificates. PT contributes to secure and robust networks and services.[141]

d. The Norwegian Centre for Information Security (NorSIS)

NorSIS is a resource center created through an initiative by the Ministry of Government Administration, Reform and Church Affairs The center offers consultancy services for information security for all Norwegian private and public entities. All levels of society can take advantage of these services. NorSIS also runs the website deleteme.no (slettmeg.no), which gives advice to those who feel offended online.[142]

e. Norwegian Directorate for Civil Protection (DSB)

DSB is the driver, advisor and coordinator for preventive and crisis measures nationally, regionally and locally. It has the capacity to supply aid to support higher authorities and all other authorities in the event of major emergencies or when needed.[143]

141 Ibid., 30.

142 Ibid., 30.

143 Ibid.

f. The Norwegian Data Protection Authority (DT)

DT oversees a number of laws and regulations, where information security is an important part of the regulation. The overall regulatory framework affects much of the public and private sectors. DT has developed a number of guidelines on information security and provides guidance on compliance with legislated requirements.[144]

g. Kripos (National Criminal Investigation Service)

The main objective of Kripos is to combat organized and other serious crime.[145] Kripos is about to change its organizational structure to meet the challenges it faces with an increased focus on cyber. The new department, "Technology and Operational Services" provides analysis, technology and research support, including evidence recovery, method development and assistance to the Norwegian police.[146]

In selected areas, Kripos will be the main provider of services and act as a center of expertise in subjects and methods. It also serves as the international contact point and the forensic laboratory.[147]

h. Norwegian Intelligence Service (NIS)

NIS is responsible for detecting and analyzing external threats to Norway. The objective of intelligence activities is to contribute to counteract threats and to provide Norwegian authorities with a solid basis for foreign, security and defense policy decisions.[148]

---

144 Ibid., 31.

145 Ibid., 30.

146 ICT online newspaper (IT bransjens nettavis) http://www.digi.no/919026/norcert-sjefen-slutter.

147 The police, Kripos' strategy 2011–2015, 10, https://www.politi.no/vedlegg/lokale_vedlegg/kripos/Vedlegg_1466.pdf.

148 FAD, "Cyber Security Strategy for Norway," December 17, 2012, 31.

In 1998, the Storting (The Parliament) passed the Public Act for the NIS.

> The NIS shall collect, evaluate, and analyze information concerning Norwegian interests in relation to foreign countries, organizations, and individuals. With this platform, it will compile threat warnings and intelligence estimates, to the extent it can contribute to securing the vital interests of the society.[149]

A Royal Instruction followed the Public Act in 2001 and stated: "The MoD can establish procedures to ensure communication and cooperation with other ministries and institutions that require information obtained from the Service."[150]

In Norway, the NIS produces all-source products, compiled from different collection assets. Technical collection and evaluation of data and human intelligence (HUMINT) is organized within the NIS. This means that NIS has both legislative and organizational authority that facilitates an active use of organizational resources in the cyber domain. According to current records of the national budget for 2013, the NIS was allocated NoK 1115 million (US$ 192 million).[151]

Cooperation between the Norwegian Intelligence Service and the Norwegian Police Security Service has become increasingly close in the post–9/11 era. In October 2006, the government passed Royal Instructions for extended cooperation between the two services. This means that the practical cooperation between NIS and the Norwegian Police Security Service is one of

149 Public Act for the Norwegian Intelligence Service (LOV 1998–03–20 nr 11; Lov om Etterretningstjenesten), §3, available from http://www.lovdata.no/all/hl-19980320–011.html (accessed October, 11, 2013). Translation from NPS master's thesis, The Norwegian Decision-Making Process And Ways To Improve It, written by Stein Kynø December 2007.

150 Royal Instruction for NIS, §16.

151 Forsvarsdepartementet [Norwegian Ministry of Defence] St. Prop 1S (2012–2013) For budsjettåret 2013 [The Ministry of Defence: For fiscal year 2013, Parliamentary Bill no. 1S (2012–2013)], 132, http://www.regjeringen.no/pages/38070918/PDFS/PRP201220130001_FDDDDPDFS.pdf.

few examples of collaboration across the responsible ministries and government agencies.

i. Norwegian Police Security Service (PST)

PST is Norway's civilian domestic intelligence and security services and is, consequently, responsible for the nation's internal security. PST is part of the police but reports directly to the Ministry of Justice and Public Security. PST's primary task is, as stated by the Police Act, to prevent and investigate crimes against national security. More precisely, this includes preventing and detecting espionage, terrorism/politically motivated violence, the spread of weapons of mass destruction, material and technology for the production of such weapons and threats against officials. This requires the service to use a variety of methods for prevention and preventive work, necessitating extensive cooperation with other countries' security services. The focus is on the collection of information about people and groups that may pose a threat, preparation of various analyzes and threat assessments, investigations and other operational measures and counseling.

PST also has an advisory role to the government and other Norwegian authorities, for such activities as preparing PST threat assessments as part of efforts to safeguard the Norwegian state's security and independence.

The Ministry of Justice determines if the PST shall be given responsibility for fighting organized crime, crimes against humanity, genocide, and aggravated war crimes.[152] According to open sources, PST was allocated NKR 525 million (US$ 90.5 million) in 2012.[153]

A new counter-terrorism center has been established in PST. To best facilitate this effort, the government has decided that it will establish a joint

152 Norwegian Intelligence Service, NSM and PST, Threats and Vulnerabilities, 2013, 2, http://www.pst.no/media/59018/Trusler_og_sarbarheter_2013.pdf.

153 TV2, "How PST uses the money," http://prosjekt.tv2.no/dybde/i/slik-bruker-pst-pengene.

counter-terrorism center in PST. The center will be staffed with personnel from both PST and NIS.[154]

j. The Cyber Defense

The Norwegian Armed Forces' ability to meet the cyber threat was strengthened in 2012 with the creation of The Cyber Defense. The main task of cyber defense is to operate and develop military communications and support military operations both at home and abroad. Cyber Defense supports network-based operations and contributes to significant improvements in interoperability, flexibility, responsiveness, mobility and deployability. Within current budget limits, the Cyber Defense can adapt the organization and tasks in accordance with the structural changes that are made in other parts of the military.[155]

An overview of the ministries and agencies responsible for cyber defense in Norway is shown in Figure 4.

154 New Joint CT Center, Presentation of Unified Threat Assessment, February 18, 2013 http://www.regjeringen.no/nb/dep/jd/aktuelt/taler_og_artikler/ministeren/taler-og-artikler-av-grete-faremo/2013/presentasjon-av-samordnet-trusselvurderi.html?id=714684.

155 Forsvarsdepartementet [Norwegian Ministry of Defence] , St.prp. Nr 73 S (2011–2012) Et Forsvar for vår tid [The Ministry of Defence: A defence for our time, Parliamentary Bill no. 73 S (2011–2012)], 102. http://www.regjeringen.no/pages/37583840/PDFS/PRP201120120073000DDDPDFS.pdf.

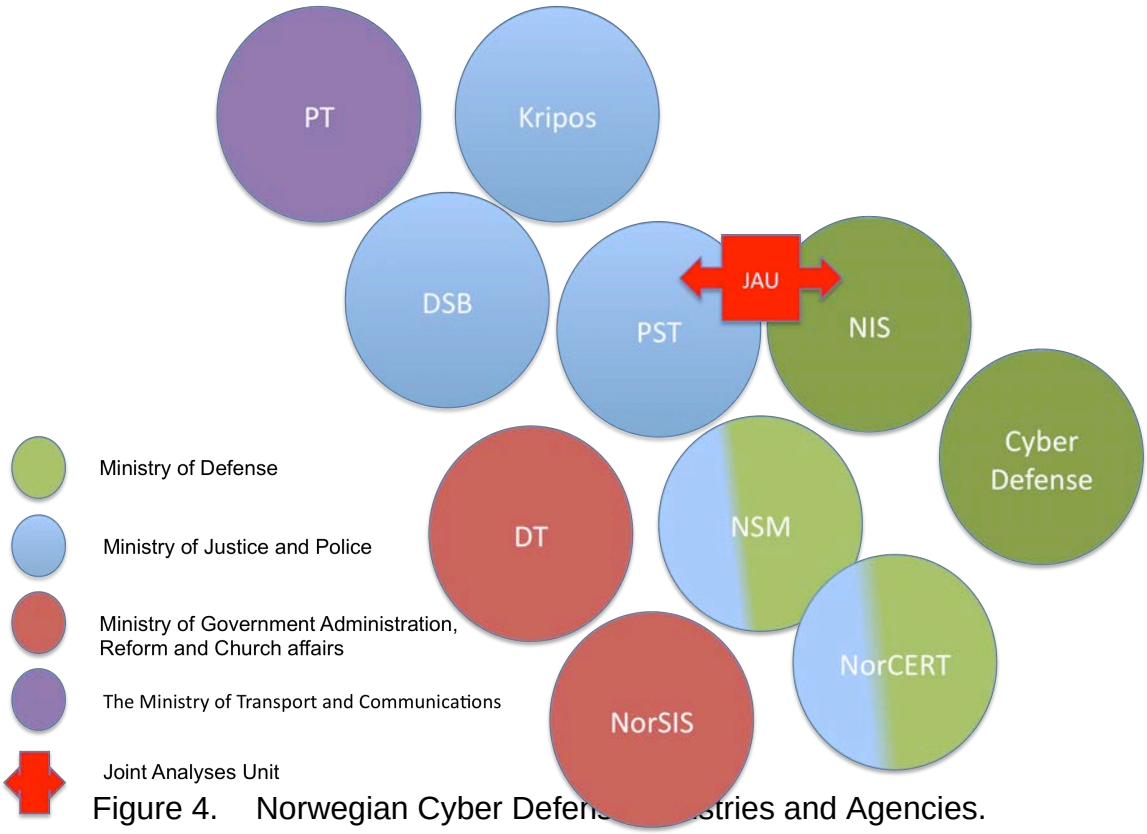

Figure 4. Norwegian Cyber Defen stries and Agencies.

This organization is not specific to Norway, and many countries, including Finland, have a similar sharing of responsibilities. In a country with limited resources, this organizational plan might not be appropriate. In China, the PLA has an apparent role in the design, planning and execution of operations in the cyber domain. A central organization with executive command in cyber defense seems to be an effective way of organizing.

F. NORWAY'S GOALS AND STRATEGIC PRIORITIES

The Government has identified four overarching goals for information security. None of these overarching information security goals is more important than another, and they are mutually dependent success factors.

1. Better coordination and common situational understanding
2. Robust and secure ICT infrastructure for everyone

3. Good ability to handle adverse ICT events

4. High level of competence and security[156]

These overarching goals will be operationalized through seven strategic priorities:

- Ensure a more comprehensive and systematic approach to information security
- Improve ICT infrastructure
- Ensure a common approach to information security in public administration
- Safeguard society's ability to detect, alert and handle serious ICT incidents
- Safeguard society's ability to prevent, detect and investigate cyber crime
- Raise awareness and competence
- Provide high quality national research and development in the field of information security[157]

The Government will follow up this strategy with specific measures in an action plan, which will be published separately.[158] The strategic document describes how Norway must be in a constant state of proactive operational preparedness in order to prevent, detect and coordinate reactions to serious ICT incidents. Relevant authorities and organizations are supposed to work in close collaboration, with special emphasis on working with those parts of the private sector that own or operate infrastructure. This collaboration must address both intentional and unintentional events, such as technical or human error, accidents, or natural disasters.

Furthermore, cyber criminals should not be able to plan or execute crimes without a significant risk of being detected and prosecuted. Society's ability to prevent, detect and investigate cyber crime must be prioritized. All stakeholders

156 FAD, "Cyber Security Strategy for Norway," December 17, 2012, 16–17.

157 Ibid., 17.

158 Ibid., 18–19.

should, on their own initiative, implement crime prevention measures in their own organizations and seek to minimize losses or damage as a result of cyber crime. Public authorities shall achieve this through increased expertise, and by improving specialist expertise and the skills of police generalists. The police must make this a priority and increase their capacity to prevent, detect and investigate cyber crime. Public authorities will continue to increase their capacity in this field in order to detect cyber crime that directly or indirectly may have an impact on national security or vital national interests.[159]

Many of the strategic priorities may seem obvious and the overall objectives are centered on protection and safety. A number of important issues are identified, but it is difficult to see clear guidance on how to meet the challenges. There are a number of correct assumptions, but where the document on the one side refers to the somewhat vague "relevant authorities," on the other side, it is specific about the police who must increase their capacities. The strategic document appears with many good ideas and plans, but there is no overarching department or agency that can implement the plans. In relation to the four areas of interest in the Finnish strategy, Norway seems to have the same focus on "Shared Situation Awareness," "Cyber Security Centre" and "Participation in International R & D and Exercises." However, it is difficult to find anything about "Strategic Agility" in the Norwegian document. This is perhaps the weakness of the Norwegian strategy, i.e., although four ministries have signed the document, it does not strengthen strategic direction.

G. SUMMARY

A review of Norway's cyber security strategy shows in all essence that the government has prepared a good document for its purpose. It is clear in the description of the threat, and it describes a number of good measures; however, it gives no definition of the cyber domain. The focus is on defense and protective

[159] Ibid., 20–22.

initiatives without acknowledging the broader aspects of cyberspace. Norway has a good strategy for information security, but lacks a strategy for cyber security.

Regarding organization, coordinating Norway's cyber defenses is a challenge, although a joint analysis unit has been established between PST and NIS. The fact that all four ministries have responsibilities that border the cyber domain increases the likelihood of problems with regard to coordination and decision-making. The organization is not optimal with respect to both leadership and resource allocation when four different ministries are to both lead and fund an activity they share with others.

The importance of the Ministry of Defense should be more significant, at the expense of the other departments. Norway's cyber defenses are small, consisting of three main intelligence and security services, one military organization and five agencies with specialist responsibility. This structuring makes the Norwegian cyber defenses scattered with subsequent risk of areas that lack coordination and responsibility. A key premise is that the NIS and the Cyber Defense are already subordinated to the Minister of Defense; NSM is also partially under the same ministry. Thus, three key players are already organized under the same minister.

The criteria for an effective cyber defense are the joint exploitation of national resources across civil and military sphere, unconventional methods and a highly professional environment.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS FOR AN IMPROVED NORWEGIAN CYBER SECURITY APPROACH

A. INTRODUCTION

This chapter presents criteria for an ideal and successful holistic approach to cyber security for the Norwegian Government and identifies current shortfalls.

B. SUMMARY

Chapters II and III of this thesis argue that cyberspace has opened up a new channel through which states can project power and that cyber power is a real force multiplier for those who have the ability to exercise such power. Cyber power is different from other powers because so many players can exercise it and the opportunities to attack an opponent are many, given that there are no clear boundaries between war and peace. This means that those who have the will, resources and access, whether they are individuals, groups or states, have a unique source of power.

Chapter IV of this thesis argues that China can be seen as an example of a state that is actively using cyberspace for espionage and as a means of deterrence. China has a coherent strategy and sufficient funds; it is training a significant number of hackers who work for the state. China's technological focus gives a hint of what is possible to achieve if a nation realizes the potential of cyberspace and illustrates how cyber power can support strategic objectives.

Chapter V of this thesis argues that in many respects, Norway's cyber defenses are modern and updated, but that the Norwegian cyber strategy is both narrow and relatively unambitious. The government has opted for a defensive information security strategy, and it is difficult to find any recognition of cyberspace as a domain of conflict in the official documents.

The thesis set out to examine how Norway can best counter threats in cyberspace. In Chapter V, the thesis explores the current status of Norwegian cyber strategy and defenses and concludes that Norway has focused scattered

resources on defensive measures. Norway has no coherent strategy for cyberspace and for how this domain can be used to establish national strategies.

An effective way to counter threats in cyberspace is a joint exploitation of national resources across the civil and military spheres, unconventional methods and a highly professional environment. This assertion forms the basis for the recommendations made in this thesis.

C. CHALLENGES

In Norway, the focus on cyber security has gained increasing attention, and the central authorities have published updated doctrines and strategies. The regular cyber attacks against Norwegian authorities and companies are mentioned in the newspapers, while the military cyber defense leadership is steadily improving the promotion of their field of responsibility. The challenge in relation to cyber defense, however, is the sector division that has characterized the Norwegian government. This division has obvious weaknesses in relation to situational awareness and in distribution of resources as well as command and control. The fact that four ministers sign a strategy can be seen as a sign of strength, but what it really says is that no one has complete responsibility and that it is unclear who will be the stakeholder during a crisis. This weakness has already been pointed out in the aforementioned Vulnerability Committee report from 2000, which suggested a separate emergency ministry: "Collection of responsibility for civil protection and emergency preparedness in a ministry that has this as primary task."[160]

This is the de facto structural division of responsibility in the Norwegian public administration and is unlikely to change any time soon, so it may be important to look at what can be done within the current organization.

160 Norges offentlige utredninger (NOU) [Norwegian Official Reports] 2000:24, "A Vulnerable Society," 11.

D. RECOMMENDATIONS

These proposals, extending from the strategic to the tactical level, are not ranked according to importance. The purpose is to point out some specific areas of improvement that can help Norway to better counter threats in cyberspace.

1. Offensive versus Defensive Posture for Norway

Most countries have prepared for cyber war. Most nations, however, seem to keep the defensive posture. As discussed in previous chapters, it is paradoxical that attacking is both simple and effective in cyberspace. One possible explanation is that there is no clear distinction between war and peace in cyberspace. This means that most operations can be termed defensive while, in reality, they may be offensive. For small countries, it is possible that the perception of warfare means that they, by default, manage their resources defensively. It is a simple and uncontroversial solution.

Offensive cyber capability requires a continuous process of collecting vulnerabilities, creating exploits, platforms and warheads, and building a network of deniable hosts on the Internet to maintain the secrecy of the operator. Since these are low-cost operations (in comparison to kinetic military capabilities), it can be argued that these preparations should be made even if the current doctrine does not include the use of offensive cyber capabilities.[161]

A proactive approach to operations in cyberspace would likely result in a change in attitude and would require political decision-makers to be aware of the consequences. The advantages of such an approach, given that it becomes public knowledge, are that the nation would be seen as a serious and tough player in cyberspace. Norway is likely to have both the technology and resources to conduct offensive cyber operations; the question is, therefore, a political trade-

[161] Timo Kiravuo and Mikko Särelä, “The Care and Maintenance of Cyberweapons,” 227 in The Fog of Cyber Defence, ed. Jari Rantapelkonen & Mirva Salminen (Helsinki: National Defence University, 2013).

off. The alternative is to focus on defense alone, thus avoiding any inconvenience with other nations.

However, Norway should establish an offensive cyber capability. This would not only complement the cyber defense, but it would also create a new dimension where threats, whether by individuals, groups or nations, could be actively contested. As described in Chapter Three, cyber power and cyber war can be analyzed in several ways, from which it should be possible to develop appropriate strategies for Norway.

2. Cross-Boundary Information Sharing

The complexity of cyberspace and the current Norwegian organization make it difficult to establish a common shared situational awareness. This may change by sharing information across government, agencies and civilian actors. In anticipation of organizational changes, a change in guidelines for classification should be considered. This would allow a selected sample of key players in both government and private business (after security clearance) to receive classified information and classified assessments.

3. Unified Command and Control

Although there are structural reasons for how responsibility and power is divided between ministries in Norway, a future goal should be unified management of cyber defense. Such a “cyber command/cyber security centre” would probably be able to coordinate Norway’s military and civilian sectors. As shown in Chapter Five, in Norway, responsibilities in cyberspace are divided among four ministries and eight agencies. An important first step would be to make one ministry responsible for the nation’s cyber efforts. This should be the Ministry of Defense (MoD), given that it has the necessary skills for crisis management and that key institutions such as NIS, NSM and Cyber Defense are already subordinated to the Ministry. It is also an important point that are no distinction between war and peace in cyberspace, something to countless offensive operations between both individuals, groups and nations shows.

Operations in this new domain will likely favor the one who masters the art of war and operational planning in the traditional domains; this also indicates that the MoD should take the lead this sector.

4. Frontline Technology and a Professional Environment

ICT depends on innovation, expertise and speed in development circles. Norway has access to the relevant technology environments, but a challenge would be to invest adequately in future technologies. This must be achieved through a combination of education and cultivation of creative and technologically strong and adaptable environments including international R & D. China has solved this challenge by investing in universities. Government investments would ensure that research is financially supported and both government and industry would take the lead of innovation. All students and many professors would work partly for the state's interests, something that should be possible in a country like Norway where so many are already working for the state. The government must show strategic agility by utilizing the ability to adjust and adapt to new innovative ideas and use those ideas to create new products and services that enhance the cyber defense.

5. The Power of Deterrence

Another philosophy of cyber defense is to focus on deterrence. Even for a small nation, a policy based on deterrence can be effective. During the Cold War, Norway's armed forces were not far from the border with the Soviet Union. Norwegian forces were significantly weaker than the Soviets', but the presence and willingness to fight sent a strong signal. Translated into a modern language and adapted to cyberspace, it is conceivable that the Finnish model is a modern version of such thinking. As mentioned above, Finland has a national goal of becoming the world's leading country in cyber security; even without going into details, this sends a strong signal of will.

E. CONCLUSION

Two factors necessitate this study. First, Norway has a strategic infrastructure that remains largely tied to the nation's oil and gas industry. This generates revenue that is essential to ensure the country's future growth and prosperity. Second, there seems to be a general understanding that the importance of cyberspace is increasing and that other nations are investing heavily to both exploit and defend their cyber domain. Acknowledging these challenges would streamline the use of existing Norwegian technology, strategy and funding, while allowing for investments in innovation, development and new command and control structures; these aspects that are crucial to a small country with limited resources.

Finally, cyber security is not only about technology and innovation. Culture, norms, organizational design and legislation are important to cyber security. These topics must be discussed, agreed upon and implemented in co-operation among decision makers, ministers, the police and intelligence agencies, the armed forces and other governmental agencies. Freer thinking about cyberspace would make Norway more open to new ideas for both defense and security.

LIST OF REFERENCES

Arquilla, John, and David Ronfeldt. “Cyberwar is Coming!” Santa Monica, CA: RAND Corporation, 1993.

Boebert, W. Earl. “A Survey of Challenges in Attribution,” in *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, Committee on Deterring Cyber Attacks: Informing Strategies and Developing Options*. National Research Council Washington, DC: The National Academies Press, 2010.

Bumiller, Elisabeth and Tom Shanker. “Panetta Warns of Dire Threat of Cyberattack on U.S.” *The New York Times*. October 11, 2012. Accessed August 12, 2013. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0.

Center for a New American Security. “Policy Brief, Active Cyber Defense, A Framework for Policymakers.” February 2013. Accessed November 5, 2013. http://www.cnas.org/files/documents/publications /CNAS_ActiveCyberDefense_Lachow_0.pdf.

Cheung, Tai Ming. “Dragon on the Horizon: China’s Defense Industrial Renaissance.” published online February 25, 2009. Accessed September 6, 2013. http://www.tandfonline.com/doi/abs/10.1080 /01402390802407418#.Uombo5FEhyg.

Cisco. “Security Flirting, Definitions.” Accessed September 1, 2013. https://docs.meraki.com/display/MX/Security+filtering.

Clarke, Richard and Robert K. Knake. “Cyber War, U.S.-China Economic and Security Review Commission,” 2012 Report to Congress, China’s Cyber Activities, November 2012. Accessed 29, 2013. http://www.uscc.gov/annual_report/2012/2012_Report_to_Congress_table .pdf.

Coleman, Kevin. “China’s Cyber Forces,” Defense Tech, 2008. Accessed September 7, 2013. http://defensetech.org/2008/05/08/chinas-cyber-forces/.

Conley, Heather A. and Theodore P. Gerber. “Soft Power in the 21st Century, An Examination of Russian Compatriot Policy in Estonia,” A Report of the CSIS Europe Program, August 2011. Accessed August 11, 2103. http://csis.org/files/publication/110826_Conley_RussianSoftPower_Web.pdf.

Cooperative Cyber Defence Centre of Excellence. *International Cyber Incidents*. Tallinn: Estland 2010. Accessed November 4, 2013. http://www.ccdcoe.org/publications/books/legalconsiderations.pdf.

Denning, Dorothy E. “Barriers to Entry: Are They Lower for Cyber Warfare?,” *IO Journal* 1, no. 1 (2009).

eEstonia. “The Digital Society.” Accessed September 2, 2013. http://e-estonia.com/components/x-road.

Finland’s Cyber Strategy: Government Resolution 24th of January 2013. Accessed October 30, 2013. http://www.defmin.fi/en/publications/strategy_documents/finland_s_cyber_security_strategy.

Forsvarsdepartementet [Norwegian Ministry of Defence] St.prp 1S (2012–2013) *For budsjettåret 2013* [The Ministry of Defence: *For fiscal year 2013*, Parliamentary Bill no. 1S (2012–2013)]. Accessed October 14, 2013. http://www.regjeringen.no/pages/38070918/PDFS/PRP201220130001_FDDDDPDFS.pdf.

Forsvarsdepartementet [Norwegian Ministry of Defence], Meld. St. 14 (2012–2013) *Kompetanse for en ny tid* [The Ministry of Defence: *Competence for a New Era*, White paper, no. 14 (2012–2013)], 12. Accessed September 13, 2013. http://www.regjeringen.no/pages/38247066/PDFS/STM201220130014000DDDPDFS.pdf.

Forsvarsdepartementet [Norwegian Ministry of Defence], St.prp. Nr 73 S (2011–2012) *Et Forsvar for vår tid* [The Ministry of Defence: *A Defense for Our Time*, Parliamentary Bill no. 73 S (2011–2012)]. Accessed August 12, 2013. http://www.regjeringen.no/pages/37583840/PDFS/PRP201120120073000.

Godwin, Paul H.B. “PLA Doctrine and Strategy: Mutual Apprehension in Sino-American Military Planning,” in *The People’s Liberation Army and China in Transition*, edited by Stephen J. Flanagan and Michael E. Marti. Institute for National Strategic Studies, National Defense University, August 2003, 272–273. Accessed September 5, 2103. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA430961.

Hillestad, Linn Kongsli, Sandli, Espen and Strømman, Ola. “In the Worst Case, People Can Die,” *Dagbladet*, October 17, 2013. Accessed November 20, 2013. http://www.dagbladet.no/2013/10/17/nyheter/innenriks/datasikkerhet/nullctrl/28572676/.

Hjortdal, Magnus. “Strategic Security in the Cyber Age: China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence,” *Journal of Strategic Security* 4, no. 2 (Summer 2011). Accessed September 14, 2013. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss.

ICT online newspaper (*IT bransjens nettavis*). Accessed October 14, 2013. http://www.digi.no/919026/norcert-sjefen-slutter.

Johnson, Nicole Blake. “Report: Cyber Attacks on Critical Infrastructure Jump 383% in 2011.” *Federal Times*, July 3, 2012. Accessed August 12, 2103. http://www.federaltimes.com/article/20120703/IT01/307030004/Report-Cyber-attacks-critical-infrastructure-jump-383–2011.

Justis- og Beredskapsdepartementet [Norwegian Ministry of Justice and Public Security], Meld. St. 29 (2011–2012) *Samfunnssikkerhet* [The Ministry of Justice and Public Security: *Civil Protection*, White paper no. 29 (2011–2012)]. Accessed September 12, 2013. http://www.regjeringen.no/pages/37919076/PDFS/STM201120120029000DDDPDFS.pdf.

Kessler, Gary C. “An Overview of Cryptography,” Accessed September 1, 2013. http://www.garykessler.net/library/crypto.html#purpose.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. Washington, DC: National Defense University Press, 2009.

Krekel, Bryan, Patton Adams, and George Bakos. *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*. Prepared for The U.S.-China Economic and Security Review Commission, Northrup Grumman Corp., October 9, 2009.

Krekel, Bryan, Patton Adams and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Northrup Grumman Corp., March 7, 2012. Accessed September 3, 2013. http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

Kuehl, Daniel T. “From Cyberspace to Cyberpower,” in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: National Defense University Press, 2009.

Kugler, Richard L. “Deterrence of Cyber Attacks,” in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: National Defense University Press, 2009.

Lachow, Irving. “Cyber Terrorism: Menace or Myth,” in *Cyberpower and National Security*, edited Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: National Defense University Press, 2009.

Langø, Hans-Inge. “Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security.” Norwegian Institute of International Affairs, 2013. Accessed August 25, 2013. http://english.nupi.no/Publications/Working-Papers/2013/Slaying-Cyber-Dragons-Competing-Academic-Approaches-to-Cyber-Security.

Liang, Qiao and Xiangsui Wang. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, February 1999.

Libicki, Martin C. *What Is Information Warfare*? Washington, DC: National Defense University, 1995.

Mandiant. “APT 1 Exposing One of China’s Cyber Espionage Units.” Accessed September 14, 2103. http://intelreport.mandiant.com /Mandiant_APT1_Report.pdf.

McAfee. Virtual Criminology Report 2009 “Virtually Here: The Age of Cyber Warfare.” Accessed October 5, 2013. http://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf.

Miller, Bill and Dale C. Rowe. “A Survey of SCADA and Critical Infrastructure Incidents.” Brigham Young University Information Technology Program, Provo, Utah. Accessed September 1, 2013. http://sigite2012.sigite.org/wp-content/uploads/2012/08/session17-paper01.pdf.

Nasjonal sikkerhetsmyndighet [National Security Authority], Rapport om sikkerhetstilstanden 2012 [Security conditions 2012]. Accessed August 22, 2013. https://www.nsm.stat.no/Documents/Risikovurdering /Ugradert%20rapport%20om%20sikkerhetstilstanden%202012.pdf.

National Institute of Standards and Technology, Computer Security Division. “Identification and Authentication of Users.” Accessed September 1, 2103. http://csrc.nist.gov/publications/nistpubs/800–11/node26.html.

New Joint CT Center, “Presentation of Unified Threat Assessment,” February 18, 2013. Accessed October 14, 2103. http://www.regjeringen.no/nb/dep /jd/aktuelt/taler_og_artikler/ministeren/taler-og-artikler-av-grete-faremo/2013/presentasjon-av-samordnet-trusselvurderi.html?id=714684.

Norges offentlige utredninger (NOU) [Norwegian Official Reports] 2000:24, Et sårbart samfunn, Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet, 4 juli 2000 [A Vulnerable Society: Challenges for Norwegian Security and Preparedness, July 4, 2000]. Accessed August 12, 2103. http://www.regjeringen.no/Rpub/NOU/20002000/024/PDFA/NOU200020000024000DDDPDFA.pdf.

Norges offentlige utredninger (NOU) [Norwegian Official Reports] 2006:6, *Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*, 5 japril 2006 [*When Security Is Important: Protecting the Nation's Critical Infrastructures and Critical Societal Functions*, April 5, 2006. Accessed September 1, 2013. http://www.regjeringen.no/nb/dep/jd/dok/nouer/2006/nou-2006–6/5/1.html?id=157439.

Norwegian Intelligence Service. "Focus 2012." Accessed August 22, 2013. http://forsvaret.no/om-forsvaret/organisasjon/felles/etjenesten/Documents/etj_lo-res.pdf.

———. "Focus 2013." Accessed August 22, 2103. http://forsvaret.no/om-forsvaret/organisasjon/felles/etjenesten/Documents/0886-FOCUS-english-2013.pdf.

———. "NSM and PST, Threats and Vulnerabilities," 2013. Accessed October 14, 2013. http://www.pst.no/media/59018/Trusler_og_sarbarheter_2013.pdf.

Norwegian Ministry of Government Administration, Reform and Church Affairs [FAD] "Cyber Security Strategy for Norway," December 17, 2012. Accessed September 12, 2013. http://www.regjeringen.no/en/dep/fad/documents/Reports-and-plans/Plans/2012/cyber-security-strategy-for-norway.html?id=710469.

Norwegian Ministry of Government Administration, Reform and Church Affairs, Meld. St. 23 (2012–2013) *Digital Agenda for Norge, IKT for vekst og verdiskaping*, [Ministry of Government Administration, Reform and Church Affairs. *Digital Agenda for Norway, ICT for Growth and Value*, White paper no. 23 (2012–2013)]. Accessed September 13, 2013. http://www.regjeringen.no/pages/38354256/PDFS/STM201220130023000EN_PDFS.pdf.

Nye, Jr., Joseph S. *Cyber Power*. Boston: Harvard Kennedy School, May 2010.

———. *The Future of Power.* New York: Public Affairs, 2011.

Nygård, Arne Roar. “Risk Management in SCADA System.” Master’s thesis, Royal Institute of Technology, Sweden, July 2004. Accesed September 1, 2013. http://brage.bibsys.no/hig/handle/URN:NBN:no-bibsys_brage_4310.

O’Neil, William D. “Cyberspace and Infrastructure,” in *Cyberpower and National Security*, edited by. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. (Washington, DC: National Defense University Press, 2009).

Owens, William A., Dam, Kenneth W. and Lin, Herbert S. (eds.). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Research Council, The National Academies Press, 2009.

Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, Committee on Deterring Cyber Attacks: Informing Strategies and Developing Options. Washington, DC: National Research Council, The National Academies Press, 2010.

Public Act for the Norwegian Intelligence Service (LOV 1998–03–20 nr 11; Lov om Etterretningstjenesten), §3. Accessed October 11, 2013. http://www.lovdata.no/all/hl-19980320–011.html. Translation from NPS Master’s thesis, “The Norwegian Decision-Making Process and Ways To Improve It,” written by Stein Kynø, December 2007.

Rantapelkonen, Jari & Salminen, Mirva. “The Fog of Cyber Defence.” Helsinki: National Defence University, 2013. Accessed October 29, 2013. http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf.

Rattray, Gregory and Jason Healey. “Categorizing and Understanding Offensive Cyber Capabilities and Their Use” in *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council, The National academics Press 2010.

Rona, Thomas P. “Weapon Systems and Information War,” Office of the Secretary of Defense, July 1, 1976.

Royal Instruction for NIS, §16.

Shackelford, Scott. “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,” *Berkeley Journal of International Law* 27:1, (2008).

Smith, David J. “How Russia Harnesses Cyberwarfare,” *Defense Dossier*, Issue 4, (August 2012). Accessed November 4, 2013. http://www.afpc.org/files/august2012.pdf.

The Economist. “War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?” *The Economist*, July 1, 2010. Accessed August 12, 2013. http://www.economist.com/node/16478792.

The Nordic Page. “China is Behind more than 20 Serious Cyber Attacks against Norway.” Accessed September 5, 2013. http://www.tnp.no/norway/politics/3580-china-is-behind-more-than-20-serious-cyber-attacks-against-norway.

Nobel Prize.org. “Liu Xiaobo – Facts.” Accessed October 21, 2013. http://www.nobelprize.org/nobel_prizes/peace/laureates/2010/xiaobo-facts.html.

“The Police Kripos’ Strategy 2011–2015.” Accessed October 14, 2013. https://www.politi.no/vedlegg/lokale_vedlegg/kripos/Vedlegg_1466.pdf.

Thuv, John, Windvik, Ron, Nystuen, Kjell Olav and Sivertsen, Tormod. “Vulnerabilities in Internet” (source of ideas for figure). Accessed August 15, 2013. http://rapporter.ffi.no/rapporter/2007/00903.pdf.

TV2. “*How PST Uses the Money.*” Accessed October 14, 2013. http://prosjekt.tv2.no/dybde/i/slik-bruker-pst-pengene.

U.S.-China Economic and Security Review Commission, 2012 Report to Congress of the U.S.-China Economic and Security Review Commission, Executive Summary and Recommendations, November 2012. Accessed September 5, 2013. http://origin.www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress-Executive%20Summary.pdf.

U.S. Department of Defense, Annual Report to Congress, “Military and Security Developments Involving the People’s Republic of China 2013.” Accessed September 5, 2013. http://www.defense.gov/pubs/2013_china_report_final.pdf.

U.S. Department of Energy, Technical Lessons Learned from the Shamoon Malware Attacks, CIP Awareness Bulletin – Joint Product October 2012, “Shamoon Malware Targets Oil and Natural Gas Critical Infrastructure Systems.” Accessed October 8, 2013. http://www.nwppa.org/CWT/EXTERNAL/WCPAGES/WCMEDIA/DOCUMENTS/_NEWSLETTERS/CIP%20AWARENESS%20BULLETIN-SHAMOON%20TECHNICAL%20LESSONS%20LEARNED.PDF.

U.S. Department of Homeland Security, “ICS-CERT Monitor.” Accessed September 2, 2013. http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf.

———. “National Infrastructure protection Plan.” Accessed September 1, 2013. http://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf.

U.S. Government Accountability Office.”Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance.” (Washington, D.C., 2010). Accessed September 29, 2013. http://gao.gov/assets/310/308401.pdf.

U.S. Joint Chiefs of Staff, Information Operations, Joint Publication 3-13. November 27, 2012. Accessed October 15, 2013. http://www.fas.org/irp/doddir/dod/jp3_13.pdf.

World Economic Forum. The Global Information Technology Report 2012, “Living in a Hyperconnected World.” Accessed October 19, 2013. http://www3.weforum.org/docs/Global_IT_Report_2012.pdf.

Yrani, Julia and Handel, William. “Cyberwar and the Deterrence Calculus, Assessing a U.S.-China Balance in the Digital Realm 2012.” Accessed September 3, 2013. http://www.scribd.com/doc/137608606/Cyberwar-and-the-Deterrence-Calculus-Assessing-a-U-S-China-Balance-in-the-Digital-Realm.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu