Implications of Cyber Weapons in Cybersecurity: A Case Study of Stuxnet and Duqu

M.A. Thesis

Cem DEMİRCAN

Eskişehir, 2019

Implications of Cyber Weapons in Cybersecurity: A Case Study of Stuxnet and Duqu

Cem DEMİRCAN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF MASTER'S DEGREE

International Relations Program / Graduate School of Social Sciences

Supervisor: Prof. Dr. Nejat DOĞAN

Eskişehir

Anadolu University

Graduate School of Social Sciences

August, 2019

FINAL APPROVAL FOR THESIS

This thesis titled "**Implications of Cyber Weapons in Cyberscurity: A Case Study of Stuxnet and Duqu**" has been prepared and submitted by **Cem DEMİRCAN** in partial fullfillment of the requirements in "**Anadolu University Directive on Graduate Education and Examination**" for the Master of Arts in **Department of International Relations** has been examined and approved on **21/08/2019.**

Committee Members		**Signature**
Member (Supervisor)	: Prof.Dr. Nejat DOĞAN	
Member	: Prof.Dr. Beytullah Gültekin ÇETİNER	
Member	: Assoc.Prof.Dr. Ramazan ERDAĞ	

21/08/2019
Date

Prof.Dr.Bülent GÜNSOY
Director
Graduate School of Social Sciences

ÖZET

Implications of Cyber Weapons in Cybersecurity: A Case Study of Stuxnet and Duqu

Cem DEMİRCAN
Uluslararası İlişkiler Anabilim Dalı
Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, July, 2019
Danışman: Prof. Dr. Nejat DOĞAN

Bu çalışma devlet temelli siber silahlar olan Stuxnet ve Duqu'nun etkilerini ve yeteneklerini literatürün belirlediği siber silah tanımlarıyla karşılaştırarak siber güvenlik ve bilgisayar ağı operasyonlarına olan etkilerini incelemeyi ve tartışmayı amaçlamaktadır. İlk siber savaş olarak nitelendirilen, Estonya devletine karşı 2007 yılında gerçekleştirilen dağıtık hizmet engeli saldırıları da siber silah olarak sınıflandırıp sınıflandırılamayacağını anlamak amacıyla incelenmiştir. Çalışma Stuxnet'in siber silah tanımlarına uyduğunu saptarken, iki devlet temelli zararlı yazılım arasındaki operasyonel farklılıklar nedeniyle Duqu yalnızca bir casusluk aracı olarak nitelendirilmiştir. Estonya'ya karşı yapılan hizmet engelleme saldırılarının ise literatürde ortaya konan siber silah ya da siber savaş kavramlarına uymadığı saptanmıştır.

Anahtar Kelimeler: Siber silahlar, Siber Savaş, Stuxnet, Duqu

ABSTRACT

Implications of Cyber Weapons in Cybersecurity: A Case Study of Stuxnet and Duqu

Cem DEMİRCAN

International Relations

Anadolu University, Graduate School of Social Sciences, July, 2019

Supervisor: Prof. Dr. Nejat DOĞAN

This work aims to examine and discuss the implications of state-borne cyber weaponry to cybersecurity and computer network operations through explaining the effects and capabilities of Stuxnet and Duqu and comparing these abilities to the definitions of cyber weapons established by the literature. Heralded as the first cyber war, case of distributed denial of service attacks of 2007 against the state of Estonia is also examined to understand whether denial of service attacks can be classified as cyber weapons. Stuxnet was found to have fit within the descriptions and definitions of a cyber weapon while the Duqu has been classified as an espionage asset due to operational differences between two state actor borne malware. Denial of service attacks against Estonia did not conform to the cyber weapon or cyber warfare definitions established by the literature.

Keywords: Cyber weapons, Cyber warfare, Stuxnet, Duqu

14/05/2019

STATEMENT OF COMPLIANCE WITH ETHICAL PRINCIPLES AND RULES

I hereby truthfully declare that this thesis is an original work prepared by me; that I have behaved in accordance with the scientific ethical principles and rules throughout the stages of preparation, data collection, analysis and presentation of my work; that I have cited the sources of all the data and information that could be obtained within the scope of this study, and included these sources in the references section; and that this study has been scanned for plagiarism with "scientific plagiarism detection program" used by Anadolu University, and that "it does not have any plagiarism" whatsoever. I also declare that, if a case contrary to my declaration is detected in my work at any time, I hereby express my consent to all the ethical and legal consequences that are involved.

Signature

Cem DEMİRCAN

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

APT : Advanced Persistent Threats

AS : Autonomous Systems

BCI : Brain Computer Interface

BGP : Border Gateway Protocol

CCDCOE : Cooperative Cyber Defence Centre of Excellence

CERT : Computer Emergency Readiness Team

CISA : Cybersecurity and Infrastructure Security Agency

CNA : Computer Network Attacks

CNE : Computer Network Exploitation

CNO : Computer Network Operations

CYBINT : Cyber Intelligence

DoS : Denial of Service

DDoS : Distributed Denial of Service

DNS : Domain Name System

HIDS : Host-based Intrusion Detection Systems

HUMINT : Human Intelligence

HTTP : Hypertext Transfer Protocol

HTTPS : Hypertext Transfer Protocol Secure

IANA : Internet Assigned Numbers Authority

ICS : Industrial Control Systems

ICT : Information and Communication Technology

IDS : Intrusion Detection System

IEEE : The Institute of Electrical and Electronics Engineers

IoT : Internet of Things

IPS : Intrusion Prevention System

ISP : Internet Service Provider

IAEA : International Atomic Energy Agency

IT : Information Technology

IW : Information Warfare

LAN : Local Area Network

MitM : Man in the Middle Attack
NIDS : Network-based Intrusion Detection Systems
PPI : Pay per Install
OSI : Open Systems Interconnection
OSINT : Open Source Intelligence
OSN : Online Social Networks
OSS : Open Source Software
P2P : Peer-to-Peer
RAM : Random Access Memory
RAT : Remote Access Tool
SCADA : Supervisory Control and Data Acquisition
SCM : Supply Chain Management
SIEM : Security Information and Event Management
TCP/IP : Transmission Control Protocol/Internet Protocol
tDCS : Transcranial Direct Current Stimulation
TMS : Transcranial Magnetic Stimulation
UDP : User Datagram Protocol
UID : Unique Identifier
USB : Universal Serial Bus
VLAN : Virtual Local Area Network
WAN : Wide Area Network
XSS : Cross Site Scripting Attack

CHAPTER 1

1. INTRODUCTION

Cyberspace is different from the real world. This statement might not come as a surprise to anyone however it has to be stated nonetheless. Commonly held misconception about cyberspace is that it is stateless and belongs to everyone all at once, like air. While I agree on the point that internet is as essential as the air we breathe, it is not accurate to believe cyberspace to be stateless and borderless. Cyberspace exists within physical infrastructure of servers, routers, switches and computers, and it is made out of autonomous systems (AS). Tens of thousands of constantly shifting autonomous systems, connected together with the border gateway protocol (BGP) route connections, always trying to find closest AS to go through to lower latency of any connection (Fontugne, et al., 2019, p. 197). All this physical infrastructure tethers the cyberspace to physical realm. Contrary to physical realm however, propensity towards change lies at the very core of cyberspace. All the information contained within it is changeable. Therefore, the cyberspace itself may not have changed as a dimension since its invention, its content and rules certainly have. To quote P. W. Singer and Allan Friedman, "cyberspace of today is both the same as but also utterly different from the cyberspace of 1982" (Singer and Friedman, 2014, p. 14). Contrary to physical world once more, states are not the most powerful entities in cyberspace. Well-funded groups with sufficient technical expertise may do more damage than what a state actor could, as these groups are often not hindered with legal repercussions if the attacks cannot be directly attributed to them. Even individuals have the ability to disrupt computer network operations (CNO) in cyberspace, deny access to parts of it or outright extract classified information to sell to the highest bidder in underground parts of the internet called the Darknet. The balance of power in cyberspace is shifting however. The world has seen the effects of specialized computer network attacks (CNA) with the Operation Olympic Games (Sanger, 2012) or more commonly referred as Stuxnet and its later, espionage oriented variant nicknamed Duqu. Furthermore, the targeted cyber-attacks and advanced persistent threats are constantly evolving, costing industries in the millions, and due to attribution problems in cyberspace, attackers are practically getting away with it.

1.1 Scope of the Thesis

In this thesis, I examine cyber threat types to state and non-state actors by first establishing the definitions of cyberspace and pursuant terms all derived from cyber. Following this set goal, I also examine prominent targeted cyber-attack cases against state actors namely Stuxnet and its variant Duqu as well as the famous denial of service attack against Estonia through defining what kind of targeted and non-targeted cyber-attacks are they and their attack vectors, as well as discuss the recommend countermeasures against these types of attacks for the future.

To limit the scope of the thesis, targeted and non-targeted cyber-attacks as well as advanced persistent threats (APT) are only examined through a technical viewpoint. Literature research shows that cyberspace is a multidisciplinary field, ranging from computer science to international relations and international law. Literature research also points to a lack of technical understanding and examinations in international relations field concerning advanced persistent threats and state borne cyber weapons. Therefore, this thesis tries to establish that even surface knowledge of targeted and non-targeted cyber-attacks, terms and attack vectors, their propagation techniques, and some simple countermeasures against these threats could not only benefit individuals, may also affect state security as with any secure network, easiest component to hack are the human elements. Following the previously set boundaries, this thesis does not examine international law regarding cyber-attacks and cyberwarfare, and only takes computer science and international relations' perspectives into account.

1.2 Purpose

The purpose of this thesis is to establish the notion that cyberspace is a multifaceted and multidisciplinary global domain, encompassing state and non-state actors. Unlike previous works done in the international relations field concerning cyberspace, this thesis does not shy away from the technicalities of cyberspace and information communication technologies (ICT). International relations and states are moving towards such new horizons that five traditional domains land, sea, air, space, and cyber are not limited to their own

confines any longer. Nowadays militaries employ cross-domain maneuvers to project force and display their tactical prowess. Simply put, a drone operating out of a carrier positioned in international waters, deploying a computer guided missile, while communicating multitude of data to a remote computer via satellites in orbit is a perfect example for explaining what the term cross-domain maneuvers tries to convey. Expanding upon this trajectory, this work is formulated along the lines that in order to be an expert in the field of International Relations, studying one of the operational domains, one would have to be able to grasp all terms and their meanings in all the domains, from simple army terms to operational computer network infrastructures. Given that the mainstream theories have failed to predict the collapse of the Soviet Union, and international relations field has struggled to put forth a new theory to offer convincing explanations to paradigm shifts that happened following the collapse of the Soviet Union, this thesis therefore, does not take the views of these mainstream theories into account when examining and explaining its main subject: targeted and non-targeted cyber-attacks employing weaponized malware against state actors.

Chapters below will explain that cyber-attacks employ weaponized malware to reach a goal set by the attacker and will examine and explain how these weapons operate. In order to better understand security implications and challenges these weapons create, weaponized malware attack cases, namely the cases of Stuxnet and its variant Duqu will be the main focus of this thesis. This thesis does not try to implicate any state or non-state actor operating within the cyberspace as cyber-belligerents, the term attackers is simply used as a pronoun to refer to broad selection of corporate and non-corporate entities creating and seeding the said weaponized malware.

This thesis hypothesizes that states do not focus on cyber security education. Which in turn leaves cyber defense strategies lackluster and unable to provide solutions to the ever changing facets of security in the cyber realm. Building upon that premise, this thesis also hypothesizes that cyber weapons are now a reality and they are indeed different from the common malware found in the cyber realm. Currently, cyber weapon capabilities of states are unknown and without further research conducted on the subject, it would not be possible to provide cyber defense policies against cyber weapons developed and deployed by the state and non-state actors alike. Lastly, this thesis hypothesizes that security in cyber space is an ongoing process, meaning, no system could ever be completely secure. Air-gapped network

breaches show that even with proper security precautions, all actors, state or otherwise can be targeted by cyber weapons. In order to tackle this problem, states need to focus on eliminating the education and knowledge gap surrounding the cyber domain.

1.3 Outline

Chapter 2 defines cyber and the derivative terms through literature research on the related subjects.

Chapter 3 focuses on identifying aspects of targeted and non-targeted cyber threats.

Chapter 4 examines case studies of some of the more prominent cyber-attacks to date.

Chapter 5 examines current cyber policies being used in some of the highest cyber-vulnerable nations as well as international organizations.

Chapter 6 formulates and explores some of the future scenarios increasing cyberspace integration in human lives through advancements such as Brain Computer Interfaces (BCI) and augmented reality and concludes the thesis.

CHAPTER 2

2. DEFINITIONS

Cyber security, is a fairly new subject in the field of International Relations. The subject is active and healthy in the fields of information technologies and computer science due to immense speed new threats and attacks propagate across global networks, many experts are striving to protect all manners of information communication technologies from unauthorized access, tampering, or modification. From the international relation field's perspective, what is meant by the term cybersecurity, is still not clear enough. Literature research shows not only cybersecurity is defined differently by almost every researcher and state, the phenomenon also affects cyberspace, cyber weapons, cyberwarfare as well as cyber-attacks. This chapter of the thesis aims clear some of the confusion surrounding the subjects mentioned above by comparing definitions from the literature.

In the beginning of this work, it would be beneficial to construct what cyberspace is from ground up. Starting with the examinations of what cyberspace is, where it exists, and

how it interacts with the real world, situated on top that foundation then, its sub elements such as cybersecurity, cyberwarfare, cybercrime, and cyberattacks can be explained. With that said, in the field of International Relations, what is meant by the term security after the collapse of the Union of Soviet Socialist Republics (USSR), has undergone a change, which has gradually shifted the focus from state to individual with term human security being used increasingly. This shift also creates a different outlook on the subject of cyber security, even though the target of a cyber-attack can be a state-owned institution or infrastructure, bearing similarities with military warfare, it is often the individuals which are affected the most. In future chapters this thesis examines cyber-attacks in depth. However, with the shifting focus of referent object of security from states to individuals, this thesis will also discuss security of individuals in cyberspace.

2.1 Cyberspace

The term cyber has little meaning on its own beyond the belief that it is derived from an Ancient Greek verb κυβερεω (kybereo), meaning "to steer, to guide, to control or to govern" (Yan, 2019, p. 1). Current dictionary definition of cyber is: "of relating to, or involving computers or computer networks (such as the internet)" (http-11). What gives cyber its actual meaning are the following words it's used in conjunction with, namely space, warfare or attack.

The term cyberspace became popular with William Gibson's novel titled "Neuromancer". Even though he had used the term in his previous work titled "Burning Chrome", his definition of cyberspace in Neuromancer is what captured the essence of the term cyberspace.

> "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..." (Gibson, 1984, p. 51)

Billions of daily legitimate users in every nation, interacting with graphical representation of complex data constructed from different computer systems across the globe,

and displayed on even the smallest screens we can carry in our pockets nowadays, however metaphorical it may sound, is a fitting description of what cyberspace represents in its core, a dimension of data, with every device connected to it acting as a gateway and an oracle. Shaping and guiding the complex bytes to human consumable form.

Returning to the not-so-metaphorical definitions in the literature, Richard Clarke and Robert Knake's definition of cyberspace is "all of the computer networks in the world and everything they connect and control… cyberspace includes the Internet plus lots of other networks that are not supposed to be accessible from the Internet" (Clarke and Knake, 2010, p. 70). While cyberspace does encompass all computer networks whether they are connected to the internet or not, to clarify Clarke and Knake's definition, for computers system to exist in cyberspace, they need not belong to the internet. In fact, the Internet is a subset of the cyberspace, metaphorically, it is merely a collection of bookmarks, where computers are identified through their assigned Internet Protocol (IP) addresses, recalled by the domain names these bookmarks are branded with, all kept within the confines of the Domain Name Server (DNS) Root, the Internet Assigned Numbers Authority (IANA). The Internet facilitates only the connection between two computer systems.

The United States Department of Defense (DOD), known for being the creator of the ARPANET, which has eventually blossomed into the Internet has also struggled with defining what cyberspace is, and they have broadened their definition of cyberspace in 2006 with the following:

> "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers" (Mazanec and Thayer, 2015, p. 13).

P. W. Singer and Allan Friedman define the cyberspace in simpler terms, "cyberspace is the realm of the computer networks (and the users behind them) in which information is stored, shared, and communicated online" (Singer and Friedman, 2014, p. 13).

Albeit more technical, on the opposite end of the simple spectrum Daniel Kuehl defines the cyberspace as:

> "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." (Robinson, Jones, and Janicke, 2015, p. 72)

It is one of this thesis' goals to provide technical background on cyberspace and Kuelh's definition of cyberspace is sufficiently clear to everyone involved in the multidisciplinary field of cyberspace and cybersecurity. Further dissection of the term from differing literature would only serve to muddy the waters and therefore this thesis accepts Kuehl's definition as the definition of cyberspace for the remainder of this work.

Table 2.1 tries to summarize some of the definitions already covered within this section as well as some other definitions found in literature which are not discussed above.

Table 2.1. *Literature definitions of cyberspace*

Author	Definition
Clarke and Knake	All of the computer networks and everything they connect and control
US DoD	Global domain of information environment of interdependent networks of IT infrastructure
Singer and Friedman	Realm of information storing, sharing and communicating computer networks
Alison Lawlor Russell	"Cyberspace is a physical domain created by the information systems that enable electronic interactions to occur" (Russell, 2014, p. 2).
Kuehl	A global domain of information which uses electronics and electromagnetics to create, store, modify, exchange data in interdependent networks

2.2 Cyber Weapons

Dictionary definitions of a weapon is (1) "a thing designed or used for inflicting bodily harm or physical damage" and (2) "a means of gaining an advantage or defending oneself in a conflict or contest" (http-20). Contrasting the physical harm to humans or infrastructure requirement for weapons in cyber environment, only those with the ability to alter data integrity in infiltrated systems could be classified as weapons. Up to this point however, there have been no confirmed bodily harm or loss of life cases through actions perpetrated by

computer code in cyberspace. By this definition, most of the targeted cyber-attacks and advanced persistent threats are simply espionage tools and are not classified as cyber weapons. Jacqueline Eggenschwiler and Janje Silomon in their work titled "Challenges and opportunities in cyber weapon norm and construction", report Thomas Rid and Peter McBurney's definition of a cyber weapon as "computer code that is used or designed to be used with the aim of threatening or causing physical, functional or mental harm to structures, systems, living beings" (Eggenschwiler and Silomon, 2018, p. 12). This thesis adopts this definition of a cyber weapon, a collection computer code that intends to harm data integrity, physically connected devices and/or their operators or their dependents.

Literature research shows that a belief that cyber weapons could either bring armageddon, or come very close to it, is quite common within the field of International Relations. Richard Clarke and Robert Knake argue that "cyber warriors can get into these networks and control or crash them. If they take over a network, cyber warriors could steal all of its information or send out instructions that move money, spill oil, vent gas, blow up generators, derail trains, crash airplanes, send platoon into an ambush, or cause a missile to detonate in the wrong place" (Clarke and Knake, 2010, p. 70). Focusing on the most destructive foresight in their gloomy outlook of a network intrusion painted by Clarke and Knake first, altering missile path alone would require extensive insider knowledge into military hardware and may even require access to the source code. In the case of Stuxnet, the weapon intercepted and modified the data reported back to monitoring station while the gas centrifuges were literally spinning out of control, lulling the operators and engineers in a false sense of security. It was able to perform this task by replacing the monitoring function of the programmable logic controllers (PLC) with the code it contained (Falliere, O Murchu, and Chien, 2011, p. 36). Contrasting Stuxnet with the missile scenario described by Clarke and Knake, an attacker would have to know the code responsible for the missile control to manipulate it, infect one of most secured and scrutinized network types with connections to the internet with malware, and lie in wait for that opportune moment to strike and take control of a missile in flight. In the last 10 years since the inception of Stuxnet, malware sophistication and stealth attack vectors have risen, but not yet to the point of being able to alter missile paths without prior access to the code responsible for the operation of a computer guided missile system.

Coming close to one of the scenarios described by Clarke and Knake, there has been a reported case of spillage due to cyber sabotage. While not exactly an oil spillage as described by the Clarke and Knake, Vitek Boden, was able to spill more than a million liters of raw sewage into local parks, rivers and even to a hotel with the motive of revenge. It is worth noting that he was the employee of the company that had installed the supervisory control and data acquisition (SCADA) systems at Maroochy Shire sewage pumps and treatment plants in Queensland/Australia, thus had prior insider knowledge into how said SCADA systems were operated. Boden's revenge plot may have spilled millions of liters of raw sewage, but he had accomplished this task with only his laptop and radio equipment to take control of 150 pumping stations instead of developing and deploying cyber weapons (Rid and McBurney, 2012, p. 10).

One of the most effective cyber weapons to be deployed against a state is known to be the Stuxnet. Highly selective targeting coupled with no propensity towards collateral damage is also what makes it one of the most intelligent cyber weapons to date. However, Stuxnet is not actually an intelligent piece of software, unlike many other software designed to learn, Stuxnet could not learn, it used preset parameters to select its targets and initiate its infection routines. This predictability is what limits the collateral damage of cyber weapons, as a break in the infection chain could render the malware inoperative. Security researchers in the field have been forecasting the advent of self-learning malware. A global security strategist, Derek Manky, had predicted the self-learning cyber-attacks could become reality as soon as 2018. According to Manky, traditional botnets could be replaced by hivenets and swarmbots which are intelligent clusters of compromised devices able to target and compromise other vulnerable systems with self-learning abilities. Extending upon this, Manky also reports that already existing computer generated malware based on automated vulnerability detection could be improved by the artificial intelligence (AI) resources to generate additional malware variations to evade already in place security systems (Manky, 2017).

2.3 Cyberwarfare

Literature research reveals various definitions for the concept of cyberwarfare as a term. Given that warfare is usually a domain of international relations and international law, this chapter focuses on definitions provided by researchers in these fields. Following chapters

will explore the ways cyber-attacks can infiltrate networks and modify or exfiltrate data in detail, so far however, there have been no loss of life through cyber-attacks which might also constitute as an armed attack according to the Charter of the United Nations.

Jon R. Lindsay in his work titled "Stuxnet and the Limits of Cyber Warfare" defines cyber warfare as an action that "employs computer network attacks as a use of force to disrupt an opponent's physical infrastructure for political gain. This includes military cyber operations that degrade enemy data processing to facilitate an integrated assault during wartime" (Lindsay, 2013, p. 372).

Richard Stiennon's definition of cyber warfare from the state actor perspective is as follows:

> "Cyber warfare is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived)" (Stiennon, 2015, p. 8).

This definition includes the non-state actors on the condition that they are either supported by states or very well-funded. Given that price ranges for Zero-Day (0-day) vulnerabilities being sold in Darknet circles range from under $1,000 to over $100,000 (http-12) the cost of developing a Stuxnet type of cyber weapon is high and once 0-day vulnerabilities are discovered, they are subsequently patched, thus eliminating the attack vectors of the weapon. The attractiveness of nuclear programs today suggest that even after the Non-Proliferation Treaty, states do not shy away from developing single-use weapons as a means of deterrence. However unlike atomic bombs, a cyber weapon can be reverse engineered by not only state actors, also by the non-state actors with sufficient technical expertise. This however should be taken as that every cyber weapon can be used as a blueprint for more weapons. Chapters below examine how some notorious cyber weapons operated and argue that every cyber weapon is effectively only against what it is designed to infiltrate or sabotage.

As this work is completed within the confines of international relations field, Stiennon's cyberwarfare definition is amply clear at conveying the requirements of cyber warfare. This thesis does not aim to speculate whether an all-out cyberwarfare could erupt at

any given time, it rather considers cyber warfare as an area best left to the fields of international law and international organizations. Given that states operate in a timeline different to humans and international law has to be ratified by individual states, and the recency of the cyber revolution drags the cyber warfare into uncharted waters.

2.4 Cybercrime

In accordance with the preset boundaries, this thesis does not refer to actors undertaking cyber-attacks as cyber criminals due to fact that crime is an action which is prosecutable by states dependent on their own laws. Considering the multidisciplinary nature of the cyberspace, comparing some of the transnational definitions of the cybercrime may be beneficial to clear some of the confusion surrounding the definitions of terms used in conjunction with the term cyber. Expanding upon this outlook, this section tries to limit the discussion of cybercrime to international organizations' definitions to avoid further confusion which may be caused by individual states' subjective definitions.

The United Nations Office of Drugs and Crime (UNODC) following the General Assembly's resolution 65/230 and two resolutions from the Commission on Crime Prevention and Criminal Justice, 22/7 and 22/8 tries to assist member states in cybercrime-related affairs by defining cybercrimes with broad terms such as "cyber-dependent" and "cyber-enabled" offences along with specific crime types, namely "online child sexual exploitation and abuse" (http-2). Extending upon these descriptions, the UNODC states that "cyber-dependent crime requires an Information Communications Technologies (ICT) infrastructure and is often typified as the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure, (e.g. the cyber-takeover of a power-plant by an organized crime group) and taking a website offline by overloading it with data (a DDOS attack)" (http-2). Secondly, UNODC accepts cyber-enabled crime as "crime is that which can occur in the offline world but can also be facilitated by ICT. This typically includes online frauds, purchases of drugs online and online money laundering" (http-2). Lastly, UNODC accepts "child sexual exploitation and abuse includes abuse on the clear internet, Darknet forums and, increasingly, the exploitation of self-created imagery via extortion – known as sextortion" (http-2).

Following on the definitions set by the United Nations, the European Commission on Migration and Home Affairs, tries to tackle the definition of cybercrime in three broad categories. "(1) Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts). (2) Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code. (3) Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia" (http-1).

As the above definitions accepted by two prominent international organizations show, unauthorized network intrusions and advanced persistent threats against secured networks as well as industrial control systems (ICS) are considered as cybercrime. However, as mentioned above, this thesis does not examine the international law aspects of the cyberspace and therefore will refer to perpetrators of cyber-attacks as cyber attackers henceforth.

2.5 Cyber Attacks

From the perspective of the international law and International Relations fields, the term attack is a complicated subject. Indeed, even the United Nations did not try to define the term "attack" when it was initially drawing up the Charter of the United Nations. The following excerpt from the Charter of the United Nations concerning self-defense permits the use of force during an 'armed attack' with these words:

> "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security" (http-21).

According to the Charter of the United Nations, self-defense, or more specifically, the retaliatory use of force, is something that states inherently possess in the event of an armed

attack and any action should be reported to the Security Council. Within the confines of physical realm, attributing an armed attack is often immediately possible with the exception of unlawful combatants and proxy warfare. Cyber-attacks however are almost impossible to attribute with any degree of certainty which would permit the use of retaliatory force. The attribution problem coupled with the previously mentioned fact that all data within cyberspace can be manipulated, no state could reliably accuse another state without solid proof originating from out of cyberspace.

Estonia's adversaries had exploited the cyberspace reliance of Estonia to a degree that almost crippled the information, media, and finance as well as governance services for three weeks during the fateful spring of 2007. Following these events, NATO had organized a cyber command initiative designated "Cooperative Cyber Defence Centre of Excellence" (CCDCOE) situated within Estonia, Tallinn. One of the most prominent outputs of this initiative was the "Tallinn Manual on the International Law Applicable to Cyber Operations" and the following 'upgrade' of this work titled "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations". It should be noted that these operational manuals are just manuals, and they are non-binding for any member of NATO. The manual defines the cyber-attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmitt and Vihul, 2017, p. 415). So far, there hasn't been any cyber-attack with reported human life loss however, as one of the chapters of this thesis discusses and formulates, future cyber integration may finally bring forth just that however considering the current situation of cyber-attacks, this definition needs to be updated with a few additions. As previously defined in the earlier sections, a cyber weapon could be deployed to recover, alter, or otherwise harm data integrity. After the invention and proliferation of hand held communication devices, or smart phones, human-data interaction has reached peak levels. Given this peak interaction levels, threats and attacks towards data integrity for all systems containing or processing data should also be considered within the bounds of this term. For the remainder of this work, constructing from these points put forth, definition of a cyber-attack will be considered as: "a cyber operation, conducted offensively or defensively to injure or terminate humans, damage or destroy objects, damage, alter, destroy or exploit data integrity through the use of cyber weapons or cyber enabled implements".

2.6 Cybersecurity

In the field of International Relations, term "security" has shifted in meaning following the collapse of the Soviet Union. Initially representing the security of the state, lately, it has shifted to represent the security of individuals or more popularly coined as human security. Literature research yields surprising results for the term cybersecurity. Researchers in International Relations often consider states as the referent object for the term cybersecurity and try to apply previously formulated theories in the field such as "deterrence". In conjunction with the goals of this thesis, it should be noted that the only hundred percent effective solution to cyber-attacks is to shut down all computers and never operate anything remotely technological ever again. Beyond these measures, there are not any other effective ways to remain cyber secure in the globally connected nature of the Internet. And as long as technology continues to develop and update, it can be stated with certainty that, no system will ever be hundred percent safe in the cyberspace. Within this section, this thesis examines some of the more prominent definitions of cybersecurity, however when these definitions are examined, previously mentioned characteristics of the cybersecurity should also be taken into account.

George Christou in his work titled "Cybersecurity in the European Union Resilience and Adaptability in Governance Policy" reports the European Union's cybersecurity definition from the EU Cyber Strategy Document as:

> "The safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein" (Christou, 2016, p. 7).

In 2010, a memorandum addressed for "Chiefs of the Military Services, Commanders of the Combatant Commands, and Directors of the Joint Staff Directorates" (http-23) happen to include the lexicon for almost all cyber related terms to bring the Chiefs of Staff up to speed with the ever-changing cyberspace with the following definition:

> "All organizational actions required to ensure freedom from danger and risk to the security of information in all its forms (electronic, physical), and the security of the systems and networks where information is stored, accessed, processed, and transmitted, including precautions taken to guard against crime, attack, sabotage, espionage, accidents, and failures. Cybersecurity risks may include those that damage stakeholder trust and confidence, affect customer retention and growth, violate customer and partner identity and privacy protections, disrupt the ability to conduct or fulfill business transactions, adversely affect health and cause loss of life, and adversely affect the operations of national critical infrastructures" (http-23).

The United States of America's National Initiative for Cybersecurity Careers and Studies (NICCS) which also includes the United States Computer Emergency Readiness Team, defines cybersecurity in their lexicon as the following:

> "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (http-22).

What all these definitions have in common is that their referent objects are not states, nor are they individuals. Their referent objects are computer systems, trust on data integrity and continued operability of national critical infrastructures, collective policies, and technologies. This in turn eliminates the possibility of adapting the old theories such as deterrence or mutually assured destruction to serve a similarly same purpose. As case studies show, costs of developing cyber weapons surpass the costs of traditional weapons of the other four domains. And thus far, only one cyber weapon actually fits within the definitions of cyber warfare or even cyber-attack, the Stuxnet. It should be noted that cyber weapons offer flexibility, plausible deniability and achieve a desirable outcome without the bloodshed.

CHAPTER 3

3. CYBER THREATS

In recent years, the term "cyber-attack" almost became synonymous with the denial of service attacks (DoS) due to their proliferation in cyberspace. DoS attacks happen globally and frequently, however they are not the greatest threat posed to state and non-state actors as well as individuals in cyberspace. In accordance with the thesis' main goals, this chapter aims to explain cyber security threats and their significance towards state and non-state actors while staying technically informative and clear.

Cyber threats can be categorized in two specific categories. Targeted and non-targeted cyber-attacks. According to Aditya K. Sood and Richard Enbody, targeted cyber-attacks are defined as "dedicated attacks that aim at a specific user, company, or organization to gain access to the critical data in a stealthy manner" (Sood and Enbody, 2014, p. 2). Deriving the opposite of the targeted attacks, non-targeted attacks can be defined as the non-discriminatory attacks conducted with the intent to affect as many computer systems/networks as possible. Targeted cyber-attacks, due to their nature, are not as much proliferated in cyberspace as compared to non-targeted vulnerability seeking and exploiting attacks. Due to multidisciplinary nature of the cyberspace, in order to better understand the security challenges both targeted and non-targeted cyber-attacks pose in cyberspace to state and non-state actors, one would need to be able to identify and distinguish between these types of attacks.

3.1 Targeted Cyber-Attack Vectors

Sood and Enbody in their work titled "Targeted Cyber Attacks" define some of the important characteristics of targeted cyber-attack vectors. In their definition a targeted cyber-attack tries to hide itself using zero-day exploits and previously unknown vulnerabilities, while being custom written to avoid present security software as well as hide the identity of the attacker, and only go after specified targets while not infecting low value targets to avoid exposure, all while executing said attack operations stealthily (Sood and Enbody, 2014, pp. 2-3).

3.2 Advanced Persistent Threats

Targeted cyber-attacks are a subset of a much larger category labelled "Advanced Persistent Threats" (APT). The United States National Institute of Standards and Technology defined advanced persistent threats as:

> "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives" (National Institute of Standards and Technology, 2015, pp. B-1).

Both targeted cyber-attacks and advanced persistent threats require a high degree of funding and technical expertise to achieve their goals. However, neither are strictly dependent on state funding and oversight. The initial Stuxnet infection has shown to have used stolen digital certificates to sign the modified driver files required for the malware's operation (Falliere, O Murchu, and Chien, 2011, p. 3). These digital certificates are kept under high levels of physical security and require physical access to obtain, and the physical proximity of the companies owning said certificates implies state level intelligence operatives within the organization responsible for developing and deploying the Stuxnet. Literature research shows that some researchers suggest that all APTs fall under state sponsored category however well-funded non-state actors could obtain zero-day exploits from Darknet to essentially hide their custom tailored malware. Zero-day exploit prices in the Darknet range from under $1,000 to over $100,000 (http-12). Stuxnet is known to have used four zero-day exploits to penetrate targets and propagate, and updated itself through peer-to-peer (P2P) networks (Falliere, O Murchu, and Chien, 2011, p. 2).

APT campaigns are designed especially for their targets and are operated with clear goals. In limited range and exposure over a long period of time ranging from months to years,

governments, highly prized intellectual properties are often the targets of these attacks. The FireEye report in 2013 found that education, finance, high-tech industries, government, consulting firms, energy companies, telecommunication entities, healthcare facilities and aerospace industries are the top ten choices for APT campaigns (Chen, Desmet, and Huygens, 2014, p. 64).

Table 3.1. *History of Targeted Attacks (or APTs) (Sood and Enbody, 2014, p. 6)*

Classification	Date	Zero-Day	Targets
Ghost Net	March 2009	Yes	Dalai Lama's Tibetian exile centers in various countries as well as ministries of foreign affairs
Aurora	January 2010	Yes. Internet Explorer and Perforce software were exploited.	~34 U.S. Companies including Google, Juniper, Rackspace, etc.
Stuxnet	June 2010	Four zero-day exploits were used along with a known vulnerability	Iranian nuclear facilities using Siemens infrastructure
RSA Breach	August 2011	Yes. Exploited Adobe Flash Player	RSA and defense contractors using RSA security solutions
Duqu	September 2011	Yes. MS Word True Type font vulnerability	Worldwide ICSs
Nitro Attack	July 2011	Yes	~29 chemical companies
Taidoor Attack	October 2011	~9 known vulnerabilities were used	US/Taiwanese policy influencers
Flame (SkyWiper)	May 2012	Yes. Terminal Service licensing component was exploited to generate rogue certificates	Cyber espionage in Middle Eastern companies

Table 3.1 shows some of the known targeted cyber-attacks as well as advanced persistent threats and their targets along with the vulnerabilities.

3.2.1 Stages of Targeted Cyber-Attacks and Advanced Persistent Threats

According to Sood and Enbody, targeted cyber-attacks go through five different stages of operation in their lifetime. They define these five stages as "intelligence gathering, infecting the target, system exploitation, data exfiltration, maintaining control and network access" (Sood and Enbody, 2014, pp. 6-8). Comparatively, APTs also share similar attack stages during their campaigns. Chen, Desmet and Huygens define APTs phases in 6 steps. Reconnaissance and weaponization, payload delivery, initial intrusion, command and control, lateral movement, and finally data exfiltration (Chen, Desmet, and Huygens, 2014, p. 65). This section tries to explain commonalities shared between both definitions of targeted cyber-attacks and advanced persistent threats' stages.

3.2.1.1 Reconnaissance and weaponization

Also known as "target intelligence gathering" is the stage when a target is discovered and selected for a cyber-attack. Information about target is gathered through sources such as Online Social Networks (OSN), public governmental records or from websites that hold pertinent information about the target. Throughout the information gathering process, attacker may use different intelligence collecting methods. Not to be confused by the open source software, Open Source Intelligence (OSINT) is performed through gathering intelligence from sources open to access. Cyber Intelligence (CYBINT) implies the use of internet sources such as search engines or already compromised networks related to targets to gather data. Finally, Human Intelligence (HUMINT) uses human interaction to gather data about the target.

When sufficient data have been collected, sifting process can begin. Related information such as personal or historical data, relationships and contacts, geographical location about the target can be categorized and analyzed. It is worth noting that data varies according to the target. Targets range from single individuals to large organizations. With the data gathered and sifted through, resource correlation and information processing can begin to lay out relationship data to identify and exploit the target's environment and behaviors.

Finally, an attack is modelled and correlated with the information gathered thus far, using methods such as spear phishing (Sood and Enbody, 2014, pp. 11-16).

3.2.1.2 Payload delivery

Following the intelligence gathering process, an attacker begins the process of infecting its target in order to install Remote Access Tools (RAT) to exploit the systems belonging to target's network. An attacker may employ two distinct attack types to achieve his or her goals; direct and indirect attacks.

Direct attacks try to exploit target network vulnerabilities discovered in the intelligence gathering phase to gain access to critical systems or pave way for the indirect attacks through identifying which indirect attack would be more successful through comparative analysis of web vulnerabilities of the target network. *Indirect attacks* are layered attacks employing components such as social engineering or phishing emails with malicious attachments/links or by waterholing to gain access to critical systems and networks through exploiting individuals' browsing habits (Sood and Enbody, 2014, pp. 23-24).

During the infection phase, an attacker may employ several attack models to gain access to critical systems, such as social engineering, phishing emails, waterholing along with vulnerability exploitation, automated exploit frameworks and advanced malware such as rootkits.

Social engineering is an attack method that exploits human weaknesses, namely gullibility and ignorance. An attacker may deceive targets into breaching their own security or revealing sensitive information about their networks (Smith, Papadaki, and Furnell, 2013, p. 249).

Spear Phishing refers to an attack model targeting only a select group of recipients with fraudulent emails containing malicious links or attachments disguised and personalized for the targets to increase the odds of success (Chen, Desmet, and Huygens, 2014, p. 66). In what is also referred as a drive-by download attack, users are coerced into visiting short-lived malicious domains usually operated by the attacker via links embedded in the emails sent by the attacker (Sood and Enbody, 2014, p. 27).

Watering Hole/waterholing attacks are traps laid out for the internet users based on their browsing habits. An attacker compromises a third party webpage frequented by the

targets and infects the said page to deliver a payload intended for their targets (Sood and Enbody, 2014, p. 30).

An attacker may employ a more direct payload delivery approach with Universal Serial Bus (USB) devices such as removable flash drives already infected and delivered to target's premises. An employee may find one of these drives laying around premises and plug them in their computers with the intention to find out the owner and return it. However most computer systems are set to automatically execute the contents of a flash drive upon plugging in. At that point, payload is already delivered and the infection phase succeeds (Sood and Enbody, 2014, p. 32).

3.2.1.3 Initial intrusion and system exploitation

Following the payload delivery, in this phase an attacker successfully infiltrates the target's network. Typically, two types of exploit launch pads are used during this phase of the campaign: Browser-based exploits and document-based exploits. Browser-based exploits try to exploit vulnerabilities found in browsers such as Internet Explorer whereas document-based exploits try to exploit the vulnerabilities found in document authoring environments such as Microsoft Office or Adobe PDF in order to deploy Remote Access Tools (RAT) on target computer to maintain access (Chen, Desmet, and Huygens, 2014, p. 67).

Browser Exploit Packs are a software solution that bundles exploits for known as well as unknown (zero-day) vulnerabilities in browser software environments including third party software included within the browsers. Completely automated with no manual input required, BEPs reduce the workload of attackers by automating the initial intrusion process (Sood and Enbody, 2014, p. 40).

A *zero-day vulnerability* is a vulnerability that is currently unknown and therefore remains unpatched by software developers. Depending on the vulnerability window of a successful remote executable, zero-day exploits can be a huge benefit for an attacker to circumvent an already established cyber defense perimeter based on known vulnerabilities. Even if the vulnerability is discovered and later patched, the dissemination window of patches may take up to months or years in the case of systems in constant operation where downtime is usually unacceptable. Therefore, even if zero-day vulnerabilities are found and patched, they are still present in some systems and are still valid attack vectors for the initial

intrusion phase of the both targeted cyber-attacks' and advanced persistent threats' campaigns (Sood and Enbody, 2014, pp. 41-42).

After the initial incursion into the target computer/networks, a foothold needs to be established to remain in the network. This step requires backdoor malware or RATs which can connect back to a command and control server, giving the attackers unfettered access (Chen, Desmet, and Huygens, 2014, p. 67).

3.2.1.4 Command and control

In this phase of the campaign, attackers use command and control techniques to exploit the network further, using various tools ranging from legitimate online services to publicly available toolkits to commercial exploitation tools. An attacker may program their malware to seek out commands from an account registered in OSNs through updates or blog posts; configure inbound connections through TOR anonymity networks to avoid blacklisting or identification of both the attacker and the intrusion; deploy legitimate or otherwise remote access tools operating with server-client parameters. While not limited to these categories, most APT campaigns' command and control phases revolve around these mechanisms to carry the campaign to next stage (Chen, Desmet, and Huygens, 2014, p. 67). Further avoiding detection, command and control servers are often categorized in three separate categories: Centralized, decentralized and hybrid command and control servers.

The concept of *centralized command and control servers* implies that malware is controlled by a single server entity. This leaves the malware vulnerable to DNS blacklisting upon discovery as was in the case of the Stuxnet worm. Designed to mitigate DNS blacklisting, *decentralized command and conquer servers* employ every instance of the malware as a command relaying mechanism through P2P connections. Finally, *hybrid command and control servers* are designed to have best of both worlds. They can use either method as a fallback mechanism should the primary control method fails to establish a connection back to master server (Sood and Enbody, 2014, p. 87).

3.2.1.5 Lateral movement

During this phase of the operation, attackers expand their incursion within the breached network in order to locate and extract valuable data through "performing internal

reconnaissance to map the network and acquire intelligence; compromising additional systems in order to harvest credentials and gain escalated privileges; identifying and collecting valuable digital assets, such as development plans or trade secrets" (Chen, Desmet, and Huygens, 2014, p. 68).

3.2.1.6 Data exfiltration

Once the target data is located and acquired by the attackers, exfiltrating this data becomes the final step in the campaign. Depending on how the malware designed by the attacker, data marked for exfiltration may choose differing methods to reach back to command and control servers. Recent malware families show preference towards Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secured (HTTPS) protocols to exfiltrate data as most firewalls securing organizations allow HTTP data to pass through. HTTPS also allows for content to be encrypted and without deep packet inspection method to analyze the said packets created by end users' systems, IT administrators cannot discover the contents. The data exfiltration techniques are not limited to HTTP protocols, alternative protocols such as File Transfer Protocol (FTP), P2P connections, Secure Shell (SSH) protocol, Simple Mail Transfer Protocol (SMTP), and even DNS queries can be programmed to transmit encrypted data. However, FTP, SSH, SMTP protocols are often monitored the most within a secure environment, which explains the rise of popularity of HTTP as a main data exfiltration option in the recent malware families (Sood and Enbody, 2014, pp. 86-90).

Table 3.2. *Comparison of Different APTs (Chen, Desmet, and Huygens, 2014, p. 69)*

Name	Operation Aurora	RAS Breach	Operation Ke3chang	Operation SnowMan
Active Time	June 2009 – December 2009	Unknown – March 2011	May 2010 – December 2013	Unknown – February 2014
Reconnaissance and Weaponization	Employee's emails, zero-day exploits, backdoor, and C&C tools	Employee's emails, zero-day exploits, trojanized docs, backdoor, RAT	Officials' emails, trojanized docs, backdoor, and C&C tools	Identify weakness in vfw.org, RAT, backdoor
Delivery	Spear phishing (malicious links)	Spear phishing (malicious XLS file)	Spear phishing (malicious zip file)	Watering hole attack (compromise and infect vfw.org)
Initial Intrusion	Drive-by download	XLS vulnerability	Targets open the executable file	Drive-by download
Command and Control	Custom C&C protocol, operating on TCP port 443 (HTTPS)	Poison Ivy RAT	Custom C&C protocol based on HTTP protocol	ZxShell, Gh0st RAT
Lateral Movement	Compromise SCM and obtain source code	Perform privilege escalation, gather SecureID data	Compromise internal systems, collect data	Unknown
Data Exfiltration	Upload data to C&C servers	Compress, encrypt data as RAR files, use FTP for transmission	Compress, encrypt data as RAR files	Unknown, could be US military intelligence

Table 3.2 compares discovered advanced persistent threats' campaign stages. As the common delivery methods indicate, personalized spear phishing is the favored delivery method for APTs that implies security awareness training is a must for all employees and potential targets for APT attacks.

3.2.2 Countermeasures Against Targeted Cyber-Attacks

3.2.2.1 Three approaches to security

Advanced persistent threats are both costly attacks often easy to miss by IT administrators and hard to eradicate once a foothold has been established by attackers within the secure network. Many attack methods and intrusion points mean that APTs cannot be solved by catch-all measures nor can they be stopped just by IT professionals acting diligently. Sood and Enbody categorize targeted cyber-attacks countermeasures in three categories: user centric study, end system security, network level security (Sood and Enbody, 2014, pp. 128-130).

"User centric security" implies that users operating end systems should be made aware of threats posed by the targeted cyber-attacks as well as advanced persistent threats. There are certain methods to improve user behavior in secured network environments through training. Safe computing practices need to be drilled into users, prompting them to use stronger unique passwords changed at regular intervals. If possible at all, users should be encouraged to use virtual machines (VM) for their browsing needs so that drive-by attacks cannot compromise the host system. It is also worth noting that often sophisticated malware tries to avoid being analyzed by security professionals and thus will react differently when confined in a virtual environment. Information security standards should be instilled in users to avoid information loss through phishing. Users should be discouraged from using their own USB devices within the secure network to avoid malicious codes from breaching the network (Sood and Enbody, 2014, p. 129).

Educating users about the dangers and costs of the APT needs to be complimented with up to date computer systems with end system security countermeasures. Operating systems, third party applications, need to be patched to their respective latest versions. As mentioned above, for browsing purposes, virtual machines should be employed to protect host computer from drive-by downloads and malicious websites. Even with these steps achieved, an anti-virus software should still be deployed to protect against known malware exploiting vulnerabilities (Sood and Enbody, 2014, p. 128).

Lastly, network level security implies the employment of network level security tools such as intrusion detection systems (IDS) and intrusion protection systems (IPS) and properly

configured firewalls to block known malware command and control servers from being resolved by DNS requests and monitor network traffic to detect and terminate anomalous network traffic. Proper encrypting of sensitive data to prevent man-in-the-middle (MitM) attacks on data flow using SSL technology along with diligent server and firewall logs reading done by network administrators, helps mitigate data loss and malicious code propagation. Lastly, networks and users should be segregated within virtual local area networks (VLAN) with network attached devices such as printers, routers, access points properly secured and maintained to harden against lateral movement of APTs and targeted cyber-attacks (Sood and Enbody, 2014, pp. 129-131).

Table 3.3 contrasts attack methods with preventive countermeasures during each stage of the APT attack.

Table 3.3. *Attack methods and countermeasures in each stage of an APT attack (Chen, Desmet, and Huygens, 2014, p. 71)*

Stage	Attack Method	Countermeasure
Reconnaissance and Weaponization	OSINT, Social engineering, Malware preperation.	Security awareness training, Patch management, Firewall
Delivery	Spear Phishing, Watering hole attack	Content filtering software, NIDS, Anti-virus software
Initial Intrusion	Zero-day exploits, Remote code execution	Patch management, HIDS, Advanced malware detection
Command and Control	Exploiting legitimate services, RAT, encryption	NIDS, SIEM, Event Anomaly detection
Lateral Movement	Privilege Escalation, Collecting data	Access Control, HIDS, NIDS, Event Anomaly detection
Data Exfiltration	Compression, Encryption, Intermediary Staging	Data Loss Prevention

3.2.2.2 Open Source versus Propriety Software

As mentioned earlier in the previous chapters, zero-day vulnerabilities are one of the most commonly exploited vulnerabilities currently threatening security in cyber domain. However, this is due to limited number of software developers trying to cope with the development and release cycles of software as efficiently as possible, leaving vulnerabilities

such as zero-days undiscovered and unpatched. Mentioned earlier in the initial intrusion section, a patch for a zero-day vulnerability may take up to a year to distribute to all users. Leaving most of the computers worldwide vulnerable. Critical infrastructures are systems that are required to be operational with as much downtime as possible. In today's modern world, almost all technological devices run on some sort of propriety or open source software. Sometimes both at the same time.

It would be beneficial to identify two types of software types, before comparing them from a security-conscious viewpoint. The term *open source software* (OSS) is defined by opensource.com, a website owned and operated by RedHat, a well-known open source enterprise software solutions company within the Linux community, as "software with source code that anyone can inspect, modify, and enhance" (http-33). Opensource.com also defines the *propriety software* as the software with its source code only available to the creators or its exclusive maintainers, restricting everyone else from viewing and altering the source code legally (http-33). From the security standpoint, this results in opposing outlooks on the software engineering as a whole. On one hand, the use of propriety software means excluding leaks, only through reverse engineering could propriety software's source code could be attained. This may lead software developers to a false sense of security and encourage wrongful thinking that their software cannot be exploited unless its source code were to be revealed. On the other hand, open source software provides faster discovery, better vulnerability protection due to faster patch deployment opportunities however requires far greater computer systems knowledge, as ability to read, alter, and recompile[1] source code demands more human resources for state and non-state actors. To be explained further in the case study of Stuxnet, only a single component of Siemens Step 7 software, responsible for data synchronization between the programmable logic controller and the host computer running Microsoft Windows operating system was targeted (Falliere, O Murchu, and Chien, 2011, p. 36). After reverse engineering was complete, a small worm was able to destroy 1,000

[1] The Linux Information Project defines compiler as "a specialized computer program that converts source code written in one programming language into another language, usually machine language (also called machine code) so that it can be understood by processors (i.e., logic chips)" (http-36). Recompiling process implies that after necessary alterations performed upon the source code, a developer may initiate compilation process once more, in order to incorporate newly written changes to the software.

gas centrifuges while lulling Natanz Fuel Enrichment Plant's operators to a false sense of security by providing false information.

Open source software thrives on being open and accessible by everyone. One of the greatest advantages it brings is the speed through which an operator may be able to deploy countermeasures against recently discovered exploits. Instead of waiting for vendors to patch vulnerabilities, an in-house programmer could deploy a patch for affected systems in a matter of hours instead of weeks or months. As Linux community demands code review in its open-source community, community is an essential part of identifying errors, bugs, and vulnerabilities (Gediya, Singh, Kushwaha, Srivastava, and Wang, 2019, p. 227). Indeed, community's approach towards code being reviewed by many members can be explained by the expression that "many hands make light work". While security, especially in the cyber domain may be far from light work, ability to review, alter, and recompile source code anytime is a must for rapid response against discovered vulnerabilities and exploits to keep the cyber enabled critical infrastructure secure.

Stuxnet was initially discovered by a small Belorussian company, named VirusBlokAda, on June 17, 2010 (Falliere, O Murchu, and Chien, 2011, p. 4). The exploited zero-day vulnerabilities were acknowledged by Microsoft almost a month later on July 16, 2010 (http-34). Microsoft then released a patch for one of the vulnerabilities Stuxnet exploited in August 2, 2010 (http-35). This timeframe given to counter an exploit for a propriety software should be unacceptable for any critical infrastructure systems. Given that the literature criticizes the lack of protective measurements imposed on the critical infrastructures and foresees apocalypse level destruction due to loss of said critical systems, state actors may find that employing open-source technologies in their critical infrastructures to be beneficial to their overall cyber security.

3.3 Non-Targeted Cyber-Attacks

Contrary to targeted cyber-attacks, non-targeted cyber-attacks do not distinguish between targets. These attacks often present themselves through casting a wide-net. These attack types while still may be harmful to states' presence in cyberspace, are most effective against non-state actors, namely individuals and enterprises.

3.3.1 Denial of Service

Denial of Service attacks can be carried against single entities in cyberspace, for instance a single website, or in the case of Estonia and Georgia cyber-attacks of 2007 and 2008 respectively, can be launched against networks belonging to a nation indiscriminately.

Distributed Denial of Service attacks require a few other components to function and realize its goal, which is the separation of a network and its users. To understand how an attack is carried, some of these components needs to be explained. DDoS attacks are often generated within the seventh layer of the OSI Model of interconnected computing which is the human computer interaction layer (International Telecommunication Union, 1994, p. 33).

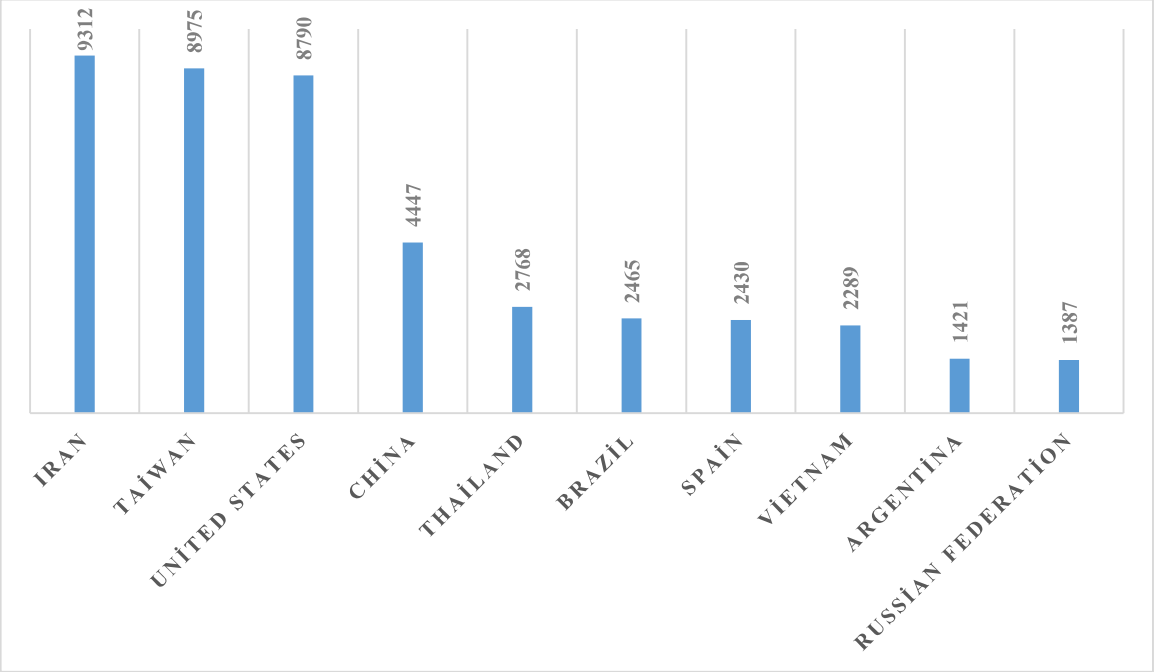
In a typical attack scenario, an attacker scans the internet for vulnerable computers to take over and add them to their bot network. A vulnerable computer which is infected by the attacker then seeks out and tries to infect any other device within their own internal network through what is called "lateral movement". When a significant number of infected devices are controlled by the attacker, he or she may launch their denial of service attack. Distributed denial of service attack implies that the load of generating high traffic is distributed amongst the computers belonging to attacker's botnet by instructing bots to send as many HTTP requests to target as possible in a short span of time, thus overwhelming the target's capacity to respond to legitimate requests (http-3).

This in turn leads to service outages for affected networks, as was the case in both Tallinn (2007) and Georgia (2008) cyber-attacks. Cyber-attacks against Estonia, along with botnets will be expanded upon in future chapters, however during the literature research of this phenomenon, it was evident that some researchers and journalists who reported these attacks in 2007 and as recent as 2017 considered these attacks as "hacks" (Tamkin, 2017). In relation to technology, dictionary definition of the verb hack is "gaining unauthorized access to data in a system or computer" (http-15). While there have been websites hacked, in other words, modified by unauthorized individuals, during the Estonian DDoS attacks, majority of the service disruption was caused by the consumption of all available bandwidth by bogus HTTP requests generated by the bots.

Another subset of denial of service attack is called the Permanent Denial of Service (PDoS) or "phlashing" (Prowell, Kraus, and Borkin, 2010, p. 9). If an attacker could access the hardware, permanent denial of service is as simple as plugging a commercially available

product such as USB Killer to any exposed USB port (http-16). Remotely executed phlashing however was a theoretical concept until a specifically written botnet named BrickerBot and its subsequent variants began targeting poorly secured Internet of Things (IoT) devices. Given the results displayed by the search engines such as Shodan.io, poorly secured IoT devices are in high supply for attackers to either add to their bot networks or in BrickerBot's case, permanently damage them. At the time of writing this thesis, a query for internet connected devices with unchanged default passwords resulted in 67,452 accessible devices (http-17). These unsecured devices are perfect zombie candidates for botnet masters, ready to generate high amounts of traffic from the get-go. In a recent attack, a botnet was able to harness the power of approximately 145,000 unsecured IPTV cameras equipped with a slimmed down version of Linux operating system for media transfer over Internet Protocol (Goodin, 2016). Most Internet of Things devices are built upon the Linux operating system and the extreme versatility Linux provides makes these devices prime targets for botnet acquisition and traffic generation due to manufacturers not properly securing their devices. Figure 3.1 shows the distribution of internet connected and vulnerable devices per country.

Figure 3.1. *Devices with default password connected to Internet (http-18)*



3.3.2 Man in the Middle Attacks

Man in the middle (MiTM) attacks happen when an attacker intercepts communication between two entities. This type of attack did exist before the cyberspace and is still relevant in both real world and cyberspace. In real world scenario, the attacker could intercept a recipient's mail before delivery or while it is in transit to modify the contents. In cyberspace, MiTM attacks are performed easier due to software automation. Unlike other attack vectors, MiTM attacks cannot be avoided by simply staying up the date with necessary security patches. MiTM attacks can be executed through a variety of vectors. Stacy Prowell, Rob Kraus, Mike Borkin in their work titled "Seven Deadliest Network Attacks" report four different ways of achieving the goal of intercepting data packets between a user and a server: Sniffing network traffic, replay attacks, command injection, and lastly Internet Control Message Protocol (ICMP) redirection (Prowell, Kraus, and Borkin, 2010, pp. 104-105).

Sniffing network traffic is the process which an attacker intercepts communicated data between a client and a server by positioning himself or herself between the user and the server. According to the client-server architecture, any service requesting entity is labeled 'user' or 'client' in this context and the service provider is labeled as 'server'. After identifying network traffic, an attacker may employ the *ICMP redirection* attack to advertise himself or herself as a better route for intended destination of user's packets. This would enable the attacker to modify or record the contents of a data packet before forwarding it to the intended destination. With *replay attacks* Prowell et al. state that after a user is authenticated by a server, this authentication data can be intercepted and saved by the attacker to gain unauthorized access to sensitive information later on. *Command injection* usually implies injecting unauthorized packets or data to a service or a server through already compromised active authenticated users by intercepting and modifying the communication in-between (Prowell, Kraus, and Borkin, 2010, pp. 104-105).

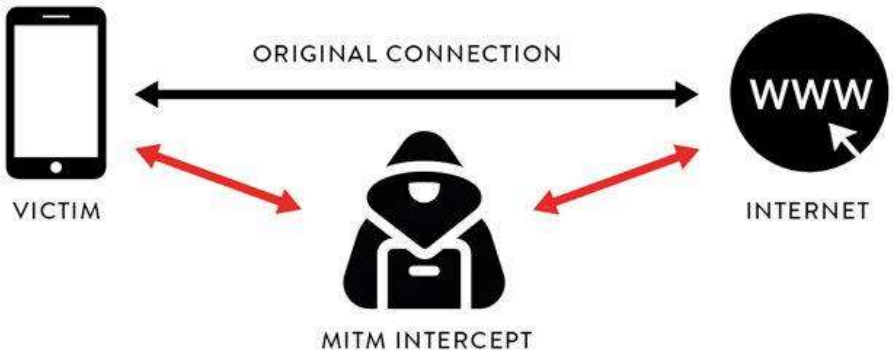


Figure 3.2. *Depiction of a typical man in the middle attack (http-24)*

3.3.3 Malicious Software

Malicious software or simply malware, are the software written to perform malicious tasks without the consent of the operator of the system software is installed. Generally created for mass infection rather than targeted attacks, these programs are tailored for specific uses. This section tries to briefly explain some of the functions of these malicious software.

3.3.3.1 Viruses

Viruses are computer codes which can inject itself into other executable files and are executed along with their hosting executable. Virus may infect system or boot process executables and remain in Random-Access Memory (RAM) for the entire duration of the computer being in operation, from hereby will be referred as uptime. The resident virus may then infect and replicate itself onto other executables in an attempt to spread (Abraham, 2018).

3.3.3.2 Worms

Computer worms are programs on their own right and spread across a network exploiting security or policy vulnerabilities in common services. They differ from the viruses due to fact they do not infect other executables thus have alternative yet faster methods of propagation (Weaver, Paxson, Staniford, and Cunningham, 2003, p. 1). Worms and viruses are often spread through email attachments and by inserting an already infected USB drive

into a computer which is programmed by the virus to automatically execute its infection protocol. It is worth noting that infamous Stuxnet malware was classified as a worm and will be referred as such in this work.

3.3.3.3 Trojans

Named after the famous wooden horse gifted to Troy in the Trojan War, a trojan is an "apparently useful program containing hidden functions that can exploit the privileges of the user [running the program] with a resulting security threat" (Ford, 1999, p. 105). Unlike viruses or worms, trojans do not spread on their own. They often rely on users willfully downloading and executing them within their secured network just as the Trojans took the wooden horse inside their city walls.

3.3.3.4 Spyware

Spyware are designed to gather information on the system it infects by monitoring the actions of the user instead of directly harming the host. Its reporting capabilities range from simple web usage monitoring to keylogging and file inspecting (Baskin, et al., 2006, p. 2). Duqu malware may have components which enabled attackers to spy on infected computers, it was beyond the scope a simple spyware as it gave remote capabilities to its masters and therefore is classified as a remote access tool.

3.3.3.5 Botnet

Previously mentioned in the DoS attacks, bot malwares are designed to infect and take control of large quantities of computer systems and provide remote control ability to its operator. After initial infection via viruses or trojans, a bot malware could be downloaded to turn over the infected host to remote operator whom, then could use said computer systems in DDoS attacks or to send out spam/phishing emails (Lysne, 2018, p. 58).

In 2011 a botnet named Festi was used to launch a DDoS attack against a payment processor named Assist which was in negotiations for a contract with the Aeroflot, Russia's largest airline. Attack was launched only a week before Aeroflot's final decision, rendering

Assist's processing systems unusable for an extended amount of time. Leading to loss of the contract with the Aeroflot (Matrosov, Rodionov, and Bratus, 2019, p. 14).

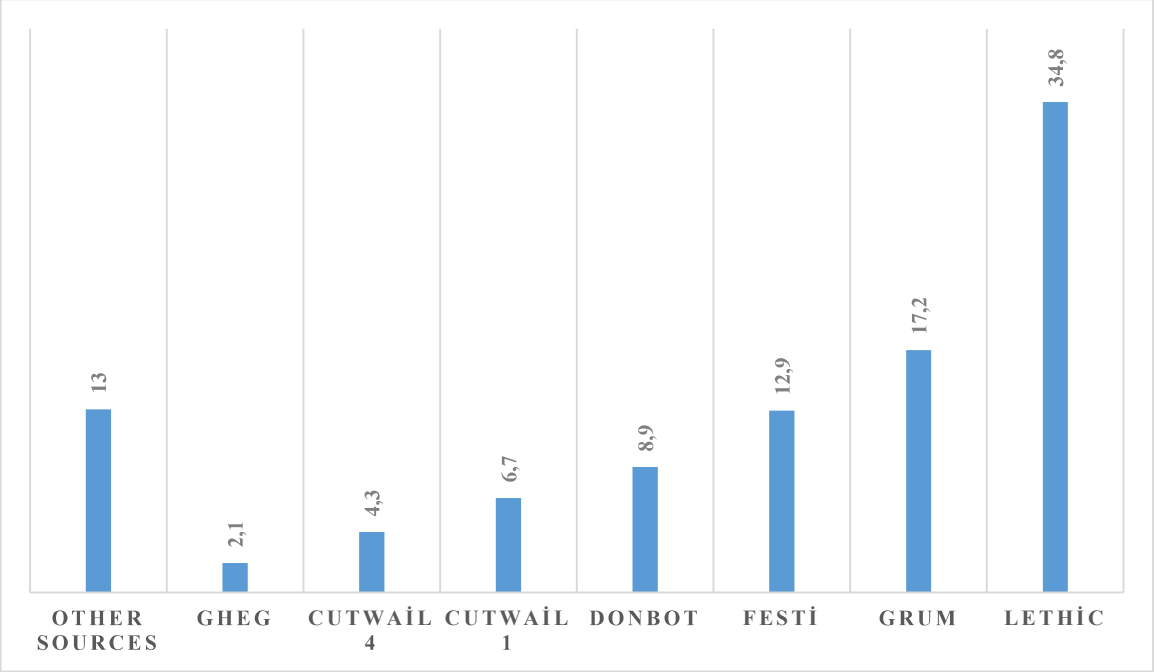


Figure 3.3. *Spam Botnet Prevalence according to M86 Security Labs' 2011 report (Matrosov, Rodionov, and Bratus, 2019, p. 14)*

3.3.3.6 Rootkits

Rootkits are used to hide another malware's presence from detection by user or anti-malware programs. Typically, rootkits aren't harming a computer system however due to their ability to cloak other malware, they are commonly used in sophisticated attacks (Lysne, 2018, pp. 58-59).

One of the infamous pieces of rootkits is known as TDSS or TDL3 was distributed through a Pay-Per-Install (PPI) business model affiliated with now defunct DogmaMillions and GangstaBucks, which tracked and billed customers of the rootkit through unique identifier (UID) numbers embedded in the executable for specific builds. Affiliates went as far as to provide username and passwords for customers as well as assigning personal managers in the event of technical difficulties (Matrosov, Rodionov, and Bratus, 2019, pp. 4-5).

3.3.3.7 Ransomware

Computer Emergency Readiness Teams (CERT) employed by the Cybersecurity and Infrastructure Security Agency (CISA) recommend 3, 2, 1, backup system for combatting data loss. 3 separate copies of any important file kept in 2 different mediums such as one copy being kept in a hard drive while the other is burned to read only medium like a compact disk; 1 copy stored off-site (Ruggiero and Heckathorn, 2012, p. 1). Recent advancements in the data storage technologies obsoleted the compact disk as a go to medium for data storage. Instead, cloud storage is now more accessible than ever. It is worth noting that cloud storage is not a read only medium and being on the internet leaves the copy vulnerable to other cyber threats.

Figure 3.4. *Recommended Data Backup Options by CERT*

This section focuses on the data backup due to fact ransomware have recently made a comeback in the recent years. Alan Liska and Timothy Gallo define ransomware as "a blanket term used to describe a class of malware that is used to digitally extort victims into payment of a specific fee" (Liska and Gallo, 2017, p. 3). European Union reported 300% increase in ransomware attacks between 2015 and 2016 (http-31). Untraceable payment options such as cryptocurrencies have made ransomware a more popular attack vector for cyber criminals. According to Liska and Gallo, a ransomware attack can be categorized in two separate categories, data encryptors and system restrictors (Liska and Gallo, 2017, p. 3). Ransomware attacks are executed in five stages.

Initial deployment of ransomware malware begins and propagates through compromised web sites, drive-by downloads or by phishing emails containing malicious links/attachments. Once the malware downloader infects a system, ransomware attack enters installation phase. Usually ransomware are reassembled after the initial intrusion in target system to avoid detection by anti-virus software. It is at this point that ransomware tries to exploit vulnerabilities and file shares to move laterally across the infiltrated network to

maximize ransom potential. Reconstructed and awaiting commands, ransomware tries to connect with command and control servers. Once a connection is established, malware relays back significant amount of information to identify potential files such as personal documents or pictures for encryption and size the infiltrated target for further escalation. Once the target files are chosen, sophisticated ransomware often generates unique encryption keys and sends them to command and control servers. If an order to encrypt data on the infected computer or network returned by the command and control servers, fourth attack phase begins. During the destruction phase, previously identified files of importance are encrypted with the unique key generated in the last phase. In the last phase of the ransomware attack, victims are greeted by a screen telling them to pay a specific amount of money in cryptocurrencies or pre-paid cards. In the event of non-compliance, usually price goes up or files are deleted permanently (Liska and Gallo, 2017, pp. 6-11).

Just as the extortion cases happening in real life, compliance does not guarantee safe return of data in ransomware attacks. Simply for this reason, data recovery from backups created in accordance with the data backup recommendation in the beginning of this section would be the only way of guaranteeing the safe return of data.

Table 3.4. *Stages of a ransomware attack (Liska and Gallo, 2017, p. 6)*

Stage	Actions
Deployment	Compromised web sites
	Drive-by downloads
	Phishing
	Vulnerability Exploitation
Installation	Reconstruction
	Memory Access
	Lateral Movement
Command and Control	HTTP/HTTPS connection
	OSN Instructions
	TOR
	Email
Destruction	Data Encryption
	System Locking
Extortion	Cryptocurrencies
	Prepaid Vouchers

CHAPTER 4

4. CASE STUDIES

This section of the thesis focuses on some of the high profile cyber-attacks involving state actors, either as suspected perpetrators or targets.

4.1 Targeted Cyber Attacks

4.1.1 Operation Olympic Games (Stuxnet)

At the time of writing this thesis, there have been more examples of cyber-attacks using cyber weapons. However Stuxnet takes precedent due to a few characteristics it bears within its structure. During the initial discovery and identification process of the Stuxnet campaign, a few state actors were suspected of involvement, namely the United States of America (USA) and Israel. In 2016, Alex Gibney, in his documentary titled “Zero Days” asserted that

Stuxnet was a joint venture between the National Security Agency (NSA) of USA and the Israel's Unit 8200 dubbed Operation Olympic Games. Gibney in his work also claims that President of the USA at the time, Barack Obama, has given the greenlight for the Operation Olympic Games as deployment of cyber weapons are treated in the same way as nuclear weapons and therefore require presidential authorization. Gibney also claims that the expiration date of June 24, 2012 hardcoded on the cyber weapon allegedly developed by the NSA and Unit 8200 was set to that date due to upcoming presidential election. Given the complexity of the Stuxnet requiring state actor level backing, how it was programmed to avoid any collateral damage and had a predetermined expiration date in all versions recovered by the security analysts give precedence to Stuxnet over other advanced persistent threats.

4.1.1.1 What was the Stuxnet?

Kaspersky Lab's co-founder and chief executive officer Eugene Kaspersky has pointed at the remarkable sophistication of Stuxnet in his speech at the Kaspersky Security Symposium at Munich in 2010 with the following words: "I think that this is the turning point, this is the time when we got to a really new world, because in the past there were just cybercriminals, now I am afraid it is the time of cyberterrorism, cyberweapons and cyberwars … This malicious program was not designed to steal money, send spam or grab personal data. This piece of malware was designed to sabotage plants, to damage industrial systems" (http-4).

Stuxnet was originally discovered by Sergey Ulasen, then working for a small Belorussian company named VirusBlokAda (http-5). Stuxnet was only discovered after the computers in Iran began displaying unexplained Blue Screens of Death (BSoD)[2] errors. Ulasen has come to suspect malware presence when he found out that networked computers, even with a fresh installation of the operating system reported same errors (http-5). Eventually, Ulasen's efforts were fruitful in locating the malware and analyzation process had begun. On June 17, 2010, VirusBlokAda reported the Stuxnet as Rootkit.TmpHider and

[2] "A blue screen of death (also referred as a stop error) is an error causing unexpected shutdown or restart of a system with Microsoft Windows operating system installed. A blue screen detailing the error is displayed while computer saves its operational memory on the hard drive, afterwards computer is promptly restarted" (http-6).

SScope.Rootkit.TmpHider.2 (http-7). Following this, malware was being detected worldwide with the majority of infections being geographically located in Iran. In their report, Nicolas Falliere, Liam O Murchu and Eric Chien were able to conclude that initial seeding of the malware was done through infecting five different organizations with Iran presence. Earliest known version of Stuxnet was used to infect these five organizations through an already infected USB drive with three organizations being attacked once with the remaining two being targeted up to three times.

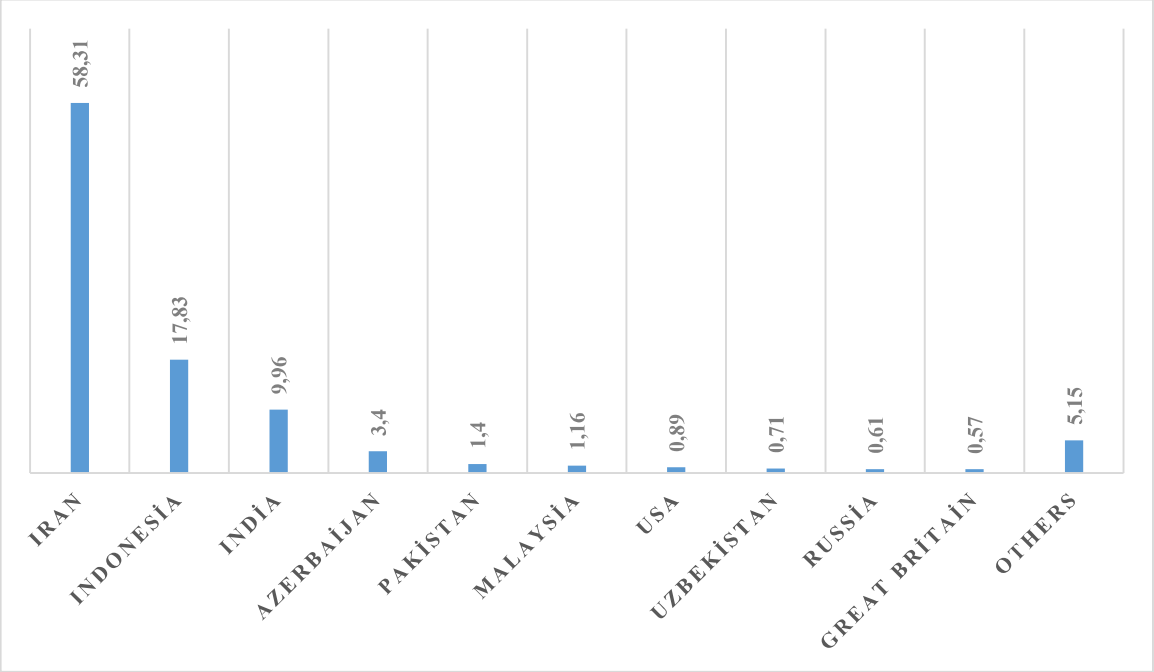


Figure 4.1. *Geographic Distribution of Infections (Falliere, O Murchu, and Chien, 2011, p. 6)*

Up to the point Stuxnet was found and analyzed by security researchers, science fiction stories predicting apocalypse level destruction done by a malware which can fit in simple diskettes were just that, stories of an active imagination. Stuxnet however, was the proof-of-concept that with sufficient knowledge and funding, these stories may come true after all. It is worth noting that compared to what is capable by targeting industrial control systems, Stuxnet is considered a harmless malware. Targeting only Microsoft Windows systems running Siemens' SIMATIC Step 7 software controlling Siemens Programmable Logic Controllers, Stuxnet is extremely selective of its targets (Falliere, O Murchu, and Chien, 2011, p. 3).

This section will analyze the campaign process of the Stuxnet in contrast with advanced persistent threats' campaign processes mentioned in earlier chapters. Stuxnet has a few key differences in its operational campaign process. Namely, it does not try to exfiltrate data. Instead, at the final stage of the infection, Stuxnet tries to damage uranium fuel enrichment process. Oftentimes industrial command systems are not connected directly to the internet. Given the nature of its target, Stuxnet cannot stay in constant communication with its command and control servers. Therefore Stuxnet employs Peer to Peer (P2P) connections to stay up to date and report back, meaning data packets meant for command and control systems are transferred to an already infected machine within the same network which has an operational internet connection (Matrosov A. , Rodionov, Harley, and Malcho, 2011, p. 56).

During the initial reconnaissance and weaponization stage, attackers would need to setup a mirror environment identical to which they would be attacking, including all the necessary hardware for controlling centrifuges in an identical configuration such as being in air gapped networks to simulate and develop ways for malware to hop over that gap. Paul Mueller and Babak Yadegari in their work titled "The Stuxnet Worm" bring attention to that photos taken and distributed to press (while the Islamic Republic of Iran's president at the time Mahmoud Ahmedinejad was visiting the Natanz Fuel Enrichment Plant) were detailing the Iran's enrichment process (Mueller and Yadegari, 2012, p. 1). Iran had used gas centrifuges to separate Uranium-238 (U^{238}) from Uranium-235 (U^{235}) by spinning the Uranium Hexafluoride (UF_6) in gas centrifuge cylinders at high speeds. The process results in heavier U^{238} atoms gathering around at the edge of the cylinder while lighter U^{235} atoms clustering around the center of the centrifuge. This layout of interconnected gas centrifuges are referred to as a cascade (http-9).

Figure 4.2. *Natanz Cascade Configuration (Pauli, 2011)*

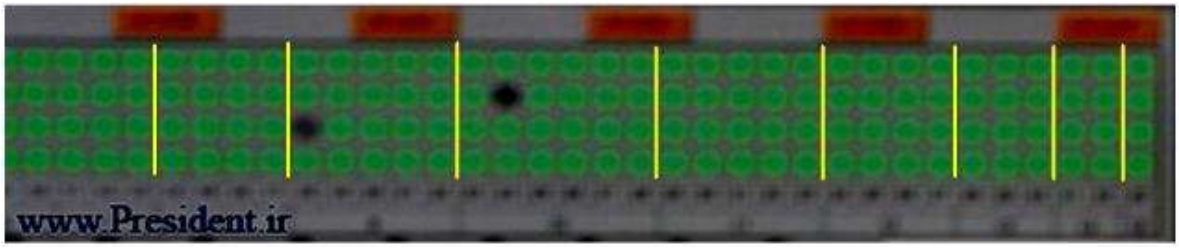


Figure 4.3. *Cascade Seperation (Mueller and Yadegari, 2012, p. 2)*

Photograph shown in figure 4.2 was published on the Office of the Presidency of Islamic Republic of Iran (president.ir) website and inadvertently shared some of the critical secrets for an adversary to affect Iran's nuclear enrichment program. Figure 4.3 details the stage separation marked with yellow lines, matching grey separators underneath the green indicators for the enrichment process, and according to Mueller and Yadegari, matches the code found in Stuxnet malware (Mueller and Yadegari, 2012, p. 2). Falliere, O Murchu and Chien estimate Stuxnet's reconnaissance and weaponization process to "have taken six months and five to ten core developers not counting numerous other individuals, such as quality assurance and management" (Falliere, O Murchu, and Chien, 2011, p. 3) for to complete. Ralph Langner in his report titled "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve" argues that attackers would need to construct a duplicate of IR-1 cascade, including real UF_6 circulating through centrifuges due to over

pressurization and rotor speed manipulation having differing effects in empty centrifuges. Given that components capable of being used in fuel enrichment process are strictly controlled export materials on a state level, Langner argues that there is no doubt Stuxnet's creators had state level resources at their disposal (Langner, 2013, p. 20).

Also during this stage, attackers had acquired two legitimate digital certificates belonging to Realtek Semiconductor Corporation as well as JMicron Technology Corporation and signed the drivers[3] required for the rootkit portion of the malware to hide the executables of the Stuxnet malware from being found. Between the earliest sample of Stuxnet in June 2009 and the final analysis in September 2010, both certificates were used to sign Stuxnet's drivers. (Falliere, O Murchu, and Chien, 2011, pp. 3-4). Both certificates belonging to Realtek and JMicron were revoked and new certificates were issued following the discovery of compromise. While it is possible that an earlier version of Stuxnet could have been used to compromise these certificates, both companies maintained offices in Hsinchu Science and Industrial Park in Taiwan and this proximity suggests physical penetration of these offices in order to steal the certificates usually guarded in air gapped networks (Raiu, 2010). Aleksandr Matrosov, Eugene Rodionov, David Harley, and Juraj Malcho, in their report published by ESET LLC, an anti-virus solutions company, titled "Stuxnet Under a Microscope: Revision 1.31" highlight the possibility of these certificates being bought from other sources as known botnets, namely Zeus, has a history of stealing certificates (Matrosov A. , Rodionov, Harley, and Malcho, 2011, p. 13).

After the reconnaissance and weaponization process, payload needed to be delivered to the target networks. Figure 4.1 displays the initial infection was concentrated around Iran and following the detailed analysis of the malware done by Falliere, O Murchu and Chien, we know that attackers initially targeted five organizations within Iran. As of the 29th September, 2010, there have been 100,000 reported Stuxnet infections with approximately 60% of hosts belonging to Iranian networks. Stuxnet, being designed in such a way, tries to identify and infect hosts with Siemens SIMATIC Step 7 software installed thus infection could not stay limited to Iran. After an initial infection occurs, Stuxnet creates a configuration

[3] A driver is "any software component that observes or participates in the communication between the operating system and a device" (http-8).

block within the infected computer, encrypting its contents to deliver them to command and control servers. This data block contains the internal and external Internet Protocol (IP) addresses of the computer, the name of the computer, installed operating system's version information and whether it is running the Siemens SIMATIC Step 7 ICS software (Falliere, O Murchu, and Chien, 2011, pp. 3-7). As previously mentioned, according to Falliere, O Murchu and Chien's report, the initial attacks against the five organizations with Iranian presence happened in three specific waves lasting between June 22, 2009 and April 14, 2010. Out of 3,280 samples recovered by the Symantec Corporation the most reported variant of Stuxnet was belonging to the second wave initiated in March 01, 2010, indicating better propagation conditions for the malware, possibly due to false sense of security stolen certificates provided during the initial payload delivery (Falliere, O Murchu, and Chien, 2011, pp. 7-10).

Upon a successful installation, Stuxnet tries to establish connection with its command and control servers. Before attempting to send the configuration block generated in initial installation to command and control servers, Stuxnet checks internet connectivity by trying to establish connection with two legitimate services, namely Windows Update and MSN. If the connection succeeds, Stuxnet then tries to send the configuration data to two, now defunct, addresses: "www.mypremierfutbol.com and www.todaysfutbol.com" (Matrosov A. , Rodionov, Harley, and Malcho, 2011, p. 66). If the internet connectivity check were to fail, a contingency plan programmed into the worm itself would implement a Remote Procedure Call (RPC)[4] function to establish a peer to peer connection between hosts belonging to a same network. This procedure would then compare worm versions and update as necessary (Matrosov A. , Rodionov, Harley, and Malcho, 2011, p. 57).

Excluding the removable drive propagation, during the lateral movement phase, Stuxnet had employed five attack vectors in its code to infect a remote host belonging to

[4] IBM defines the Remote Procedure Call protocol as "a protocol that provides the high-level communications paradigm used in the operating system. RPC presumes the existence of a low-level transport protocol, such as Transmission Control Protocol/Internet Protocol (TCP/IP) or User Datagram Protocol (UDP), for carrying the message data between communicating programs. RPC implements a logical client-to-server communications system designed specifically for the support of network applications" (http-10).

same internal network. (1) Previously mentioned peer to peer connection, (2) propagating through network shared files, (3) propagating through zero-day vulnerabilities relating to network architecture, (4) propagating through Windows Server Service related vulnerability and lastly (5) infecting Siemens WinCC machines due to a hardcoded database server password (Falliere, O Murchu, and Chien, 2011, p. 25). The fifth vector implies that attackers had ample time to reverse engineer the WinCC database software to learn about the hardcoded server password which would support the six months reconnaissance and weaponization window theory maintained by the Falliere et al. While Stuxnet had these options to propagate through a network, the main vector for infections was still the removable drives due to Stuxnet exploiting one of its four zero-day vulnerabilities malware contains as the previously mentioned second version, the version containing the zero-day vulnerability for removable drive propagation, is shown to be the most popular version.

Building upon the earlier premise that the Stuxnet does not exfiltrate data but instead damages centrifuges, the campaign stage normally referred data exfiltration will be referenced as the PLC modification phase for the Stuxnet section of this work. Before examining how Stuxnet was able to take control of the PLCs installed in Natanz Enrichment Plant, it would be helpful to explain the connection between a controlling computer and a PLC unit. A controlling computer, loaded with the Siemens' Step 7 controlling software in Stuxnet's case, establishes connection with a PLC through a data cable and communication between the two computers are handled through Step 7. It is worth noting that while Stuxnet was able to destroy centrifuges, it never actually infected the PLCs themselves as that would require having complete access to source code operating the PLCs. Instead, Stuxnet targeted the controlling systems often using outdated versions Microsoft Windows to intercept the data being transmitted between the controlling computer and PLC. Controlling computer uses different languages like Statement List (STL) or Structured Control Language (SCL) to program the PLCs. Once programmed, PLCs then can operate on standalone mode with no controlling computer. However in the case of uranium enrichment, constant monitoring and supervision of centrifuge cascade is necessary. As discovered and published in Eric Chien's report in 2010, Stuxnet was used to take over the read and write functions of computers running Step 7 with frequency converter drives manufactured by two specific vendors, one located in Finland while the other was headquartered in Iran. These drivers needed to spin

between 807 Hz to 1210 Hz before Stuxnet could begin altering these frequencies. As previously mentioned, these are the specific operating frequencies for a gas centrifuge designed to separate U^{235} and U^{238}. According to Chien's report Stuxnet achieved its sabotage goal over a period of months through altering the frequencies of these centrifuges to 2 Hz and then to 1064 Hz (Chien, 2010). This in turn leads to centrifuge failure rates higher than what is acceptable according to guidelines set by the International Atomic Energy Agency (IAEA) as published in the report titled "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report" by the David Albright, Paul Brannan and Christina Walrond's Insititute for Science and International Security (Albright, Brannan, and Walrond, 2011, p. 3).

4.1.1.2 Aftermath of the Stuxnet

Earlier section has examined Stuxnet worm's inner workings and how it was able to spread within a secure network in detail. During the final phase of the malware activation, Stuxnet was extremely selective of its targets. Analysis has revealed that Stuxnet did infect computers other than its target, however it did so to reach its final destination, which is air-gapped and is not connected to the internet; all this, to finally deploy its payload. Effects of this infection were negligible and until the previously mentioned Blue Screen of Death error caused by the worm, there were no indications of any malfunctions or infections for the infected computer systems.

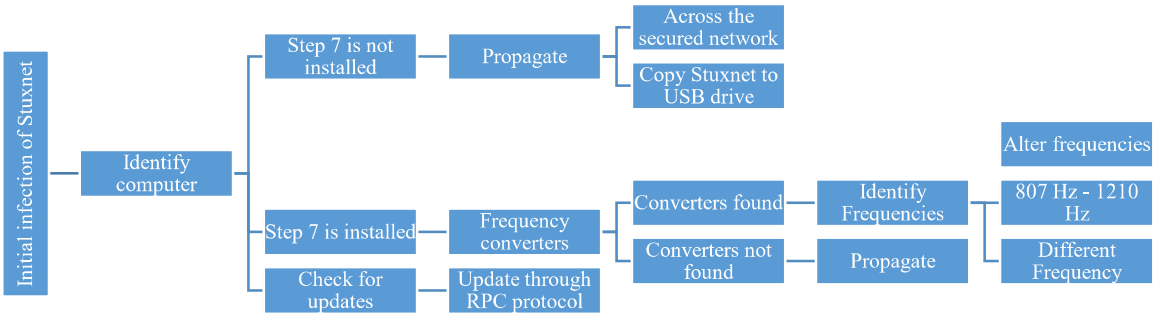


Figure 4.4. *Steps taken by Stuxnet following an infection*

Figure 4.4 demonstrates the steps Stuxnet worm takes to ensure that it only alters Step 7 installed machines, controlling frequency converter drivers manufactured by two vendors, one headquartered in Finland while the other is located in the Islamic Republic of Iran, operating at the frequency ranges between 807 Hz to 1210 Hz and after initiating the monitoring process, over the course of months, the worm alters the frequencies of the centrifuges to either 2 Hz or 1410 Hz that eventually destroys them. Albright, Brannan and Walrond's report published in 2010 highlights the final outcome of the Stuxnet with the following:

> "Another link between the IR-1 centrifuge and Stuxnet is the maximum frequency listed in one of the attack sequences. Stuxnet commands an increase in the frequency to a maximum of 1410 Hz. For the IR-1 centrifuge rotor, this frequency corresponds to a tangential wall speed of 443 meters per second, very close to the maximum speed the spinning aluminum IR-1 rotor can withstand mechanically. The rotor tube of the IR-1 centrifuge is made from high strength aluminum and has a maximum tangential speed of about 440-450 meters per second, or 1,400-1,432 Hz, respectively. As a result, if the frequency of the rotor

> increased to 1410 Hz, the rotor would likely fly apart when the tangential speed of the rotor reached that level" (Albright, Brannan, and Walrond, 2010, p. 4).

Albright et al. also highlight that at the height of the Stuxnet campaign, Iran had approximately 9,000 centrifuges in the Natanz Fuel Enrichment Plant and Stuxnet thus far only managed to destroy 1,000 gas centrifuges. In contrast with this number, Albright et al. estimate the approximate number of centrifuges to ever been employed at the Natanz Fuel Enrichment Plant would be around 11,000 mark. While 1,000 centrifuges may not seem significant in compared to remaining 10,000 in operation following the upgrades, Albright et al. state that "Iran would have struggled to understand this failure and likely would have lost valuable time worrying about more failures" (Albright, Brannan, and Walrond, 2011, p. 4).

In the aftermath of what is now generally accepted as the first cyber weapon created and deployed by a state actor, fears of impending cyber warfare of ran rampant. Jon R. Lindsay in his work titled "Stuxnet and the Limits of Cyber Warfare" mentions media coverage of Stuxnet with the following:

> "Breathless media accounts have portrayed Stuxnet, which physically injured no one, as 'the cyber equivalent of the dropping of the atom bomb' and 'a new era of warfare.' Concerns soon surfaced about unbridled proliferation of Stuxnet code, now openly available on the internet, and potential collateral damage to Natanz and beyond. As the Russian ambassador to NATO worried, 'These 'mines' could lead to a new Chernobyl'." (Lindsay, 2013, p. 366).

Media channels aren't the only ones showing a lack of understanding when it comes to the limiting aspects of cyberwarfare. Stuxnet was developed to exploit the weaknesses of the Iranian fuel enrichment program had, namely a propensity to equipment malfunction due to speed manipulations rendering centrifuge rotors unreliable (Langner, 2013, p. 19). Even an IT security consultant to United Kingdom of Great Britain and Northern Ireland (UK), Will Gilpin at the time of the attack assumed something like Stuxnet could "(1) shut down the police 999 system, (2) shut down hospital systems and equipment, (3) shut down power stations and transport network across the United Kingdom" (Matrosov A. , Rodionov, Harley, and Malcho, 2011, p. 23). Gilpin is by no means off the target, it is certainly possible to do all these things. However, the cost of reverse engineering the systems in place, looking for attack vectors to exploit and yet remain stealthy enough to target only the systems mentioned

by Gilpin would require extensive resources, most likely well exceeding any reasonable peace time budget of most nations' intelligence divisions. Langner states in his report that he estimates "well over 50% of Stuxnet's development cost went into efforts to hide the attack" (Langner, 2013, p. 21). Indeed, Stuxnet's main propagation method, removable drive infection method, even had measures in place so that after the third machine infection, the worm would remove itself from the drive in order to remain undetected. Exploiting the LNK vulnerability identified as the CVE-2010-2568 to remain undetected, Stuxnet developers did not want their creation to be found (Falliere, O Murchu, and Chien, 2011, p. 29). It is worth mentioning that zero-day vulnerabilities are not created in infinite quantity. For every application's operational lifetime, there are only a limited number of vulnerabilities that can remain undetected for so long, before it is discovered, either by a malware exploiting that vulnerability or during code review. This is one of the reasons that zero-day vulnerabilities giving unfettered access to a system fetch previously mentioned prices in Darknet ranging from $1,000 to $100,000 (http-12).

Politicians and policy makers have suffered from the lack of knowledge in this fifth operational domain. Just like any other weapon developed and deployed through the human history of warfare, cyber weapons are not at all different from their material counterparts. The collective effort required to reverse engineer a critical infrastructure is not something to be taken lightly, yet it is within the grasp of well-funded non-state actors as well as state actors with necessary expertise at their command.

4.1.2 Duqu

In this section of the thesis, Duqu and later updated version of Duqu 2.0 will be examined and compared to Stuxnet. The previous section covered the Stuxnet campaign in detail and due to similarities between the two threats, therefore instead of focusing campaign stages, similarities between the Stuxnet and the Duqu family will be discussed in this section. As established previously, Stuxnet had managed to destroy around 1,000 gas centrifuges used for uranium enrichment purposes. In contrast, Duqu is an espionage-focused malware. Remembering the previous definitions of a cyber weapon defined in the earlier chapters of this thesis, Duqu does not affect data integrity and therefore cannot be explicitly classified as a cyber weapon. Symantec's report on the initial version of the Duqu classifies it as a Remote

Access Tool (RAT) and mentions that it does not self-replicate (Symantec Security Reponse, 2011, pp. 1-2). The Hungarian Laboratory of Cryptography and System Security (CrySyS) has released the initial report and follow up reports on the Duqu in 2011, the same year the effects of Stuxnet were understood by security researchers in the computer science field. Security researchers across the globe have concluded on two possibilities that either Duqu and Stuxnet belong to the same malware family, or the developers of the Duqu had access to Stuxnet's source code. Duqu received its name due to malware creating files with the "~DQ." extension in infected systems (Bencsáth, Pék, Buttyán, and Félegyházi, 2011, p. 5). As mentioned in the previous section, Stuxnet was allegedly developed and deployed by the NSA and the Unit 8200 according to Alex Gibney, in his documentary titled "Zero Days". While neither accused party claimed responsibility for the construction of the cyber weapon, we already established that Stuxnet did indeed require state-level resources due to requirements to test the weapon on the components being sabotaged to confirm its functionality. Stuxnet had contained four exploits for four zero-day vulnerabilities. Duqu however, exploits a single zero-day exploit found within the Microsoft Word software. If the attackers had access to Stuxnet's original source code, the costs between two malwares would be incomparable, rendering Duqu quite affordable, even without the state level backing.

4.1.2.1 Centrifuge sabotage versus data exfiltration

Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, Márk Félegyházi, in their work titled "The Cousins of Stuxnet: Duqu, Flame, and Gauss" state that in September 2011, a European company requested the help of CrySyS to identify an indecent within their secure network. During this investigation, Bencsáth et al. discover that unlike Stuxnet, Duqu did not contain any code relating to the programmable logic controllers (PLC) instead had an information stealing toolkit, that targets Microsoft Windows based computers (Bencsáth, Pék, Buttyán, and Félegyházi, 2012, p. 973).

As established by security researchers dissecting the Duqu, Duqu does not try to incur damage to any system it infects. Instead, Duqu's main goal is ensuring that the infected system is able to be controlled remotely by Remote Access Tools and that targeted organizations were specifically selected and initial intrusion was done with the spear phishing method with a malicious Microsoft Word document (Symantec Security Reponse, 2011, p.

2). Duqu's initial discovery had been reported in six different organizations situated within eight countries.

Figure 4.5. *Geographic distribution of the initial Duqu malware (Symantec Security Reponse, 2011, p. 3)*

Figure 4.5 displays the infections reported by six different organizations at the time of the discovery with the table below where as table 4.1 contrasts the organizations with the countries they operate within. Due to sensitive nature of the compromise however, initial reports were published by under the effects of a non-disclosure agreement, meaning that the reports had to be anonymized to protect the identities of these organizations.

Table 4.1. *Organizations by Countries (Symantec Security Reponse, 2011, p. 3)*

Organization	Country
Organization A	France, Netherlands, Switzerland, Ukraine
Organization B	India
Organizations C, D	Iran
Organization E	Sudan
Organization F	Vietnam

Feature	Stuxnet	Duqu
Modular malware	✓	✓
Kernel driver based rootkit	✓	✓ very similar
Valid digital signature on driver	Realtek, JMicron	C-Media
Injection based on A/V list	✓	✓ seems based on Stux.
Imports based on checksum	✓	✓ different alg.
3 Config files, all encrypted, etc.	✓	✓ almost the same
Keylogger module	?	✓
PLC functionality	✓	✗ (different goal)
Infection through local shares	✓	No proof, but seems so
Exploits	✓	?
0-day exploits	✓	?
DLL injection to system processes	✓	✓
DLL with modules as resources	✓ (many)	✓ (one)
RPC communication	✓	✓
RPC control in LAN	✓	?
RPC Based C&C	✓	?
Port 80/443, TLS based C&C	?	✓
Special "magic" keys, e.g. 790522, AE	✓	✓ lots of similar
Virtual file based access to modules	✓	✓
Usage of LZO lib	?	✓ multiple
Visual C++ payload	✓	✓
UPX compressed payload,	✓	✓
Careful error handling	✓	✓
Deactivation timer	✓	✓
Initial Delay	? Some	✓ 15 mins
Configurable starting in safe mode/dbg	✓	✓ (exactly same mech.)

Figure 4.6. *Feature comparison between Stuxnet and Duqu (Bencsáth, Pék, Buttyán, and Félegyházi, 2011, p. 8)*

Duqu and Stuxnet share some notable similarities both in the code aspects of the malware as well as execution of the initial intrusion phase. Namely, both malwares use valid certificates to impersonate legitimate software components to evade detection. During the Stuxnet investigation, researchers had suspected physical intrusion or a Stuxnet like malware being used to steal digital certificates (Falliere, O Murchu, and Chien, 2011, p. 4). Similar to

Realtek Semiconductor Corporation and JMicron Technology Corporation, C-Media Electronics Incorporated too has headquarters in Taiwan (http-25). Further supporting the claim that intelligence operatives were involved in the compromise of the said digital certificates. Furthermore both malwares were programmed with what is known as "kill switch" (labeled as deactivation timer above), effectively limiting the malware's lifespan.

Duqu's creators seemed to have improved upon the command and control aspects of their malware. Instead of connecting to two previously configured web servers, Duqu's connection targets are either proxy servers relaying the connection to actual command and control servers or to other proxy servers in an attempt to improve command and control infrastructure. Mentioned earlier in the command and control process of the Stuxnet, Stuxnet had two hardcoded servers embedded within the malware's configuration file. Following this discovery, Iran was quickly able to contain the Stuxnet's further spread by separating the malware from its command and control servers (Falliere, O Murchu, and Chien, 2011, p. 7). Following the public discovery of the Duqu's existence, proxy servers, all running on virtual machines were removed on October 20, 2011, limiting the already constrained investigation options further (Symantec Security Reponse, 2011, p. 15).

The established differences of Stuxnet and Duqu become clearer as Duqu is used to steal the following information from the computer it infects. Initially downloading a harmless looking image containing the encrypted instructions for infostealing[5] from the infected target. Duqu gathers:

> "(1) Lists of running processes, account details, and domain information[6]; (2) Drive names and other information, including those of shared drives[7]; (3) Screenshots; (4) Network information (interfaces, routing tables[8], shares list,

[5] An infostealer is a sub type of a trojan malware, used by the Symantec to identify malwares gathering confidential information from an infected system such as credit card information, bank or email accounts, or login credentials (http-26).

[6] A domain in this context refers to the internal network, in other words, intranet

[7] Shared drives are data storage devices available to the all computers within the same internal network

[8] "A routing table maps destinations to the router and network interface that IP must use to reach that destination" (http-27)

etc); (5) Key presses; (6) Open window names; (7) Enumerated shares[9]; (8) File exploration on all drives, including removable drives; (9) Enumeration of computers in the domain through NetServerEnum[10]" (Symantec Security Reponse, 2011, p. 17).

The Symantec Security Response teams report that this infostealer module was updated three times while the investigations were ongoing. Updated modules were all seeking similar information to capture from an infected system. The final difference between the Stuxnet and the Duqu comes with the ability to extend the lifespan of the malware through module downloads mentioned above. Duqu comes equipped with a self-uninstallation protocol to remove itself from the infected hosts, if the advanced persistent campaign is deemed as end of life (Symantec Security Reponse, 2011, pp. 18-19).

4.1.2.2 Implications of the stolen data

Previous chapter has detailed some of the information Duqu was programmed to acquire from a host attackers infect with the spear phishing method. This section will examine what these information nuggets attackers exfiltrate may enable them to achieve.

4.1.2.2.1 Process list, account details, domain and network information

A populated process lists contains detailed information about what processes are currently being used in a computer system. This information alone may reveal the purpose of a computer within the internal domain as task oriented computers would be running software relating to that specific task. This task may range from controlling programmable logic controllers (PLC) to operating security cameras within a guarded complex. The figure below demonstrates some of the readily available information about the processes a Microsoft Windows operating system typically runs. This information also contains currently deployed end user system protection software, namely anti-virus programs or host-based

[9] As mentioned in the 6th footnote, enumeration action populates a list of all these network available shares

[10] Similar to enumerating shares, this action populates a list of all reachable computers within an internal network

intrusion detection systems (HIDS). This information provides the necessary background information for an attacker to exploit the system more effectively.

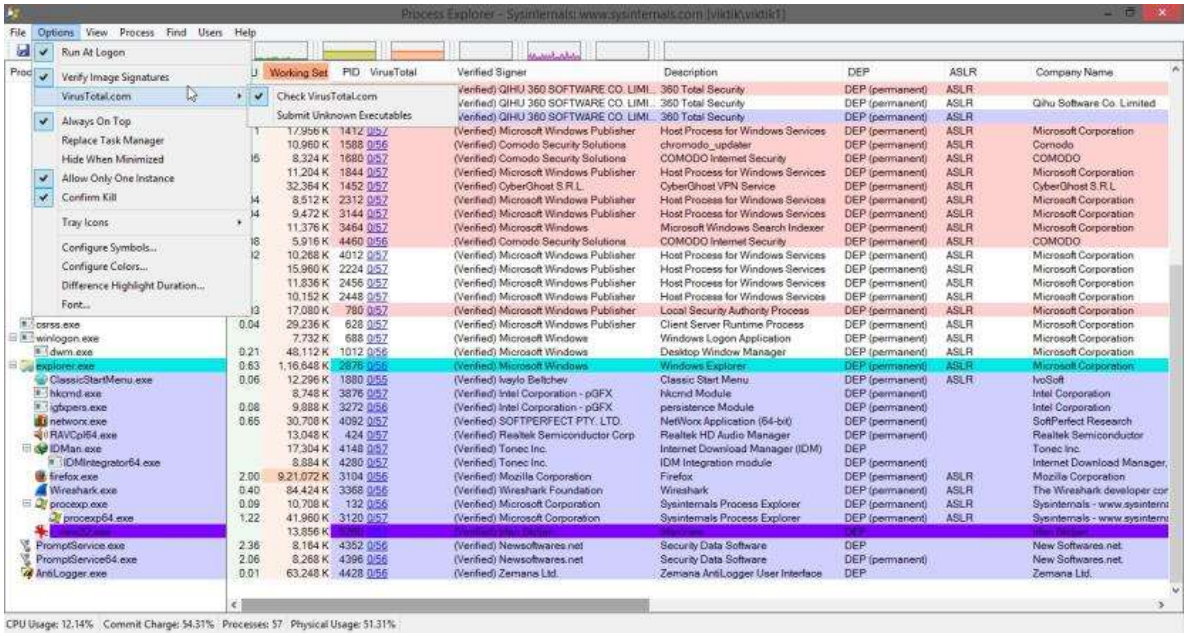


Figure 4.7. *An image excerpt from the software Process Explorer (http-28)*

Account details contain valuable information about the saved user names and passwords. If the currently infiltrated computer has clearance for accessing network drives, attacker would acquire this knowledge to improve their lateral movement capabilities. When combined with the domain information also provided, this could lead to total network compromise, depending on the clearance level of the compromised credentials. Network information contains data about the IP addresses of all reachable computers, routers, firewalls, and all network reachable cyberspace implements within the same network. Manufacturers of these implements, serial numbers, which operating systems they use, and given that most computers are named after their designated functions, the function they serve within the network are also reported to the attackers.

4.1.2.2.2 Local and network drives

This piece of the puzzle gives the complete file list of a computer at the hands of the attacker. Essentially laying their secrets bare for all to see. If the attacker had compromised

high enough clearance, network shared drives' contents would also be accessible through this bit of information. Following this, an attacker may choose to exfiltrate specific files or alter or destroy files and all copies of the said file.

4.1.2.2.3 Screenshots and keypresses

Figure 4.7 is also a screenshot of a computer system, running Microsoft's Windows operating system. A screenshot is a capture of what is displayed in the computer screen. The tool can be used to leak highly confidential documents, blueprints for a weapon, or even steal important piece of code that can be used by a cyber weapon. Nowadays, passwords are not directly displayed in the clear, at this point, keypresses captured by keylogging software will provide every keystroke user registers on their keyboard to the attacker. From personal information to usernames and passwords to bank accounts and credit card numbers can be exfiltrated with these tools. Given the inclination towards apocalypse level scenarios originating from cyberspace in the field of international relations, poorly generated and kept nuclear launch codes could too be compromised if they were ever entered into the cyberspace.

4.2 Non-Targeted Cyber Attacks

When compared to their targeted counterparts, non-targeted cyber-attacks are more often than not relatively harmless simply due to fact scope of damage that can be inflicted upon a computer network by denial of service (DoS) attacks are rather limited. Parallel to this point, while DoS attacks do target individual websites in their attacks, they are not operated within the framework of advanced persistent threats nor are they sophisticated as much as APTs. DoS attacks can be launched with a single line of command from any computer that has been made in the last twenty years. In comparison with real world warfare, an advanced persistent threat may be likened to a laser guided, satellite controlled missile whereas DoS attacks are more akin to artillery weapons of World War II era.

It is worth noting that while this section only examines the Estonian denial of service attacks, as established in earlier chapters, malware infections in secured networks could very well escalate into advanced persistent threats. Earlier sections of this chapter have dissected the Stuxnet worm and has demonstrated the stealthy destructive capabilities of targeted cyber-attacks. This thesis examines the Estonian denial of service attacks in this chapter due

to fact that it was the first well-documented case of a cyber-attack against the networks of a state actor, allegedly perpetrated by another state actor to cripple the cyber infrastructure of an "adversarial state" during peace time.

4.2.1 Estonian Denial of Service Attacks of 2007

The following section details the events what have been heralded by the media at time as the "first case of" (Mite, 2007) "cyberwar to disable Estonia" (Traynor, 2007). This section not only focuses on the underlying ethnic conflict between Russian Federation and Estonia but also examines the effects of the so called "cyberwar". Estonia's dependency on cyberspace to facilitate financial transactions as well as provide government services to its citizens under the "paperless government" (Herzog, 2011, p. 51) model has proven a weakness which its adversaries could and did exploit during the Bronze Soldier crisis.

4.2.1.1 Prelude to the attacks

This section examines the series of events deemed as a "wake-up call to other nations and the Alliance" by NATO (http-13), subsequently resulting in the creation of a cyber command for NATO and its allies designated the Cooperative Cyber Defence Centre of Excellence (CCDCOE) located in Tallinn, Estonia. During the political dispute between Estonia and the Russian Federation (RF) that had arisen from the proposed relocation of the Bronze Soldier, a war memorial dedicated to Soviet troops situated within the Tallinn city center to a newly constructed military cemetery, Estonia has come under distributed denial of service (DDoS) attacks lasting for 22 days. Rain Ottis, in his report to the CCDCOE on the Estonian DDoS attacks titled "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" highlights the dual identity of the war memorial. He states that the monument represents "liberator" for the local Russian minority whilst Estonians came to identify the monument as the "oppressor". He asserts that this duality was responsible for increasing the tensions between pro-Kremlin and Estonian nationalist movements (Ottis, 2008, p. 1). The duality of clashing identities between Estonian and Russian ethnicity did not simply happen overnight. Geographical location of the Estonia meant that during World War II, they could not stay neutral and had to choose a side. Occupied by both Nazi Germany and the Soviet Union during WWII, Estonia had suffered

under both regimes, however Alison Lawlor Russell in her work titled “Cyber Blockades” argues that during 1941, the “one year of Soviet occupation, Estonia had suffered greater losses than it did in the subsequent three years of Nazi rule” (Russell, 2014, p. 72). According to Russell, this view of the Soviet “liberation” served to divide the Estonian society “ethnically, linguistically, and culturally” (Russell, 2014, p. 73). This hostility stemming from the wounds left by the Soviet occupation has remained within the Estonian people, as they considered the Soviet occupation period between 1940 and 1991 as an illegal occupation. Summary executions, mass deportations, and resettlements have served to clinch the hatred towards the Soviet rule (Russell, 2014, p. 72). And following this political atmosphere, amid the clashing identities of Russian ethnicities versus Estonian nationalist, the work to move monument and the associated remains of fallen soldiers had commenced. The initially peaceful protests at the site had turned violent by the late evening of April 26, 2007. Following the violent outbursts, April 27 had marked the start of DDoS attacks (Ottis, 2008, pp. 1-2).

4.2.1.2 Beginnings of DDoS attacks and the aftermath of cyber-attacks

According to World Bank statistics, Estonia has enjoyed the benefits of increased cyber connectivity compared to rest of the European Union (EU) by having 66.19 percent of its population as active users compared to the EU’s median of 60.25 percent. Its small size at approximately 45,000 square kilometers meant that interconnectivity could be achieved with relative ease (http-14). This interconnectivity has resulted in the reliance on cyber infrastructure for Estonian people, even going so far as to use the internet for elections. At the time of the attack, approximately 98 percent of banking transactions were done through the internet (Russell, 2014, p. 71). This meant that DDoS attacks which lasted between 27 April and 18 May of 2007 affected Estonian banks and their customers the most. Due majority of attacks originating from outside of Estonia, as a countermeasure some Estonian banks chose to blacklist incoming external connections for the duration of the attacks. Upon inspection, malicious packets were discovered to contain Russian language, with Estonian governmental sites being targeted with profanities going as far as labeling the Estonian Prime Minister at the time, Andrus Ansip as “racist” (Ottis, 2008, p. 2).

Figure 4.8. *Attack instructions found on a web site during the event (Ottis, 2008, p. 3)*

Figure 4.8 details the instructions for how to initiate what is called as a "ping flood" on May 9, the Victory Day celebrated by the Russian Federation to commemorate the Allied victory in WWII. It targets the http://www.riik.ee web site, now moved to http://www.eesti.ee, which is the main website for Estonian governmental e-services. Command displayed in red within the figure above: "*ping –n 5000 –l 1000 www.riik.ee –t*" sends a ping request, in other words a question whether the host is operational and accepting connections, to the computer hosting riik.ee, 5,000 times with 1,000 bytes of data as opposed to 32 bytes of data used in legitimate purposes, until manually stopped (http-19). The Victory Day brought with it an intensive data packet bombardment, reaching up to 4 million packets a second, included 58 separate botnets with zombies reaching up to a million computers. Estonia might have enjoyed tightly knit cyber infrastructure, however was not up to the task of servicing 95 megabits per second through their servers. Even though Russian state had denied any involvement, Urmas Paet, Estonian foreign affairs minister at the time, had stated that "IP

addresses of some of the attacking computers were inside Russian government institutions, including the president's administration" (Russell, 2014, pp. 76-77).

The attacks lasted twenty two days and have impacted the daily life of everyone in Estonia significantly. Financial transactions between users and banks were failing due to the overload of the networks, attackers had disabled email servers of the parliament, hampering the state of Estonia's ability to communicate internally and externally, almost all devices operating on a client-server architecture over the internet were unable to operate. Stephen Herzog in his work titled "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses" estimates these attacks to have costed Estonia around "$1 million in damages" (Herzog, 2011, p. 52).

Eventually, an ethnically Russian Estonian individual named Dmitri Galuškevitš was fined for organizing a DDoS attack against a political party's web site in Estonia based on the evidence gathered which shows that he perpetrated the attack from within the Estonia. According to Martin C. Libicki in his work titled "Cyberdeterrence and Cyberwar", "considerable evidence suggests that he had help from the parts of the Russian mafiya [sic], which helped organize hijacked computers for him" (Libicki, 2009, p. 2). However in the conditions of 2007, previously mentioned count of 58 botnets would require more than one individual to compromise, tend to, and operate. While the evidence collected did prove his crime, he was not the sole perpetrator of this grand orchestration.

Symptoms of escalating tensions between the Russian Federation and Estonia did not stay limited to the cyberspace. Organized Russian youth groups in Moscow had surrounded the Estonian embassy, which escalated to tearing down the Estonian flag. Relaying from the reports at the time Russell states that, Nashi, one of the more prominent groups within the protestors with ties to the Russian government, going as far as paying protestors to make an appearance during the six days the Estonian embassy remained besieged (Russell, 2014, p. 77).

The interconnectivity of Estonia had yielded to the challenge of external cyber interference, essentially diminishing the Estonian state's capability to provide services to its citizens. Previously mentioned history between the Estonian and Russian peoples combined with the inability to access services, media, and critical information has caused panic amongst the Estonian people. As expected, no permanent damage or loss of life were reported by these

attacks, and the Bronze Soldier was eventually moved to his new home. Russia continued to deny the allegations of being involved in the cyber-attacks, with Deputy Press Secretary for the Russian President Dmitriy Peskov replying to the allegations with "Russia can no way be involved in cyber terrorism, and all claims to the contrary are an absolute lie" (Russell, 2014, p. 82).

CHAPTER 5

5. CURRENT CYBER STRATEGIES IN WESTERN NATIONS

Previous chapters have examined and discussed the cyber threats concerning the denizens of the cyberspace, state and non-state actors alike. This chapter focuses on the state strategies regarding securing states' interests in cyberspace. This chapter focuses on strategies put forth by the Western bloc only due to its reliance on the deterrence theory. Given that Stuxnet and its later variant, namely Duqu, are suspected to have emerged from the Western bloc and their allies, the cyber strategies of these countries it would be beneficial to examine.

5.1 The United States of America

The White House has released a report detailing the cyber strategy of the United States of America titled "National Cyber Strategy of the United States of America" in September, 2018. The report signed by the sitting President of the United States of America, Donald J. Trump, claims that "with the release of this National Cyber Strategy, the United States now has its first fully articulated cyber strategy in 15 years" (Trump, 2018, p. I). The report singles out the Russian Federation, the Islamic Republic of Iran, the People's Republic of North Korea as well as the People's Republic of China for engaging in cyber-attacks against American international businesses and its allies. Furthermore the report states that non-state actors exploited the cyberspace created with the American vision of "free expression and individual liberty", "to profit, recruit, propagandize and attack United States and its allies" while enjoying the protection of hostile states to United States of America (Trump, 2018, pp. 1-2). This section of the thesis examines relevant sections of the report released by the White House in conjunction with the preset goals of the thesis with relative perceived threats and countermeasures against these threats examined in this thesis being the primary focus.

To combat the aforementioned challenges posed by its adversaries, the report details and explains the four pillars, upon which the national cyber strategy of United States of America will be founded. “Pillar I: Protect the American People, the Homeland, and the American Way of Life; Pillar II: Promote American Prosperity; Pillar III: Preserve Peace through Strength; Pillar IV: Advance American Influence” (Trump, 2018, pp. V-VI).

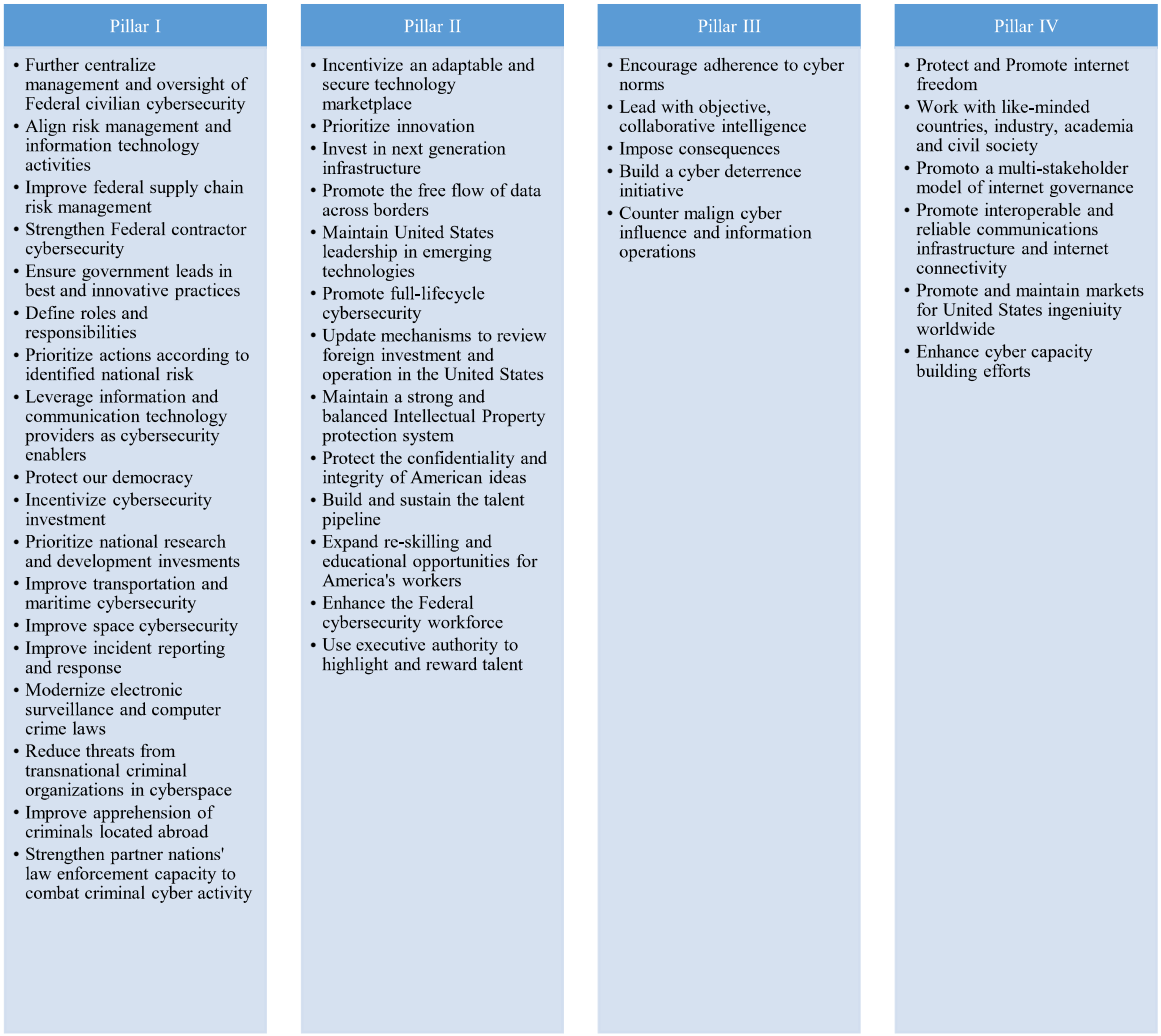


Figure 5.1. *Pillars upon which the National Cyber Strategy of the United States of America stands (Trump, 2018, pp. V-VI)*

In the report, Trump administration defines the objective of the first pillar as “manage cybersecurity risks to increase the security and resilience of the Nation’s information and information systems” (Trump, 2018, p. 6). The Trump administration aims to achieve this objective through focusing on outlined priority actions, in order to secure the federal

networks, The Trump administration promises to enable the Department of Homeland Security (DHS) with The Office of Management and Budget's (OMB) oversight to secure all federal and agency networks through improved compliance with standards, policies and applicable laws (Trump, 2018, pp. 6-7). The report mentions that Chief Information Officers (CIO) would be empowered to align cybersecurity risk management decisions with the information technologies (IT) budgeting while implementing supply chain risk management tools to ensure that all technology government deploys is secured through increased interdepartmental information connectivity to raise awareness against supply chain risks going as far as banning risky vendors (Trump, 2018, p. 7), as was the case for recent sanctions against the Huawei with President Trump ordering Huawei to be blacklisted from doing any business with American companies (Keane, 2019).

In order to strengthen the federal contractor cybersecurity, the Trump administration proposes more action-oriented approaches toward contractors' risk management practices by monitoring testing, hunting, and responding processes through authorizing Federal departments to take part in similar exercises. In other words, Federal agencies should be able to conduct their own cybersecurity exercises similar to what CCDCOE has been doing within NATO. In a bid to increase resilience towards the threat of quantum computers' ability to break public encryption keys, Trump and his administration appoints the National Institute of Standards and Technology (NIST) with evaluating quantum-resistant public key algorithms (Trump, 2018, pp. 7-8). If the current public key algorithms were to be broken by quantum computers, secured connections in the internet would be in jeopardy, leaving all traffic exposed to discovery and manipulation by all actors.

Focusing on the second pillar, the Trump administration defines the objective of Pillar II as to "preserve United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation and efficiency" (Trump, 2018, p. 14) The report mentions that the United States should prioritize innovation by promoting and implementing continuous updates of standards and best practices, while investing in next-generation infrastructure of telecommunication and information communication networks, namely 5G network, quantum computing, artificial intelligence, while being risk aware to deter hazards and evolving threats in all areas of cyberspace (Trump, 2018, pp. 14-15). National cyber strategy aims to push back against the restriction of free

flow of information across borders as the report states that "restrictive data localization and regulations as pretexts for digital protectionism under the rubric of national security" (Trump, 2018, p. 15) negatively impact companies of United States' ability to compete in the cyberspace and views this competitiveness as paramount for maintaining the United States leadership in emerging technologies. Through trade-related engagements, the national cyber strategy aims to promote innovation all while exposing oppressive regimes that use these tools and services to undermine human rights. The Trump administration proposes to promote awareness for strong, default security settings, meaning that internet of things (IoT) devices should no longer be able so easy to take over, as mentioned previously in this work within the denial of service chapter. The report states that crowd-sourced vulnerability testing and disclosure could improve the resiliency prior to any computer network exploitation attempts. Regarding the education of Federal workers, report aims to increase cybersecurity competitiveness through building talent pipeline by investing in programs that aim to increase domestic talent output as well as utilize the "President's proposed merit-based immigration reforms" (Trump, 2018, p. 17) to sharpen the competitive edge of the United States in cybersecurity.

In the third pillar of the report, the Trump administration defines its objective as to "identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace" (Trump, 2018, p. 20). With one of the priority actions defined under this pillar, the United States aims to encourage all states to affirm and adhere to international law and non-binding norms regarding the stability of the cyberspace by promoting greater predictability through universalizing acceptable behavior within the confines of the cyberspace. Expanding further upon this predictability, the United States aims to employ all assets of national power to prevent and respond to, or deter, malicious cyber activity within areas such as diplomacy, finance, information, military, as well as law enforcement to deter further malicious cyber activity against the United States (Trump, 2018, pp. 20-21). According to the report, the United States will coordinate with like-minded states to create a cyber deterrence initiative to follow up on attribution claims and share intelligence to send a strong message toward malignant actors. Through increased coordination between the United States and foreign government partners as well as the private sector and academia, the United

States aims to take stern stance against the flood of online malign influence and propaganda campaigns perpetrated by United States' adversaries (Trump, 2018, p. 21).

The report defines the objective for the final pillar of the National Cyber Strategy of the United States as to "preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by United States interests" (Trump, 2018, p. 24). The Trump administration's report views the internet freedom as online exercising of human rights and aims to encourage this freedom that enhances international commerce and innovation with respect to cybercrime and counterterrorism efforts. The report reiterates the need for coordination with stakeholders, namely like-minded states, industries, academies and civil societies, to promote a multi-stakeholder approach and to improve internet freedoms and counter the rising tide of authoritarianism. With this cyber strategy Trump administration aims to promote the interoperability of communications infrastructure and internet connectivity by investing in interoperable, reliable systems to counter the statist influences being felt within the areas that the United States and its companies currently compete within (Trump, 2018, pp. 24-26).

The recent National Cyber Strategy for the United States of America remarks on some valuable points. Complete explanation of the policy in regards to interstate cooperation and multi-stakeholder approaches would not fall within the predefined limits of this thesis. Therefore this thesis will only focus its examination on the technical areas that stand out. The aforementioned quantum computers' ability to break public key encryptions is especially relevant to state security. Researchers predict that the current encryption algorithm may be safe for the next 20 years (http-29) while quantum computers are still in infancy but unless a security improvement is achieved now, encrypted documents in the future may be exposed to an attack. The previous chapters have shown the ability of Duqu to exfiltrate data through covert means. The encrypted documents exfiltrated today may have their encryption broken by these quantum computers in the future, leading to undesirable outcomes for the state actors and their stakeholders such as defense contractors and government employees. The report also states that information systems should be interoperable, reliable, secure and up to date as well as be open for improvements. The previous chapters have demonstrated the outcome of zero-day vulnerabilities. These vulnerabilities exist within systems that may be present unknown to the users and developers alike. Given that cyber weapons are getting more

sophisticated every time new a variation is discovered, a new approach toward securing data might be necessary. One of the key lessons to be learned from this new strategy is the importance of education. Duqu was able to infect systems with spear phishing attacks, meaning that, personalized and legitimate emails were infected with the cyber weapon to compromise targets. This report falls short on detailing on what kind of educational policies President Trump and his administration will focus however, a secure network is as safe as its weakest link. This weak link is quite often happens to be the users, namely, humans. Generational cyber awareness gap can only be eliminated through extensive education programs as pinning the network security squarely on the shoulders of few network administrators would not result in the expected security. More likely, the false sense of security provided would lead to even further compromises that, in turn, may lead to further cyber weapons similar to Stuxnet, with the ability to affect the physical world more profoundly.

5.2 The European Union

In an effort to extend European Agency for Network and Information Security (ENISA) to help member states dealing with cyber-attacks, the EU Cybersecurity Act was proposed in 2017. In his State of the Union address President Jean-Claude Juncker stated that "In the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber-attacks. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks" (http-30). Report references that more than 4,000 ransomware attacks in the year of 2016 and 80 percent European companies did experience at least one cyber incident. EU Cybersecurity Act proposes yearly cyber exercises titled "Pan-European Cybersecurity Exercises" to improve threat intelligence sharing in a bid to improve the preparedness of the cyber infrastructure of the European Union. The EU Cybersecurity Act of 2017 aims to increase EU's cybersecurity capacity in a five-step plan. In the first step of the plan, EU aims to set up a European Cybersecurity Research and Competence Centre that will improve member state coordination on a national level to provide the tools and technology to defend the EU against cyber weapons employed by the cyber criminals in cyber space. Within the second step of the plan, the EU plans to come up with a blueprint operational plan to improve

the Union's cyber response capabilities against large-scale cyber-attacks by establishing an 'EU Cybersecurity Crisis Response Framework'. The third step of the plan to increase the EU's cyber capacity entails increased solidarity between member states through a new proposed 'Cybersecurity Emergency Response Fund' to aid member states at a time of crisis that is similar to physical protection mechanisms already in place within the European Union framework. The Fourth step of the plan describes the efforts to increase the cyber defense capabilities of the EU by releasing grants from European Defence Funds to support cyber defense initiatives. This step of the plan also aims to address the 'skills gap' in cyber defense by creating education and exercise platforms in cooperation with the NATO. In the final step of the plan, EU aims to increase international cooperation through "implementing the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, supporting a strategic framework for conflict prevention and stability in cyberspace" (http-30) to assist the third countries in this endeavor.

The EU Cybersecurity Act has passed on December 11, 2018 (http-31), extending the mandate of the ENISA permanently and providing the basis for a new cybersecurity certification framework in an effort to improve assistance towards member states. As was the most important issue in the National Cyber Strategy of United States of America, the knowledge gap, the lack of educational resources, or the skills gap, in cybersecurity has started to appear in the agenda for some of the most cyber reliant countries. Cyber defense and offense strategies could very well serve to improve international cooperation within the cyber domain and extend it beyond the limits of traditional domains due to the differences of the cyberspace covered within the initial chapters of this thesis.

CHAPTER 6

6. FUTURE OF THE CYBER DOMAIN AND CONCLUSIONS

This chapter of the thesis focuses on some of the future scenarios that state-level actors and non-state actors may encounter through increased interdependence and interconnectivity of computer systems, and, it tries to summarize the conclusions of the thesis. Science pursues human enhancements in areas proving beneficial to the skills of workforce or simply to our

daily lives. On the other hand, the convenience of connectivity and Moore's Law[11] may lead to an entirely unmanned warfare. Nowadays, remote controlled unmanned aerial vehicles (UAV) are gaining in popularity for a multitude of purposes among militaries due to their flexibility. Returning to the chapter where the purpose of this thesis was defined, a cross-domain maneuver was exemplified with the following: "a drone operating out of a carrier positioned in international waters, deploying a computer guided missile, while communicating multitude of data to a remote computer via satellites in orbit". This example includes all branches of the operational domain: land, sea, air, space, and cyber. The success of the maneuver is dependent on all the operators of operational domains to operate interdependently. Militaries may try to improve their members through invasive and non-invasive implants, brain computer interfaces (BCI), head mounted displays (HMD). Even these upgrades could be interconnected and they could even download and update their information from the Internet. Head mounted displays could be reduced to the size of ordinary goggles, instead of relying on input from external, it may enable control of the system through brain computer interfaces implanted in or attached to the cranium of a person. Nick Bostrom, the author of the simulation theory has described benefits of the brain computer interfaces in his work titled "Superintelligence: Paths, Dangers, Strategies" as "perfect recall, speed and accurate arithmetic calculation, high bandwidth data transmission" (Bostrom, 2016, p. 54). Bostrom states that from these operations infections may develop leading to hemorrhages, electrodes may displace, rending the implant useless, while still unproven scientifically, these implants may lead to cognitive decline. According to Bostrom, these negative side effects are too much for able individuals to voluntarily submit to these invasive and permanent operations, therefore limiting the development of the brain control interfaces as a handicap elimination technique (Bostrom, 2016, pp. 54-55).

A recent work performed in the area of Transcranial Magnetic Stimulation (TMS), has lowered the expertise floor required for employing the technique, therefore shifting the limited accessibility of the technique towards more accessible. Thus creating the conditions

[11] Commonly referred in IT field, Moore's Law is a "computing term which originated around 1970; the simplified version of this law states that processor speeds, or overall processing power for computers will double every two years" (http-32)

for its misuse by either state or non-state actors. Michael Dando, in his work titled "Neuroscience Advances and Future Warfare" reports from Jonathan D. Moreno, TMS could be employed for "erasing the memory of someone to make him unable to disclose information under interrogation or to enhance the ability of a terrorist to carry an attack" (Dando, 2015, p. 1790). Mark Hallett defines TMS as "a technique for noninvasive stimulation of the human brain" (Hallett, 2007, p. 187). Non-invasive in this context means without any incisions or insertion of equipment or apparatus. TMS employs magnetic coils placed over subject's head to produce magnetic fields, briefly activating or inhibiting the brain (Hallett, 2007, p. 188). In a recent study titled "Transcranial Direct Current Stimulation Use in Warfighting: Benefits, Risks, and Future Prospects" Steven E. Davis and Glen A. Smith report on the effects of transcranial direct current stimulation (tDCS) for military personnel. While TMS uses magnetic coils to induce an electric field to activate or inhibit subject's brain, tDCS employs electrodes placed in anodal and cathodal positions to provide direct current. This in turn, creates mobility and portability compared to TMS application. During field operations, aforementioned mobility could be the key difference in a life and death situation. Davis and Smith have reported in their work that the anodal stimulation of certain cortices could help improve a soldiers tactical capabilities by enhancing visual and auditory responses thus resulting in improved situational awareness (Davis and Smith, 2019, p. 3).

Ordinary infantry squads may be replaced with robots that can be remote controlled through what is called telepresence by the military. In essence, these robots may be employed in hazardous environments without risking valuable human life to achieve hazardous goals. Already, small robots are being employed to defuse improvised explosive devices (IED). In future applications of remote controlled robots may range from law enforcement to orbital construction. In a similar setting, self-driving vehicles are being developed with haste by a multitude of manufacturers and independent parties. Adopting these technologies into the military domain would lead to interesting security and legal challenges as well as fuel the philosophical debate for decades to come. As established so far within the confines of this work, securing a system is far harder than exploiting and taking control over it. Seeking out vulnerabilities, potentially and practically exploiting these vulnerabilities may result in higher gratification levels in malware and cyber weapon developers compared to cyber

defense specialists, with whom the burden of cyber defense lies. These automation opportunities will of course result in unemployment affecting the society at large, no doubt raising interesting questions in due time. However current outlook seems that at the very least, cyber offense and defense focused jobs would remain in constant demand for the duration of the cyber revolution. As examined within the cyber strategies chapter of this work, only now the skill gap is being addressed by the states. Undoubtedly, future generations would need to be raised in accordance with the countermeasures to be taken by the aforementioned policies, aimed at eliminating this skill gap.

Cyber weapons are here to stay. States and non-state actors may start to develop these even further, using cyber espionage tools like Duqu to gather digital certificates, software source code of critical infrastructure to reverse engineer and to use in cyber weapons specific to these critical infrastructures. Lack of attribution has come to be viewed something vilified by international law and International Relations due to cyber-attacks causing up to trillions of dollars in intellectual property loss, in the case of Stuxnet, costing teams valuable development time and may go as far as damaging the credibility of the programs that such cyber weapons target. While these may seem like negative outcomes of the cyberspace's global proliferation, the challenges may bring with them the opportunity to exploit untold new resources both in cyber and human domains.

Current progress on artificial intelligence research is still at its infancy. Current generation of the artificially intelligent software may distinguish between two pictures, animate images from a single frame or may be deployed to monitor and sever malicious connections. These examples are only a few task oriented intelligences developed to perform a specific task by self-learning. An actual artificial intelligence would be on par with human intelligence. Philosophical questions aside, literature is currently brimming with negative scenarios detailing the consequences of this event. James Cameron's popular movie titled "The Terminator" tells the story of an alternate reality, where the artificial intelligence named Skynet, developed with the single purpose of "defending the world" began assimilating data at an exponential rate. The panicked human response to this action was to shut down the Skynet, which led to the Skynet to categorize attempts of its controllers as an act of attack, resulting in global thermonuclear annihilation, nearly eradicating the human race. Figure 6.1

details the differences between artificial intelligence, deep learning networks and machine learning in an attempt to clarify bring some order into the terms.

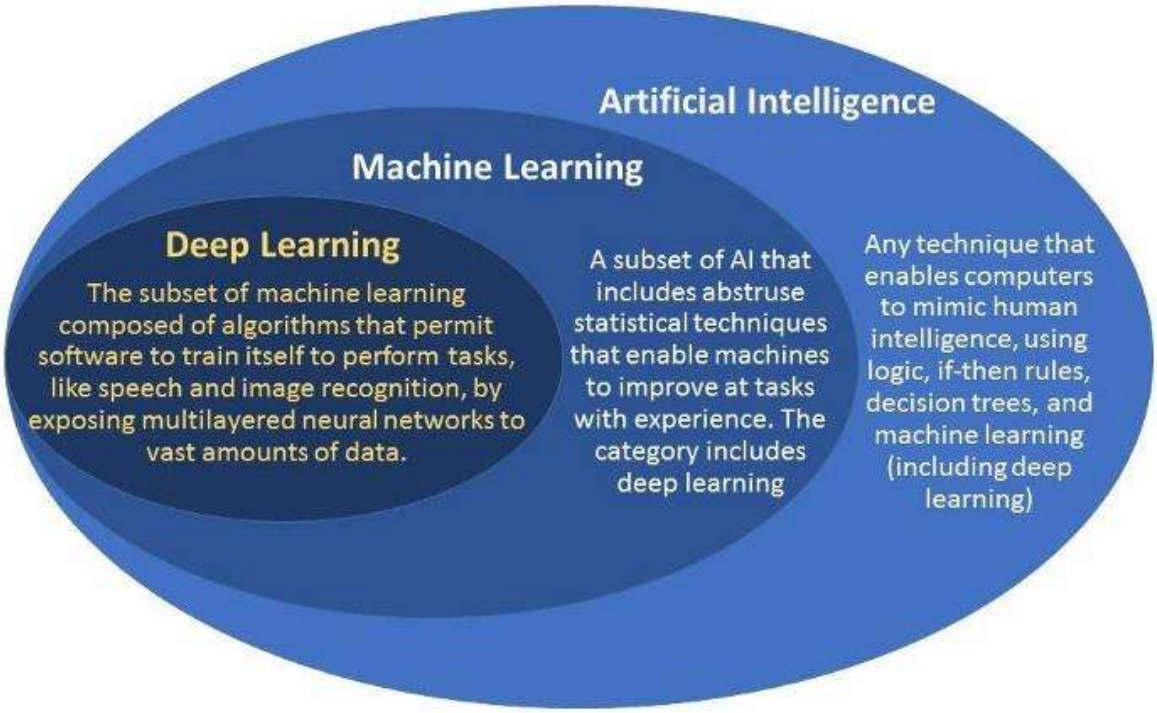


Figure 6.1. *Differences between the three fields of study for artificial intelligence (Bahmani, 2018)*

Future remains uncertain on whether if we will ever develop a true artificial intelligence. Among the fears of possible Skynet scenario, one thing will remain certain, in the event of a superintelligence becoming reality, future would no longer belong to the humans alone.

Before we get there however, the multidisciplinary field of cyberspace has plenty of hurdles and dilemmas on its plate. International law regarding cyberspace barely exists, leaving the domain of cyber in total anarchy while the field tries to catch up. Cyberspace however, is not a static entity, it shifts and changes with time. Rendering previous Meta obsolete. Cyber security researchers are uncertain whether if we will ever see a cyber war. Some experts are claiming “a digital Pearl Harbor” may be at the gates, with all areas of cyber dependent life falling face first into chaos. Certainly, an industrial control sabotage may lead to another Chernobyl, but so can a guided missile. Of course, infected SCADA systems may open dam gates, flooding towns below, killing thousands, but so can a terrorist attack. If there is anything certain this work may conclude, it is that perfect security, cyber or

physical, does not exist. We can only educate and train the users on ever changing dangers of advanced persistent threats in a bid to improve secure network security with preventive measures. We could speed up the law making process to keep up with the speed of advancements in the cyber domain, but law does not prevent misdeeds or stop malicious actors on its own. Failing this we may have to stop using technology. But just as the case in Pandora's Box, we may never be able to go back to a traditional world without all the evils and goods of technology.

The previous chapters have explained the current situation in cyber domain. States are facing new challenges they are ill equipped to tackle the challanges head on. As one of the primary hypotheses of this thesis, education gap regarding cyber domain on policy maker level is leading to a total lack of comprehensive and inclusive cyber strategies. It is worth mentioning that this thesis does not try to convey that cyber strategies could somehow future-proof the security in cyber domain. This is simply not the case because the speed through which the cyber domain evolves. While some states may have assumed more active roles in cyber domain, most of the states, including some of the most powerful ones, are still playing the reactionary role. Educating policy makers is simply the first step towards creating better cyber strategies which will benefit not only the state in question but the whole of international community.

The newest threat to emerge against states is the cyber weapon. This thesis has proved that cyber weapons are now indeed reality through detailed examination of the Stuxnet worm. A stealth weapon which went undetected for almost a year and managed to destroy 1000 gas centrifuges in Natanz Fuel Enrichment Plant. International community has to react and discuss the possibilities of cyber weapons. Stuxnet was not an intelligent cyber weapon however, with the right code, it could be the deadliest one yet. Even with the lack of human casualties through cyber acts so far, the interconnectivity and cyber dependence will only increase with time, creating more attack vectors for attackers to be. This thesis recommends future research regarding the use and development cyber weapons, as they are just as destructive as a nuclear weapon in capable hands.

Summarizing the earlier chapters, security is a never-ending process. Cyber security is even more-so, as the threats are constantly evolving. This burden of security falls squarely on system administrators and cyber security experts, yet they cannot bear this burden alone

without proper cyber security strategies set by the policy makers. Connecting with the earlier hypothesis regarding the importance of education, in order to provide the maximum amount of safety, states need to improve their education regarding cyber domain. Cross domain operations are heavily dependent on the cyber domain and as a future research project, a sixth operational domain, human domain, may emerge which would include the system administrators and cyber security experts mentioned earlier.

Literature research regarding the cyber domain in International Relations fail to account the technical aspects of cyber domain. Cyberspace and cyber domain is a multidisciplinary field. Unlike nuclear weapons, effects of cyber weapons cannot be simplified to 'total annihilation across an area'. Without technical knowledge about limits and possibilities of cyber domain, healthy discussion regarding state actions in cyberspace could not proceed. And due to this lack of understanding, future research regarding cyber weapons and cyber defense strategies would fall short of helping the international community. International Relations, international community, policy makers, non-state actors and humans have one common ability, the ability to adapt. To survive and better the future, we must adapt and overcome the challenges presented by the fifth operational domain.

REFERENCES

Abraham, S. (2018, January 09). *12+ Types of Malware Explained with Examples (Complete List)*. Retrieved 30 May, 2019, from MalwareFox: https://www.malwarefox.com/malware-types/

Albright, D., Brannan, P., and Walrond, C. (2010). *Did Stuxnet Take out 1,000 Centrifuges at the Natanz Enrichment Plant.* Washington, D.C.: Institute for Science and International Security.

Albright, D., Brannan, P., and Walrond, C. (2011). *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report.* Washington, D.C.: Institute for Science and International Security. Retrieved 09 June, 2019, from http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf

Bahmani, M. (2018, November 07). *AI vs Machine Learning vs Deep Learning*. Retrieved 07 June, 2019, from Medium: https://medium.com/datadriveninvestor/ai-vs-machine-learning-vs-deep-learning-ba3b3c58c32

Baskin, B., Bradley, T., Faircloth, J., Schiller, C. A., Caruso, K., Piccard, P., . . . Piltzecker, T. (2006). Chapter 1 - An Overview of Spyware. In B. Baskin, T. Bradley, J. Faircloth, C. A. Schiller, K. Caruso, P. Piccard, . . . T. Piltzecker, and T. Piltzecker (Ed.), *Combating Spyware in the Enterprise* (pp. 1-25). Syngress.

Bencsáth, B., Pék, G., Buttyán, L., and Félegyházi, M. (2011). *Duqu: A Stuxnet-like malware found in the wild.* Budapest: Laboratory of Cryptography and System Security (CrySyS).

Bencsáth, B., Pék, G., Buttyán, L., and Félegyházi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, 971-1003. doi:10.3390/fi4040971

Bostrom, N. (2016). *Superintelligence Paths, Dangers, Strategies.* Oxford: Oxford University Press.

Cameron, J. (Director). (1984). *The Terminator* [Motion Picture].

Chen, P., Desmet, L., and Huygens, C. (2014). A Study on Advanced Persistent Threats. In B. De Decker, and A. Zúquete (Ed.), *Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science. 8735*, pp. 63-72. Berlin: Springer. doi:10.1007/978-3-662-44885-4_5

Chien, E. (2010, November 12). *Stuxnet: A Breakthrough*. Retrieved 09 June, 2019, from Symantec Connect Community: https://www.symantec.com/connect/blogs/stuxnet-breakthrough

Christou, G. (2016). *Cybersecurity in the European Union Resilience and Adaptability in Governance Policy.* Hampshire: Palgrave Macmillan.

Clarke, R. A., and Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* New York, NY: HarperCollins.

Dando, M. (2015). Neuroscience Advances and Future Warfare. In J. Clausen, and N. Levy, *Handbook of Neuroethics* (pp. 1785-1800). New York: Springer Science+Business Media Dordrecht.

Davis, S. E., and Smith, G. A. (2019). Transcranial Direct Current Stimulation Use in Warfighting: Benefits, Risks, and Future Prospects. *Frontiers in Human Neuroscience, 13*, 1-18. doi:10.3389/fnhum.2019.00114

Eggenschwiler, J., and Silomon, J. (2018). Challenges and opportunities in cyber weapon norm construction. *Computer Fraud & Security, 2018*(12), 11-18. doi:10.1016/S1361-3723(18)30120-9

Falliere, N., O Murchu, L., and Chien, E. (2011, February 11). *W32.Stuxnet Dossier.* Retrieved 15 June, 2019, from Symantec: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Fontugne, R., Bautista, E., Petrie, C., Nomura, Y., Abry, P., Goncalves, P., . . . Aben, E. (2019). BGP Zombies: An Analysis of Beacons Stuck Routes. In D. Choffnes, and M. Barcellos (Ed.), *Passive and Active Measurement. PAM 2019. Lecture Notes in Computer Science. 11419*, pp. 197-209. Cham: Springer.

Ford, R. (1999). Malware: Troy Revisited. *Computers & Security, 18*(2), 105-108. doi:10.1016/S0167-4048(99)80027-3

Gediya, J., Singh, J., Kushwaha, P., Srivastava, R., and Wang, Z. (2019). 7 - Open Source Software. In R. Oshana, and M. Kraeling (Eds.), *Software Engineering for Embedded Systems* (pp. 207-244). Cambridge, MA: Elsevier.

Gibney, A. (Director). (2014). *Zero Days* [Motion Picture].

Gibson, W. (1984). *Neuromancer.* New York: Ace.

Goodin, D. (2016, September 29). *Record-breaking DDoS reportedly delivered by >145k hacked cameras*. Retrieved 25 June, 2019, from Ars Technica: https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

Hallett, M. (2007). Transcranial Magnetic Stimulation: A Primer. *Neuron*, 187-199. doi:10.1016/j.neuron.2007.06.026

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49-60. doi:10.5038/1944-0472.4.2.3

International Telecommunication Union. (1994, July 01). *ITU-T Recommendations Database.* Retrieved 15 May, 2019, from International Telecommunication Union: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=2820&lang=en

Kaplan, J. (2016). *Artificial Intelligence: What Everyone Needs to Know.* New York: Oxford University Press.

Keane, S. (2019, July 15). *Huawei ban: Full timeline on how and why its phones are under fire*. Retrieved 15 July, 2019, from Cnet: https://www.cnet.com/news/huawei-ban-full-timeline-on-how-and-why-its-phones-are-under-fire/

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr, and L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 24-42). Washington, D.C.: Potomac Books.

Langner, R. (2013). *To Kill a Centrifuge.* Arlington: The Langner Group.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies, 22*(3), 365-404. doi:10.1080/09636412.2013.816122

Liska, A., and Gallo, T. (2017). *Ransomware Defending Against Digital Extortion.* Sebastopol, CA: O'Reilly.

Lysne, O. (2018). *The Huawei and Snowden Questions Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment.* Cham: Springer.

Manky, D. (2017, November 14). *Fortinet Predicts Highly Destructive and Self-learning "Swarm" Cyberattacks in 2018*. Retrieved 25 June, 2019, from Fortinet:

https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2017/predicts-self-learning-swarm-cyberattacks-2018.html

Matrosov, A., Rodionov, E., and Bratus, S. (2019). *Rootkits and Bootkits Reversing Modern Malware and Next Generation Threats.* San Francisco: No Starch Press.

Matrosov, A., Rodionov, E., Harley, D., and Malcho, J. (2011). *Stuxnet Under the Microscope: Revision 1.31.* ESET LLC. Retrieved 09 June, 2019, from http://daveschull.com/wp-content/uploads/2015/05/Stuxnet_Under_the_Microscope.pdf

Mazanec, B. M., and Thayer, B. A. (2015). *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace.* Basingstoke: Palgrave Macmillan. doi:10.1057/9781137476180.0005

Mite, V. (2007, May 30). *Estonia: Attacks Seen As First Case Of 'Cyberwar'*. Retrieved 11 June, 2019, from Radio Free Europe / Radio Libery: https://www.rferl.org/a/1076805.html

Mueller, P., and Yadegari, B. (2012). *The Stuxnet Worm.* University of Arizona, Department of Computer Science. Retrieved 08 June, 2019, from https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf

National Institute of Standards and Technology. (2015, January 01). Security and Privacy Controls for Federal Information Systems and Organizations. *National Institute of Standards and Technology Special Publication 800-53, Revision 4*. Gaithersburg, Maryland, United States of America. doi:10.6028/NIST.SP.800-53r4

Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Tallinn: Cooperative Cyber Defence Centre of Excellence.

Paul, C., Porche, I. R., and Axelband, E. (2014). *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces.* Santa Monica, CA: RAND.

Pauli, D. (2011, December 09). *Stuxnet a 'perfect match' to Iran nuclear facility, photo reveals*. Retrieved 08 June, 2019, from iTnews: https://www.itnews.com.au/news/stuxnet-a-perfect-match-to-iran-nuclear-facility-photo-reveals-282735

Prowell, S., Kraus, R., and Borkin, M. (2010). *Seven Deadliest Network Attacks.* Burlington, MA: Syngress.

Raiu, C. (2010, July 21). *Stuxnet signed certificates frequently asked questions*. Retrieved 05 June, 2019, from Securelist: https://securelist.com/stuxnet-signed-certificates-frequently-asked-questions/29725/

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

Robinson, M., Jones, K., and Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*(49), 70-94. doi:10.1016/j.cose.2014.11.007

Ruggiero, P., and Heckathorn, M. A. (2012). *Data Backup Options.* Retrieved 30 June, 2019, from Cybersecurity and Infrastructure Security Agency: https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf

Russell, A. L. (2014). *Cyber Blockades.* Washington, D.C.: Georgetown University Press.

Sanger, D. E. (2012, June 01). *Obama Order Sped Up Wave of Cyberattacks Against Iran*. Retrieved 15 May, 2019, from The New York Times: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Schmitt, M. N., and Vihul, L. (Eds.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press.

Singer, P. W., and Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Smith, A., Papadaki, M., and Furnell, S. M. (2013). Improving Awareness of Social Engineering Attacks. In R. C. Dodge, and L. Futcher (Ed.), *Information Assurance and Security Education and Training. WISE 2009. IFIP Advances in Information and Communication Technology. 406*, pp. 249-256. Berlin, Heidelberg: Springer.

Sood, A. K., and Enbody, R. (2014). *Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware.* Waltham: Elsevier.

Stiennon, R. (2015). A short history of cyber warfare. In J. A. Green (Ed.), *Cyber Warfare A Multidisciplinary Analysis* (pp. 7-32). New York: Routledge.

Symantec Security Reponse. (2011). *W32.Duqu.* Mountain View, CA: Symantec. Retrieved 12 June, 2019, from

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Tamkin, E. (2017, April 27). *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?* Retrieved 10 June, 2019, from Foreign Policy: https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

Traynor, I. (2007, May 17). *Russia accused of unleashing cyberwar to disable Estonia*. Retrieved 11 June, 2019, from The Guardian: https://www.theguardian.com/world/2007/may/17/topstories3.russia

Trump, D. J. (2018). *National Cyber Strategy of the United States of America.* Washington, D.C: The White House.

Weaver, N., Paxson, V., Staniford, S., and Cunningham, R. (2003). A taxonomy of computer worms. *In Proceedings of the 2003 ACM workshop on Rapid malcode* (pp. 11-18). ACM.

Yan, S. Y. (2019). *Cybercryptography: Applicable Cryptography for Cyberspace Security.* Cham: Springer.

ELECTRONIC RESOURCES

http-1: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en (retrieved on 15.06.2019)

http-2: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html (retrieved on 21.06.2019)

http-3: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (retrieved on 15.06.2019)

http-4: https://www.kaspersky.com/about/press-releases/2010_stuxnet-worm-insight-from-kaspersky-lab (retrieved on 05.07.2019)

http-5: https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/ (retrieved on 08.07.2019)

http-6: https://support.microsoft.com/en-us/help/14238/windows-10-troubleshoot-blue-screen-errors (retrieved on 08.07.2019)

http-7: http://anti-virus.by/en/tempo.shtml (retrieved on 08.07.2019)

http-8: https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/what-is-a-driver- (retrieved on 05.07.2019)

http-9: https://www.nrc.gov/materials/fuel-cycle-fac/ur-enrichment.html (retrieved on 05.07.2019)

http-10: https://www.ibm.com/support/knowledgecenter/en/ssw_aix_71/com.ibm.aix.progcomc/ch8_rpc.htm (retrieved on 09.07.2019)

http-11: https://www.merriam-webster.com/dictionary/cyber (retrieved on 15.06.2019)

http-12: https://vuldb.com/?exploits.201905 (retrieved on 08.07.2019)

http-13: https://ccdcoe.org/about-us/ (retrieved on 09.07.2019)

http-14: https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2008&locations=EE-EU&name_desc=false&start=2004&view=chart (retrieved on 10.07.2019)

http-15: https://www.lexico.com/en/definition/hack (retrieved on 10.07.2019)

http-16: https://usbkill.com/products/usb-killer-v3 (retrieved on 11.07.2019)

http-17: https://www.shodan.io/search?query=%22default+password%22 (retrieved on 11.07.2019)

http-18: https://www.shodan.io/report/ZjDeRDNM (retrieved on 12.07.2019)

http-19: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping (retrieved on 12.07.2019)
http-20: https://www.lexico.com/en/definition/weapon (retrieved on 12.07.2019)
http-21: https://www.un.org/en/sections/un-charter/chapter-vii/index.html (retrieved on 12.07.2019)
http-22: https://niccs.us-cert.gov/about-niccs/glossary#cybersecurity (retrieved on 12.07.2019)
http-23: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf (retrieved on 12.07.2019)
http-24: https://www.wandera.com/mobile-security/man-in-the-middle/man-in-the-middle-attack/ (retrieved on 12.07.2019)
http-25: https://www.cmedia.com.tw/about/locations (retrieved on 13.07.2019)
http-26: https://www.symantec.com/security-center/writeup/2000-122016-0558-99 (retrieved on 13.07.2019)
http-27: https://docstore.mik.ua/orelly/networking_2ndEd/tcp/ch02_04.htm (retrieved on 13.07.2019)
http-28: https://cyberraiden.wordpress.com/2015/04/19/sysinternals-process-explorer/ (retrieved on 13.07.2019)
http-29: https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/ (retrieved on 14.07.2019)
http-30: http://europa.eu/rapid/press-release_IP-17-3193_en.htm (retrieved on 14.07.2019)
http-31: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en (retrieved on 14.07.2019)
http-32: http://www.mooreslaw.org/ (retrieved on 14.07.2019)
http-33: https://opensource.com/resources/what-open-source (retrieved on 23.07.2019)
http-34: https://docs.microsoft.com/en-us/security-updates/securityadvisories/2010/2286198 (retrieved on 23.07.2019)
http-35: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046 (retrieved on 23.07.2019)
http-36: http://www.linfo.org/compiler.html (retrieved on 23.07.2019)