THE UNITED STATES CYBER WARFARE STRATEGY TOWARD IRAN: OPERATION OLYMPIC GAMES AND CYBER WARFARE AS THE NEW INTERNATIONAL SECURITY THREAT (2010-2016)

By

Hinayah Nur M. Asri

016201300066

A thesis presented to

Faculty of Humanities,

President University

In partial fulfillment of the requirements for

Bachelor's Degree in International Relations

Concentration of Strategic and Defense Studies

2017

THESIS ADVISOR RECOMMENDATION LETTER

This thesis entitled **"THE UNITED STATES CYBER WARFARE STRATEGY TOWARD IRAN: OPERATION OLYMPIC GAMES AND CYBER WARFARE AS THE NEW INTERNATIONAL SECURITY THREAT (2010-2016)"** prepared and submitted by **Hinayah Nur M. Asri** in partial fulfillment of the requirements for the degree of Bachelor Degree in the Faculty of Humanities has been reviewed and found to have satisfied the requirements for a thesis fit to be examined. I therefore recommend this thesis for Oral Defense.

Cikarang, Indonesia, May 26th, 2017

Prof. Anak Agung Banyu Perwita, Ph.D.

DECLARATION OF ORIGINALITY

I declare that this thesis, entitled **"THE UNITED STATES CYBER WARFARE STRATEGY TOWARD IRAN: OPERATION OLYMPIC GAMES AND CYBER WARFARE AS THE NEW INTERNATIONAL SECURITY THREAT (2010-2016)"** is, to the best of my knowledge and belief, an original piece of work that has not been submitted, either in whole or in part, to another university to obtain a degree.

Cikarang, Indonesia, May 26th, 2017.

Hinayah Nur M. Asri

PANEL OF EXAMINERS APPROVAL SHEET

The Panel of examiners stated that the thesis entitled **"THE UNITED STATES CYBER WARFARE STRATEGY TOWARD IRAN: OPERATION OLYMPIC GAMES AND CYBER WARFARE AS THE NEW INTERNATIONAL SECURITY THREAT (2010-2016)"** that was submitted by Hinayah Nur M. Asri majoring in International Relations from the Faculty of Humanities was assessed and approved to have passed the oral examinations on May 30th, 2017.

Prof. Anak Agung Banyu Perwita, Ph.D.

Chair of Panel of Examiner – Thesis Advisor

Hendra Manurung, S. IP, M.A.

Examiner

Bustanul Arifin, BA.IR, M.A.

Examiner

ABSTRACT

The nuclear program of Iran has become the utmost concern of the U.S since decades ago. The security dilemma it has brought, have heightened the tension between the two countries' relations. Several negotiation attempts have been made under the intergovernmental forum for nuclear field International Atomic Energy Agency (IAEA), yet it floundered several times as Iran had not complied with the agreements. An alternative option imposed by the international community, including the U.S., was to impose economic sanctions and embargo Iranian oil. Even so, Iran did not put a halt on its nuclear development program. This resulted in the U.S using other measures to hinder the Iranian nuclear program, which is through the implementation of its cyber warfare strategy.

This thesis attempts to comprehend the United States cyber warfare strategy towards Iran through the Operation Olympic Games. It will begin by shining the light on how cyber threats have become an emerging issue in the 21st century, examining the importance of politically-motivated cyber attacks that targeted critical infrastructures of governments as an alarming threat to national security. Followed is the exploration the United States cyber warfare strategy, including the Presidential Policy Directives (PPD) and other documents that supported the U.S cyber warfare doctrines. Lastly, this research will elaborate the detailed case study of the Operation Olympic Games as the implementation of the U.S cyber warfare strategy, providing the timeline of the operation and details of the Stuxnet, Duqu, and Flame malwares that attacked Iran's nuclear facilities.

Keywords: Cyber Warfare, Critical Infrastructure, Operation Olympic Games.

ABSTRAK

Program nuklir Iran telah menjadi kekhawatiran utama bagi Amerika Serikat sejak puluhan tahun yang lalu. Dilema keamanan tersebut telah meningkatkan ketegangan antara hubungan kedua Negara. Berbagai upaya negosiasi telah dilakukan dibawah forum antar pemerintang di bidang nuklir seperti Badan Energi Atom Internasional (IAEA), namun beberapa kali telah gagal karena Iran tidak mematuhi kesepakatan tersebut. Pilihan alternatif yang diberlakukan oleh masyarakat internasional termasuk A.S., adalah untuk menjatuhkan sanksi ekonomi dan embargo minyak Iran. Namun demikian, Iran tidak menghentikan program pengembangan nuklirnya. Alhasil, A.S menggunakan langkah-langkah lain untuk menghambat program nuklir Iran, yaitu melalui penerapan strategy perang maya.

Penelitian ini mencoba untuk memahami strategi perang maya Amerika Serikat terhadap Iran melalui Operasi Olympic Games. Penelitian ini dimulai dengan menyoroti bagaimana ancaman cyber telah menjadi isu yang muncul di abad ke-21, memeriksa pentingnya serangan maya bermotif politik yang menargetkan infrastruktur penting pemerintah sebagai ancaman bagi keamanan nasional. Diikuti dengan mengeksplorisasi strategi perang maya A.S, termasuk Petunjuk Kebijakan Kepresidenan (PPD) dan dokumen dokumen lain yang mendukung doktrin perang maya A.S. Terakhir, penelitian ini akan menguraikan studi kasus secara rinci dari operasi Olymcic Games tersebut, termasuk kurun waktu mengenai terlaksanakya operasi Olympic Games dan menjelaskan secara rinci tentang Stuxnet, Duqu, dan Flame, *malwares* yang menyerang fasilitas nuklir Iran.

Kata Kunci: Perang Maya, Infrastruktur Penting, Operasi Olympic Games.

ACKNOWLEDGEMENT

First and foremost, I would like to present my highest gratitude to Allah SWT. Were it not for His blessing, guidance, support, and power, I would not have the motivation and strength to finish my thesis. Secondly, I would like to thank God for blessing me with the best gifts I could ever receive, my dad—Mr. Muhammad Asri, my mom—Mrs. Evidayanti, my brothers—Maula Rizky and Sultan Abdurrahman, and the last but not least, my one and only sister—Nasywa Meutia. Their endless support and prayers are what gets me through the hardest times of my life, each with their own ways of showing me they care, and always supporting my decisions in whatever I make. Thirdly, to my relatives, aunts, uncles, and grandparents, thank you for always including me in your prayers.

Throughout my thesis writing and university life, I would also like to deliver my gratitude to these very helpful people:

1. The best thesis advisor and lecturer anyone could ever ask for, Prof. Anak Agung Banyu Perwita, Ph.D. Thank you for your time, consultations, constructive feedbacks, and advice. Your lectures have always been thought-provoking and broadened my knowledge in International Relations.
2. The Head of Study Program, Mr. Hendra Manurung, and the Dean of the Faculty of Humanities, Teuku Rezasyah, Ph.D.
3. My childhood friends, the only two people who knows everything about me, Tia Julyta and N.Z Nanda.
4. My most humble and down-to-earth best friend since birth, Yun Rizkika, for always reminding me to stay spiritual and never forget what life is about.
5. The people who started out as friends but now have become family to me, my truest support system during this university life, my non biological sisters, Fatimah Zuhra, Qatrunnada F. Arista, Inggita Shanty, Winie

Kosasih, and Cynthia Ongga. They are the people who can make my darkest days turn bright.

6. Siti Raudina, thank you for always listening to my rants, day and night. Thank you for motivating me and being there for me even in my lowest moments when I didn't even feel like getting out of bed on my 8th and 9th semester. Thank you for putting up with me.
7. My right-hand men, Reza Putra, Rizky A. Putra, Teuku Haikal Putra, and Muttaqin Amri. Each of them having their own unique personalities, which is why I am thankful to have them in my life, for always looking out for me and being the replacement brothers that I needed.
8. My wildest friend, Mentary R.R, we argue a lot and have a love/hate relationship with each other, but we always make up in the end. Through ups and downs, the friend who taught me more about hard work and determination.
9. Naomi Kifta, Dewi Adnyani, Elena Minarni, and Sarah Philipp, my very few first friends when I arrived in university. My partners in crime. We have experienced so many things together and been to so many weird/shady places together.
10. Anggi DNA, Elsa Faradila, Onasis Tarigan, and Fenni Adella, thank you for being helpful and kind in your own ways.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

LIST OF ACRONYMS

DDoS	Distrbution Denial of Service
DoS	Denial Of Service
NATO	North Atlantic Treaty Organization
CrySyS	Cryptography and System Security
CERT	Community Emergency Response Team
PPD	Presidential Policy Directive
OCEO	Offensive Cyber Effect Operation
WMD	Weapons of Mass Destruction
DoD	Department of Defense
ICS	Industrial Control System
NIST	National Institute of Standards and Technology
ICT	Information and Communication Technology
GAO	Government Accountability Office
IoT	Internet of Things
SCADA	Supervisory Control and Data Acquisition
UPS	Uninterruptible Power Supply
NSPD	National Security Presidential Directive
NSA	National Security Agency
IO	Information Operations
EW	Electronic Warfare
CNO	Computer Network Operations

PSYOP	Psychological Operations
MILDEC	Military Deception
OPSEC	Operation Security
IRC	Information-Related Capabilities
IE	Information Environment
MISO	Military Information Support Operation
USSTRATCOM	US Strategic Command
CNA	Computer Network Attacks
CNE	Computer Network Exploitation
CND	Computer Network Defense
JP	Joint Publication
JFC	Joint Force Commanders
TAO	Tailored Access Operations
IAEA	International Atomic Energy Agency
CoveOps	Covert Operations
PLC	Programmable Logic Control

CHAPTER I:

INTRODUCTION

1.1 Background of Study

The internet has revolutionized the way we conduct things in our society. It has become an essential part of our society; the internet has paved its way into making lives more convenient, in all aspects. This is also true for states that heavily rely on the internet for their civilian and military infrastructure, such as coordinates and the use of drones. This internet dependency has now posed a threat for many states that now view the cyberspace as part of their strategic interest.[1]

According to Sarah Gordon and Richard Ford from Symantec[2], Interactions between human motives and information technology for terrorist activities in cyberspace or in the virtual world can be addressed as cyber terrorism, or as they define it "pure cyber terrorism". Cyber warfare poses a significant threat in the 21st century. This is especially true for states and nation-states. Today, it has replaced conventional means of war and has become an issue that has no boundary, as the cyberspace practically touches everything. The globally interconnected world where digital information as well as communications infrastructure known as "cyberspace" has affected many countries to reassess their current foreign policies regarding cyber security.

Another definition of cyber warfare is symmetric or asymmetric offensive or defensive digital network activity by states or state-like actors, encompassing

[1] The Department of Defense Cyber Strategy, April 2005, Retrieved on March 29 2017 from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[2] Gordon, Sarah; Ford, Richard. "Cyberterrorism?" Retrieved from http://www.symantec.com/avcenter/reference/cyberterrorism.pdf on March 29 2017

danger to critical national infrastructure and military systems. It requires a high degree of interdependence between digital networks and infrastructure on the part of the defender, and technological advances on the part of the attacker. It can be understood as a future threat rather than a present one, and it fits directly into the paradigm of Information Warfare. [3] Cyberwar is also understood as the act of disruption to sabotage with motivation of hacking adversaries' computer networks. The motives are mostly based on political background, seen as the bloodless non-kinetic warfare yet cause similar destruction to critical infrastructure.[4]

The term cyber terrorism itself has various definitions; this term can be defined as the use of information technology by terrorist groups or individuals to achieve their goals. This includes attacks against networks, computer systems and telecommunications infrastructure, as well as to exchange information and perform electronic threat. These type of threats can manifest in many ways, including: hacking computer systems, programming viruses, web page attacks, Denial or service (DoS) attacks, or conducting terrorist attacks through electronic communications.

Recently, cyber attacks are emerging as they are increasingly attractive to those that have limited funds and require a smaller number of people. Anonymity is also another advantage of cyber attacks, as terrorists or any of the actors remain unknown, as they could be very far away from where the act is committed. Unlike terrorists that have camps in countries with weak governance, cyber terrorists can reside anywhere and remain anonymous[5]. It is also believed that the most effective use of cyber terrorism is when it is combined with physical terrorism. For example, disabling the operation of emergency services in

[3] Shane M. Coughlan, "Is There a Common Understanding of What Constitutes CyberWarfare?" The University of Birmingham School of Politics and International Studies, 30 September 2003, p.2
[4] Sanger, David E. (1 June 2012). "Obama Order Sped Up Wave of Cyberattacks against Iran". The New York Times, Retrieved March 29, 2017.
[5] M., Cereijo. May 16, 2006 "Cuba The Threat II: Cyberterrorism and Cyberwar" Retrieved March 29,2017

situations where the need for deployment of such services when it was needed. It could also tamper with government computer networks, financial networks, and power plants and the like.

Cyber warfare is now a form of modern warfare. It has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[6] Despite the fact that the cyberspace lacks institution, hierarchy, and ordering principle, as Kenneth Waltz mentioned in the definition of international politics: "with no system of law enforceable," cyberspace can become a cyber power through "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power," as formulated in 2009 by Daniel T. Kuehl. Cyberspace has provided a battlefield for cyber warfare.[7]

The first major cyber warfare event that caught the world's attention was the 2007 DDoS attacks on the Estonian government that aimed to disable the Estonian governmental organizations including Estonian parliament, banks, ministries, newspapers, and broadcasters.[8] This rendered the country disconnected to the rest of the world, despite Estonia being considered to be the most wired country in 2007. This was due to the relocation of the Bronze Soldier of Tallinn, viewed differently by ethnic Estonians and ethnic Russian immigrants in the area for having different symbols. Following this event, tensions rose among Russia and NATO and the European Commission, for many speculate that the attacks couldn't have been done without the support of Russia, as it served within their interests[9]. Since then, Estonia has become one of the leading nations in the area of Cyber Strategy and Cooperative Cyber Defence Center.

[6] Clarke, Richard A. & Knake, Robert K. "Cyber War: The Next Threat to National Security and What to do About it." Harper Collins, New York, 2010, p.6. Retrieved on March 29, 2017
[7] Kuehl, Daniel T.2009 "From Cyber Space to Cyber Power: Defining the Problem." Retrieved on March 29 , 2017.
[8] Davis, Joshua. August 21, 2007. " Hackers Take Down the Most Wired Country in Europe", Wired. Retrieved March 29, 2017.
[9] "Estonia Fines Man for CyberWar". BBC. 25 January, 2008. Retrieved March 29, 2017

Another similar attack also took place in Georgia, during the Russo-Georgian War, in which Russia targeted many of the government websites as well as banks; this cyber war in fact coincided at the same as the shooting war that was taking place in the country. In fact, even after the two countries had reached a ceasefire, many Georgian servers were still down, which hindered the communication in Georgia.

In 2010, the United States joined forces with Israel to conduct a covert operation targeting the Iranian Nuclear facilities using a worm called Stuxnet; also known as Operation Olympic Games[10]. Stuxnet is considered to be the first-known worm designed to target real-world infrastructure such as power stations, water plants, and industrial units. [11] Having been detected in June 2010 by Symantec, Stuxnet was unlike any other virus or worm that came before it. Instead of simply hijacking targeted computers and stealing confidential information, it escaped the digital realm to wreak physical destruction on equipment the computers controlled.[12] Once the machine has been infected, it seeks out the specific configuration of the control software. With this malware, the U.S targeted give Iranian organizations with uranium enrichment infrastructure as their main functional purpose. The five organizations were targeted repeatedly between June 2009 and April 2010.[13]

Initiated by former President Bush in 2006, the program was then expanded by President Obama, urged by the former president to continue the Olympic Games Operation. This Operation managed to cause roughly 1000 centrifuges, 1/5 of Iran's centrifuges to crash, in an effort to slow Iran's nuclear efforts. By 2012, intelligence agencies in the US and Israel seek out to further

[10] Sanger, David E. (1 June 2012). "Obama Order Sped Up Wave of Cyberattacks against Iran". The New York Times, Retrieved March 29, 2017.
[11] Fildes, Jonathan. "Stuxnet Virus Targets and Spread Revealed." BBC News. Retrieved March 29 2017.
[12] Zetter, Kim. March 11, 2014, " An Unprecedented Look at Stuxnet, The World's First Digital Weapon". Retrieved March 29, 2017
[13] Fildes, Jonathan. "Stuxnet Virus Targets and Spread Revealed." BBC News. Retrieved March 29 2017.

upgrade malicious programs that further slow Iran's progress, such as the Duqu malware and Flame.

In the following 2011, the Duqu malware is also thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University of Technology produced a sixty-page report stating that the worm is a Stuxnet-like malware.[14] Instead of destroying like the previous worm, Duqu is considered as a Trojan, collecting information that could be useful in attacking the industrial control system.[15] The purpose of Duqu was to modify computer protections with the help of an infected Microsoft Word document. Duqu used the Zero-Day exploit method in which on the day when the attack occurs, there was zero awareness of the attack happening. The infection of Duqu was reported to be found in countries including France, Netherlands, Switzerland, Ukraine, India, Indonesia, Iran, Sudan, and Vietnam.

What followed Stuxnet and Duqu by 2012 was Flame, a more upgraded form of the malware. This was the newest form of malware that infiltrated several networks in Iran and across the Middle East that was discovered in early 2012.[16] This malware was discovered by MAHER Center of Iranian National Computer Emergency Response Team (CERT)[17], Kaspersky Lab, and CrySyS Lab.[18] Experts that reported the malware also mentioned that this was the most complex and sophisticated malware they have ever encountered. Flame is also believed as part of the covert act code-named Operation Olympic Games.

[14] "Duqu: A Stuxnet-like Malware Found in the Wild, Technical Report".laboratory of Cryptography of Systems Security (CrySyS). Retrieved March 29 2017
[15] 'W32.Duqu – The Precursor to the Next Stuxnet (Version 1.4)". Symantec. Retrieved on March 29 2017.
[16] McElroy, Damien; Williams, Christopher (28 May 2012). Flame: World's Most Complex Computer Virus Exposed". The Daily Telegraph. Retrieved March 29 2017.
[17] "Identification of a New Targeted Cyber-Attack." Iran Computer Emergency Response Team. 28 May 2012. Retrieved March 29 2017.
[18] (28 May 2012)"SkyWiper: A Complex Malware for Targeted Attacks". Budapest University of Technology and Economics. Retrieved on March 29 2017.

1.2 Problem Identification

Cyber attacks conducted upon a country has a political agenda, in which Operation Olympic Games, was responsible for doing a covert campaign through cyber disruption of other nation-state's classified information. In other words, an political espionage. Cyber attacks can have different interpretations based on the organizations conducting it, and by its target of attacks. Cyber attacks conducted by non nation-states are usually used to steal banking information from the internet, or to send a political message. However, if a cyber attack is conducted by a nation-state towards another nation-state, it's usually in line to protect its national interests and security, causing greater damage compared to the attacks conducted by non nation states or private organizations as countries has greater resources. Besides being in the national interest of the US to slow down the development of nuclear power plants in Iran, this program initiated by George W. Bush was believed to be the only way to stop or prevent Israel from conventionally attacking Iran's nuclear facilities.[19]

The United States and Israel's involvement in the Operation Olympic Games targeting uranium enrichment centrifuges has been the subject of controversy. On June 2013, the Whistleblower Edward Snowden leaked to The Guardian the Presidential Policy Directive 20 (PPD-20)[20] which superseded the NSPD-38, which provides the framework for U.S cyber security by establishing principles and processes. The eighteen-page presidential memo revealed to the world how Barack Obama ordered intelligence officials to draw up a list of potential overseas targets for U.S cyber attacks and gives the U.S government power to conduct surveillance through monitoring.

[19] Sanger, David E. (1 June 2012). "Obama Order Sped Up Wave of Cyberattacks against Iran". The New York Times, Retrieved March 29, 2017.
[20] Presidential Policy Directive/PPD-20. Retrieved on March 29, 2017 from https://fas.org/irp/offdocs/ppd/ppd-20.pdf

In addition to that, the policy also published U.S policy on Offensive Cyber Effects Operations (OCEO)[21] which is:

"OCEO can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."[22]

Obama has authorized the "anticipatory actions taken against imminent threats"[23]. It reserves the right to use offensive cyber-attack in foreign nations without government permission as long as it is in line with "U.S national interest and equities"[24]. Many evidences of cyber attacks conducted by the state and non-state actors have significantly increased for the past ten years. The leaked Presidential Policy Directive is relevant to the Operation Olympic Games where the Offensive Cyber Effects Operations was implemented.

The purpose of this thesis is intended to address and further examine the implementation of the U.S cyber warfare strategy from the year 2010 to 2016, specifically the Operation Olympic Games, and to elaborate more on how cyber warfare has become a new threat to national and international security. As evidence suggests, it has already been used several times by nation-states.

1.3 Statement of the Problem

Research Question: How did the United States implement its Cyber Warfare Strategy towards Iran through Operation Olympic Games (2010-2016)?

[21] Greenwald, Green and MacAskill, Ewen, " (7 June 2013) "Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks, The Guardian, Retrieved on March 29, 2017.
[22] Presidential Policy Directive/PPD-20. Retrieved on March 29, 2017 from https://fas.org/irp/offdocs/ppd/ppd-20.pdf
[23] Ibid. P.3
[24] Ibid. P.7

1.4 Research Objectives

Based on C. R. Kothari's book of Research Methodology (2004)[25], this thesis will use the method of **analytical-descriptive** research to analyze the variables that construct the title as well as the discussions on this topic. This research will also use empirical research on primary resources from mass media release, governmental websites, government-official data obtained from reports, as well as several studies from various authors to support the theoretical framework of this thesis.

The researcher believes that the objectives of this research is to penetrate and explore the depths of cyber warfare strategies of the U.S as its means to pursue national objectives, in this case, towards Iran. In addition to this, this research will also reveal the mechanism of attacks as well as the motives behind the cyber attacks conducted by the U.S on Iran.

1.5 Significance of Study

Social science research often use the term *Ex Post Facto Research* for descriptive research, where the researchers have no control over the variables and can only report what has happened or what is happening. The researcher is convinced that the significance of this study will contribute greatly for further research in the International Relations studies.

The significance of this study may well become:

- A source for further understanding the 21st century phenomenon of cyber warfare
- To gain an in-depth understanding of the implementation of the U.S cyber attack strategy as political means to achieve national objective.

[25] Kothari, C.R (2004) Research Methodology: Method and Techniques (Second Revised Edition) New Delhi: New Age International Ltd.

- To encourage a more elaborative research regarding cyber crimes conducted by nation-states towards other countries.

1.6 Theoretical Framework

1.6.1 Cyber Warfare and Neo-Realism

Cyber war is a new phenomenon in the 21st century which has not been fully revealed yet. As Richard A. Clarke and Robert K. Knake defines cyber war: "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or destruction."[26] Many events have been considered to be the starting point of cyber warfare between states that have the technological capacity to carry it out. In this thesis, the researcher will examine the issue of cyber war and how it can be understood through the neo-realist security theory and how Cyber war has presented a number of challenges to the international order.

Through the classic realism theory, the international system is just viewed as an anarchic system, as there are no supreme authority that has control over the states; which means that all states compete over power and security in zero-sum game with one state's gain as another state's loss. The neorealist theory, like the classic realists, see the world as a dangerous place where states are in constant competition for power, however the key point of neorealist theory lies upon the belief that the distribution of capabilities measured by the number of great powers (ideally a bi-polar structure) within the international system could constrain anarchy and instability within the international system. The principle of survival, or self-help, in this theory is also viewed as an essential for states. Since the international system is anarchic and the state

[26] Clarke, Richard A. and Knake, Robert K. "Cyberwar: The Next Threat to National Security and What to Do About it" Harper Collins, 2010. Retrieved on March 31st 2017

cannot rely on any higher authority for their survival they must achiever it by providing security for themselves; this can either be through military build-up or the creation of alliances to counter another state or alliance power. The neo-realist theory also acknowledges that one state's military build up to increase its security can be viewed as a decrease in the security of its neighboring states.

In order to examine the development of cyber warfare as a new global threat, this section of research will discuss Kenneth Waltz theory on Neorealism to elaborate the issue using offensive and defensive realism to understand the concept of cyber war. In terms of nuclear weapons, both offensive and defensive realism have the agreement over its utility for offensive purposes. In relevance to the theory mentioned, the U.S has always been suspicious over Iran's nuclear program, because they believe that such program is developed for offensive purposes. Therefore, the security dilemma here is that the offensive capabilities outweigh the defensive capabilities. Therefore, cooperation and agreements with the international community are harder to achieve.

Similar to the emergence of nuclear weapons, cyber warfare has also provided state with the weapons that have the capacity to challenge states with superior military and financial capabilities, albeit having different destructive powers. As aforementioned, many states have already started reaching towards cyber space as a security interest, so as not to risk falling behind in the development of cyber warfare and become the victim of other states with strong cyber warfare capabilities. Based on the offensive theory, many states would challenge other major states to become hegemonic powers, if the opportunity and probability are high.[27]

According to the thesis submitted by Gabriel Strinde from Lund University in 2011, cyber warfare enables a certain asymmetry in power that could change the way realism view nation-states power and its

[27] Strinde, Gabriel, Lund University, 2011. "Cyberwarfare: Connecting Classical Theory to a New Security Domain." Retrieved on March 29, 2017

interaction. In terms of cyber space, the technological sophistication that a nation-state possesses is regarded as a power that plays a major role in which the correlation between its offensive capabilities, defensive capabilities and dependence on cyberspace are relied upon. The impact of cyber warfare on defense realism is basically centered on the same ability as the offensive one, as their capabilities are both parallel to each other. Strinde also mentioned that with the logic of indistinguishable weapons within cyber space, it provides unbalanced and unequal perceivable threat for a state to respond to.

1.6.2 The U.S Defense Policy and Cyber Defense in the Military

The U.S defense policy is aimed at global security and prosperity, and to counter the impending threats posed by other regional state actors towards the U.S national interest. Based on the Defense Policy during the Obama administration in 2012, titled, "Sustaining Global Leadership: Priorities for the 21st Century Defense", U.S economic and security interests are centered in the developments starting from the Western Pacific and East Asia into the Indian Ocean region until South Asia, which is basically half of the globe.

Starting from the Bush until the Obama administration, many of the U.S foreign and defense policies were towards the Gulf and Middle East region. The U.S defense efforts focused more on countering violent extremists', regime changes, as well as the proliferation of weapons of mass destruction (WMD). The U.S also emphasized the prevention of Iran's development of nuclear capabilities and to counter its destabilizing policies. In line with the Olympic Games Operation, in order to do so, to protect U.S national interest and achieve its objective, the U.S has combined its arms campaign across all domains – land, air, maritime, space, and cyberspace.

The U.S defense policy recognizes it has to include electronic and cyber warfare in order to deter and defeat any aggression by potential adversaries with any asymmetric capabilities. It is also stated that modern armed forces cannot effectively conduct its operations without the use of information and communication network access to the cyberspace, as quoted below :

"Accordingly, Department of Defense (DoD) will continue to work with domestic and international allies and partners and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace and space. "[28]

Based on the Department of Defense Cyber Space Policy Report, it is also stated that to have an effective deterrence in the cyber space, the U.S has the capability to respond to hostile acts with a proportional and justified response.[29] The International Strategy for Cyberspace also provided a clear statement that the United States have the right use means such as diplomatic, informational, military, and economic, in order to defend U.S, its allies, and partners, as well as their interest in cyberspace. This also includes the capability to conduct offensive cyber operations to do so.

1.6.3 Cyber Attack on Critical Infrastructure

Another concept that will be used to address this issue is to understand how cyber attacks on critical infrastructure (CI) can be done. The deployment of the Stuxnet worm provides an outline for how targeted cyber attacks that could destroy the computer programming of a highly secured government facility could be accomplished. The Department of Homeland Security defined CI as "the backbone of our

[28] Obama, Barack, January 2012, "Sustaining U.S Global Leadership:Priorities for the 21st Century Defense" Retrieved on April 19, 2017

[29] Department of Defense Cyberspace Policy Report, November 2011, Retrieved on April 19, 2017

nation's economy, security, and health." Since everything is interconnected to the network nowadays, it is almost taken for granted just how critical infrastructures are used in people's daily lives, including the use of electricity, mass transportation, cell phone communications, as well as its use in industry machineries. Many industries now are computer-reliant, and use industrial control systems (ICS) to measure and control many industrial and mechanical processes.

The National Institute of Standards and Technology (NIST) defined ICS as "combinations of control components that act together to achieve an industrial objective."[30] ICS is used to facilitate the management and regulation of the generation, transmission, and distribution of electricity.[31] It is accomplished by "opening and closing circuit breakers and setting thresholds for preventive shutdowns."[32] The electric and gas industry controls refinery operations by using integrated ICS to, "remotely monitor the pressure and the flow of gas pipelines, and control the flow and pathways of gas transmissions."[33] Due to this, the integration of ICS to the internet is more susceptible to attacks as the control systems weren't necessarily built to withstand advanced cyber threats, and therefore vulnerable to cyber attacks initiated through both wireless signals and the internet.[34] In addition to this, the NIST also highlighted the fact that "unauthorized changes to instructions, commands, or alarm thresholds. This could damage, disable, or shut down equipment, create environmental impacts and endanger human life." This is relevant to the case of the Stuxnet malware implanted into Iran's Natanz Nuclear facility. The stuxnet attack was unprecedented as

[30] Keith Stouffer, National Institute of Standards and Technology, 2014 "Guide to Industrial Control Systems Security."Retrieved on April 20, 2017 from http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
[31] Boaru, G. and Badita, G., Romanian National Defense University, 2008. "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems."p.148 Retrieved on April 20, 2017
[32] Ibid.
[33] Ibid. p.149
[34] Dana A. Shea "Critical Infrastructure: Control Systems and the Terrorist Threat" Congressional Research Service, 2004. P.3 Retrieved on April 20, 2017.

it was the first use of a cyber weapon to destroy the critical infrastructure of another country through the use of computer programming. This kind of action used to only be possible through bombing or traditional sabotage. It provides a blueprint on how to conduct a specifically target cyber attack on the computer systems on a highly secured government-controlled CI.[35]

1.7 Scope and Limitation of the Study

The issue addressed in this thesis is still not primarily talked about. Therefore, the scope and limitations of this study includes:

- This thesis will mainly focus on the strategy implemented by the US in conducting cyber-attacks towards Iran that targeted its nuclear facilities initiated in 2006, conducted throughout 2010-2016 under the Operation Olympic Games. It will also elaborate from the historical perspective of both countries, which is considered a driving force for the attacks.
- The researcher will also address current global issues in the cyber world and its development in recognizing cyber-terrorism as a new security threat as well as the actions that organization or institutions have taken to resolve the issue.

1.8 Definition of Terms

Most commonly mentioned definitions of terms used in this thesis are as noted below:

a. *Cyber warfare:* Cyber warfare refers to politically motivated hacking to conduct sabotage and espionage. It is considered as form of information

[35] Nakashima, Ellen, Washington Post, 2010, "Stuxnet Malware is Blueprint for Computer Attacks on U.S" Retrieved on April 20, 2017.

warfare between persons and/or nation-states. Cyber warfare refers to the information-related conflict at a grand level between nations, private organizations, or societies. This represents a new entry on the spectrum of conflict that spans economic, political, social, as well as a military form of "war". Cyber warfare could be identified by their targeting of classified information and communications. Motives behind Cyber warfare are varied, from military to political reasons.

b. *Cyber-attacks:* Referring to the Australian Cyber Security Center (ACSC) Threat Report 2015, a Cyber attack is a deliberate act through cyber space to manipulate, destruct, deny, degrade, or destroy computers or networks, or the information residing in them, with the effect, in cyber space or the physical world, of seriously comprising national security, stability, or prosperity. Cyber attacks can be launched from outside the network, using hackers, or from the inside using agents and rogue components. Cyber-attacks are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities.

c. *Operation Olympic Games:* Operation Olympic Games is an unacknowledged campaign of sabotage by means of cyber disruption targeting on Iran's nuclear facilities designed by the US and Israel. It was first initiated in 2006, under the Bush administration. The strategy was believed by Bush to be the only way to hinder Israel from launching conventional strikes on Iran.

1.9 Structure of Thesis

The research paper consists of five chapters and the structure is as follows:

Chapter I: Introduction

Beginning with a background of the study to give a closer exposure on the chosen topic, followed by the identification of the problem which elaborates

briefly on the problematic issues that the researcher is concerned about, why the problems appear and why it's become an object of investigation. Significance of study explains the key areas of study that will contribute in bringing about the benefits to the academic community. This will be followed by theoretical framework, the concept needed to formulate the variables or the relationships, and scope and limitations of study as well as the research methodology used to analyze the research.

Chapter II: Cyber Terrorism as the New Global Threat

This chapter gives a brief analysis on the current issues on cyber threats and attacks. It will also shine the light on how cyber security is an emerging issue of the 21st century. The chapter will also focus on the global trends of cyber warfare including the countries that were attacked. The definitions and implications of cyber threats and attacks on state's security will also be elaborated in this chapter.

2.1 Defining Global Cyber Threats

2.2 Current Trends on Cyber Warfare

2.3 Major Cyber Attacks in History

2.3.1 Estonia 2007

2.3.2 Georgia 2008

2.3.3 Burma 2010

2.3.4 Ukraine 2015

Chapter III: The United States Cyber Warfare Strategy

This chapter will explore the depths of the United States Cyber Warfare strategy in defending its nation's national interest. This section of the thesis will also mention the United State's cyber security activities and actions taken as well

as how the government works with certain agencies, and allies to conduct its cyber warfare strategy.

3.1 The United States Offensive Cyber Effects Operations (OCEO)

3.2 The United States Cyber Warfare Doctrine

3.2.1 DoD Directive No.3600.1 Information Operations

3.2.2 DoD Information Operations Roadmap

3.2.3 Joint Publication (JP) 3-13 Information Operations

3.3 The United States Cyber Warfare Method

3.3.1 Computer Network Exploitation (CNE)

3.3.2 Computer Network Attack (CNA)

3.4 The United States Cyber Warfare Results

Chapter IV: The Implementation of the U.S Cyber Warfare Strategy: Operation Olympic Games

As the core of every thesis, this chapter will analyze and interpret the chosen topic. The extensive report of the research will be reported systematically into a full analysis of the data gathered using charts, tables, and figures to support the explanation. This chapter will revolve around the strategy being implemented by the U.S in achieving their foreign policy through cyber warfare.

4.1 Historical Background of Operation Olympic Games

4.2 Operation Olympic Games Timeline

4.3Stuxnet

4.4 Duqu

4.5 Flame

4.6 Implications for Government and Private Sectors

4.7 Ethical Implications

Chapter V: Conclusion

The last chapter of every thesis will end with a conclusion, allowing the researcher to evaluate whether the questions have been answered through the process of the research as well as give the information on how far the development of the cyber security in the international level.

CHAPTER II:

CURRENT GLOBAL CYBER THREATS

2.1 Defining Global Cyber "Threats"

Today, developments in the world of information technology and communications (ICT) have reformed the true definition of a country's power and sovereignty. The power and sovereignty of a country is currently not only limited to its strength in the military and economy, but also depends on the country's technological sophistication. This is due to the fact that in this 21st century, also called the age of information, almost all activities conducted, starting from personal until governmental activities cannot be separated from the utilization and implementation of technology.[36]

The rapid development of technology at various parts of the world also impact on the emergence of more sophisticated and advanced threats toward a nation-state's national security and the sovereignty of a country. To face and anticipate such conditions, it is necessary for the enforcers and leaders of state to have comprehensive knowledge in the field of IT. The rapidly intertwined development in the world of international relations and ICT is also known as globalization. In the interaction between nations, globalization takes place in two dimensions: space and time. Space gets narrower and time is shortened significantly in order to communicate across the globe. The existence of technology has eliminated a lot of geographical barriers and changed many mankind life patterns that resulted in a more knowledge-based society.

[36] Saputra, Y. M. *"Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare"* Retrieved on April 20, 2017 from http://download.portalgaruda.org/article.php?article=349381&val=6444&title=PENGARUH%20CYBER%20SECURITY%20STRATEGY%20AMERIKA%20SERIKAT%20MENGHADAPI%20ANCAMAN%20CYBER%20WARFARE

On the contrary, the use of technology for negative/destructive purposes also cannot be prevented, be it by individuals, non-state actors, or state actors, each with aims of exploiting information in order to exert their influence in the information warfare or cyber warfare. In the current cyber era, the use of technology for destructive purposes can become a threat towards a nation's security. This is why a nation-state must have a capable cyber defense in order to face such threats.

2.2 Current Trends on Cyber Warfare

According to the United States Government Accountability Office (GAO) Report in 2013[37], the evolvement of cyber-based threats that nations face include threats to national security, commerce and intellectual property, and individuals. Sources of adversarial threats to cyber security include:

Table 1 : Sources of Adversarial Threats to Cybersecurity

	Threat Source	**Description**
1.	Bot-net Operators	Bot-network operators use a network of compromised remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. e.g.: purchasing a denial-of-service attack or services
2.	Criminal Groups	Criminal groups seek to attack systems for monetary gain, usually using spam, phishing, and spyware/malware to commit identity thef, online fraud, and computer extortion. This includes industrial espionage, and large-scale monetary theft or to hire or develop hacker talent.
3.	Hackers	Hackers break into networks for the challenge,

[37] GAO, February 2013, "Cyber Security: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." Retrieved on April 20, 2017 from http://www.gao.gov/assets/660/652170.pdf

		revenge, stalking, monetary gain, political activism, and can download attack scripts and protocols form the internet and launch them against their victims. The CIA stated that the majority of hackers do not have the ability to threaten critical U.S networks, yet at a large scale, they pose a relatively high damage.
4.	Insiders	The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
5.	Nations	Nations are working to develop information warfare doctrine, programs, and capabilities as its cyber tools for information-gathering and espionage activities. These capabilities include the disruption of supply, communications, and economic infrastructure that support military power.
6.	Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gains. Phishers may use spam and spyware to accomplish their objectives.
7.	Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations
8.	Spyware/malware authors	Individuals or organizations that produce and distribute spyware and malware. Several destructive viruses and worms have also harmed hard drives and cause physical damage to critical infrastructure (CI).
9.	Terrorists	Terrorist aim to destroy or exploit critical infrastructures in order to threaten national security,

		cause mass casualties, weaken economy, and damage public morales.

The most common types of attacks conducted towards nation-states, based on the researcher's point of view, is through cyber espionage, either by Distributed Denial of Service (DDoS) attacks or through malwares. Cyber espionage is the practice of obtaining nation-state or institutions 'classified information, specifically targeting them for malicious purposes. DDoS attacks are mainly used to disrupt the nation-state's communication systems and power grids altogether. This tool of cyber attack is usually used to make online services of a nation-state unavailable by overflowing it with traffic that has different requests from multiple sources, which causes the services to crash[38]. This type of attack mainly target banks, news websites, and government services, in order to prevent people from publishing and accessing important information. Malwares, short for 'malicious software', are software programs are popular tools for disrupting normal computer operations. Malwares include viruses, worms, Trojan horses, as well as spywares[39].

2.3 Major Cyber Attacks in History

As more of our infrastructure is becoming computerized via the "Internet of Things (IoT)", our dependency on the internet has gone from our mobile gadgets to daily household objects like refrigerators, vehicles, and other machineries. According to The Guardian, IoT refers to the networks of embedded devices, from smart meters to connected automobiles, which communicate with each other in an automated fashion to make lives more

[38] "What is a DDoS Attack?" Retrieved from http://www.digitalattackmap.com/understanding-ddos/ on April 23, 2017
[39] Christensson, P. (2006) "Malware Definition" Retrieved from https://techterms.com/definition/malware on April 23, 2017

efficient.[40] This has all made us susceptible to all sorts of attack on the networks connected. The actors who usually conduct these attacks are called cyber terrorist, with aims of financial gains or simply to cause terror for the general public. Aforementioned above, sources of threat could include individuals with different interests, however, large-scale attacks like Denial or Service (DoS), attacks on vital infrastructures like power plants, air traffic control systems, Supervisory Control and Data Acquisition (SCADA), could only be capably carried out with the support and sponsor of a powerful nation-state.[41]

The term "cyber terrorism" was first coined in the late 1980s by Barry C. Collin from the Institute for Security and Intelligence. The concept, however, began receiving attention from the general public beginning from the year 2000, when the millennium age started. [42] Connected, therefore it is hackable, devices can be found in control systems that run a nation's critical infrastructure, as is such of the cases that have occurred to sovereign states, starting with the most infamous case of the 2007 Estonian attacks, the 2008 Georgian attack, the 2009 attacks in Burma. And the 2015 attacks in Ukraine.

2.3.1 Estonia 2007

In April 2007, Estonia and Russia experienced an increase in tensions due to Estonia's decision to remove the statue of Bronze Soldier of Tallinn, which, for the Estonians, was a symbol of oppression.[43] For Russia, however, it commemorated the Soviet soldiers and the lack of respect for the Red Army that fought in World War II against the Germans, as well as the destruction of cultural heritage. Due to this, protests both in Estonia and Moscow erupted and massive cyber attack campaigns quickly spread.

---

[40] Brewster, T. (20 March 2014) "There are Real and Present Dangers around the Internet of Things." Retrieved from https://www.theguardian.com/technology/2014/mar/20/internet-of-things-security-dangers on April 23 2017.
[41] Curran, Paul, (May 04, 2016) "Cyber Terrorism – How Real is the Threat?" Retrieved from https://www.checkmarx.com/2016/05/04/cyber-terrorism-real-threat-2/ on April 23, 2017.
[42] Bradley, Nicolas "Cyberterrorism is Real—is it? " Retrieved from http://www.lowlandssolutions.com/downloads/talent/Cyberterrorism%20-%20Nicholas%20Bradley.pdf on April 23 2017.
[43] (28 April 2007) "Tallinn Tense After Deadly Riots" BBC NEWS, Retrieved on April 29, 2017.

For three weeks, Estonia experienced a wide-scale attack on its government websites beginning from the Estonia Reform Party's website, which then continued on to other parties' websites, not excluding commercial sites as well. Estonia in 2007 was considered the most wired country[44], having had the whole country covered in WiFi, offering online government services, and 86% of its population did banking online. Hence, when the DDoS attacks started, the country was rendered unconnected to the rest of the world. The attacks successfully targeted government websites, two major banks, political parties, as well as news organizations.[45]

According to the Economist, the cyber attack in Estonia was considered "Web War 1"[46], it showed how new technologies could be used to attack a modern country. Tallinn authorities accused the Kremlin of instigating such acts as most of the protests were from Russian-ancestries that resided in Estonia. This is reasonable, as most of the DDoS attacks were addressed from Russian IP addresses, some of which were from Russian state institutions.[47] In the end, a member of the youth Russian organization, NASI, which was Putin-affiliated, was found guilty of the attacks.

The significance of the Estonian cyber attacks is not in the scope and size of the attacks, however in the precedent that it has made for future cyber conflicts. These attacks showed how the Russian did not need to bring its army into Estonia to inflict damages to Estonia. The attacks also resulted in NATO to

[44] Traynor, Ian, (17 May 2007) "Russia Accused of Unleashing Cyber War to Disable Estonia" , The Guardian, Retrieved on April 29, 2017.
[45] Ibid.
[46] (1 July 2010) "Cyber War: War In the Fifth Domain" The Economist, Retrieved on April 29, 2017. "Estonia, now home to NATO's centre of excellence for cyber-defense was established in response to what has become known as "Web War 1", a concerted denial-of-service attack on Estonian government, media, and bank web servers that was precipitated by the decision to move a soviet-era war memorial in central Tallinn in 2007."
[47] "Russia Accused of Unleashing Cyber War to Disable Estonia" , The Guardian, Retrieved on April 29, 2017

have established a cyber defense center located in Estonia[48], the Cooperative Cyber Defense Center of Excellence.

2.3.2 Georgia 2008

The second major cyber attack on a sovereign nation occurred in Georgia in August 2008. According to experts, this Georgian incident was the first time a cyber attack took place at the same time as a conventional warfare. Russian military was involved in the region, as Georgia and South Ossetia had conflicts due to Georgia's pursuit of the reintegration of South Ossetia and Abhkhazia, both of which are aligned more towards Russia.[49]

Once again, government servers were attacked with an overwhelming number of requests. Many government websites hacked and information changed. Georgian websites were also more vulnerable to cyber attacks as they didn't have the cyber capabilities as Estonia against DDoS attacks. For 5 days, majority of government websites were inaccessible and communications with the outside world through the internet had been cut off. Hackers also changed the Georgian President's website with pictures of Hitler, depicting him as one. The Georgian Foreign Ministry stated that a Russian-led cyber campaign was disrupting many Georgian websites, including the Ministry of Foreign Affairs. However, Russia denied all accusations regarding its involvement in igniting a cyber warfare campaign against Georgia.[50]

The attack on Georgia just shows how information warfare is successful in cutting off Georgian authorities as well as its society from any news. The actors that conducted these attacks aimed for two things; firstly, to reveal the vulnerability of the Georgian President's regime who lost two of its states and

[48] Kozlowski, Andrzej, (February 2004) "Comparative Analysis of Cyberattacks on Estonia, Georgia, and Kyrgyzstan" Retrieved on April 29, 2017 from http://www.eujournal.org/index.php/esj/article/viewFile/2941/2770

[49] Stucke, Kaisa, (June 23, 2015) "Cyber Attacks, Security, and Terrorism: Case Studies" Retrieved on April 29, 2017 from http://www.valuewalk.com/2015/06/cyber-attacks-security-and-terrorism-case-studies/?all=1

[50] Rohan, Brian (August 11 2008) "Georgia Says Russian Hackers Blocked Government Websites", Reuters, Retrieved on April 29, 2017.

was left paralyzed after a Russian military offensive. Secondly, it aimed in intimidating and undermining the faith of Georgian society towards its government so they would stop supporting the regime. Despite these efforts, Georgia reached out to its allies for aid and websites were restored.

2.3.3 Burma 2010

In 2010, Myanmar, also known as Burma had undergone a series of DDoS attacks on the country just before the first general election that Burma had in 20 years. One of BBC's journalists, reported that the cyber attacks has raised suspicion towards Burma's military authorities, stating that this could be one of the ways the government was trying to restrict the flow of information during the election period[51]. It is also known that the Burmese military junta, State Peace and Development Council, was best known for its restrictive and denial of basic human rights and freedom of expression, and in this case, cyberspace and freedom in the internet[52]

In addition to that, many also believe that the 2010 to be a sham, as the last Burmese election on 1990 saw the victory of Aung San Suu Kyi, yet the military Junta (SPDC) still holds the power over the country. According to Dr Craig Labovitz, from Arbor Networks, the DDoS attack in Burma was "significantly larger" than the attacks in 2007 Estonia and 2008 Georgia, respectively.[53]

The attack targeted Burma's main internet provider, the Ministry of Post and Telecommunications, which severed communications with the outside world, raising the suspicion towards Burma's military authorities. Prior to this, Burma had also experienced a series of cyber attacks, including the 2007 Saffron

[51] (November 4 2010) "Burma Hit by Massive Net Attack Ahead of Election", BBC News, Retrieved on April 29, 2017

[52] Villeneuve, N. and Crete-Nishita, M. "Control and Resistance: Attacks on Burmese Opposition Media" Retrieved on April 29, 2017 from http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-08.pdf

[53] Sutherland, JJ (November 4 2010) "Myanmar's Internet Under Cyberattack" Retrieved on April 30 2017 from http://www.npr.org/sections/thetwo-way/2010/11/04/131070830/myanmar-s-internet-under-cyberattack

Revolution, which sparked protests throughout the country by Buddhist monks.[54] Independent news outlets at the time continued to report the situation in Burma to the international community, despite heavy restrictions that were imposed under the regime. As a result, the SPDC completely shut down the internet in Burma for two weeks.[55]

2.3.4 Ukraine 2015

Amidst the ongoing Russian-Ukrainian War, on December 23 2015, Ukraine had a major shutdown to its power grid. This was due to the service outage of three regional electricity companies of Ukraine, Prykarpattyaoblenergo, Chernivtsioblenergo, and Kyivoblenergo. This shutdown was due to the hacking of the systems using remote access to the SCADA[56] of administrative computers inside the company. This was the first confirmed cyber attack on a power grid which was successful. This left the country without electricity for six hours. Even so, control centers of the companies were still not able to operate fully, two months after the attack.

The cyber attack was done in the following steps[57]:

- The Infection of corporate networks using fake emails (Spear-phishing), and the use of BlackEnergy Malware
- Hacking the SCADA, switching off the substations
- Disabling the elements of IT infrastructure: Modems, RTU, switches, Uninterruptible Power Supplies (UPS)

[54] Villeneuve, N. and Crete-Nishita, M. "Control and Resistance: Attacks on Burmese Opposition Media" Retrieved on April 29, 2017
[55] Ibid. P.156
[56] The Supervisory Control and Data Acquisition

[57] (February 12 2017) "The Ministry of Energy and Coal Industry Ukraine: *"Міненерговугілля має намір утворити групу за участю представників усіх енергетичних компаній, що входять до сфери управління Міністерства, для вивчення можливостей щодо запобігання несанкціонованому втручанню в роботу енергомереж"* Retrieved on April 30, 2017 from http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109

- Using the KillDisk Malware to destroy information of servers and workstations
- DDoS attacks on call centers to deny people information.

Following the attacks, Ukraine government officials claimed the power outages a cyber attack, due to this, Ukraine also had the aid of private companies and the U.S to analyze and assist in determining the source of outage. This resulted in the US Security Firm, *iSight*, linking the attacks to a Russian threat group known as 'Sandworm'.[58]

[58] (26 February 2017) "Hackers Behind Ukraine Power Cuts, Says US Report." Retrieved on April 30, 2017, from http://www.bbc.com/news/technology-35667989

CHAPTER III:

THE UNITED STATES CYBER WARFARE STRATEGY

3.1. The Presidential Policy Directive 20

3.1.1 The United States Offensive Cyber Effects Operations (OCEO)

On June 2013, a leaked top-secret President Policy Directive was published on the internet showing an integrated plan of the U.S towards offensive cyber capabilities including a drawn up list for its potential target overseas.[59] The Presidential Policy Directive-20 (PPD-20) was called the Offensive Cyber Effects Operations (OCEO), as it was believed to offer unique and unconventional efforts in order to advance the U.S national adjectives globally. The operations may use very little to no warning at all to the potential adversary with the effects ranging from subtle to severely damaging.[60] The PPD-20 was signed secretly after the failure of the U.S senate pass the cyber security act of 2012 in August.[61] The mentioned document is also a part of the 2013 Mass Surveillance Disclosures, the phenomenon of the reveals on the operational details of the U.S National Security Agency (NSA) by Edward Snowden.[62]

The leaked 18-page documents aimed to provid8e the framework that enabled the U.S government to make decisions on cyber-operations. Said framework was signed by then-president Barack Obama in 2012 that supersedes the National Security Presidential Directive NSPD-38 authorized in July 7,

[59] Greenwald, Glenn, MacAskill Ewen (June 7, 2013) " Obama Orders U.S to Draw Up Overseas Target List of Cyber-Attacks. The Guardian, Retrieved on April 23, 2017.
[60] Ibid.
[61] Rizzo, J.(August 02, 2012) "Cybersecurity Bill Fails in Senate." CNN. Retrieved on April 23, 2017
[62] Gellman, Barton. (December 24, 2013). "Edward Snowden, After Months of NSA Revelations, Says his Mission's Accomplished" The Washington Post, Retrieved on March 23, 2017.

2004[63]. The policy directive is closely linked to the classified unpublished directive by the NSA called the NSPD-54 which was signed and authorized by George W. Bush. NSPD-54 had given authority to the U.S government to conduct surveillance through monitoring.[64]

The Presidential Policy Directive-20 Offensive Cyber Effects Operations (OCEO) is defined as "Operations and related programs or activities … conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States government networks."[65] In the PPD, the criteria for offensive cyber operations in the directive is not limited to retaliatory action but it is vaguely framed in order to advance the U.S national objectives around the world. The U.S government was also acknowledged to be participating in the major cyberattack which was subjected to controversy, namely, Stuxnet.[66]

The full classified document repeatedly elaborated that all cyber attacks should be done in accordance with the U.S law as a complement to the diplomatic and military options. The document emphasizes the U.S national interest as written below:

"Matters of vital interest to the United States to include national security, public safety, national economic security, the safe and reliable functioning of 'critical infrastructure' and the availability of 'key resources'.[67]

Elaboration of the purpose and scope of the cyber operations is written on the PPD-20 as seen below:

"The United States has abiding interest in developing and maintaining use of cyberspace as an integral part of the U.S national capabilities to collect

[63] Presidential Direcetives and Cybersecurity (PPD-20). EPIC. Retrieved on April 23 from http://epic.org/privacy/cybersecurity/presidential-directives/cybersecurity.html.
[64] Presidential Policy Directive/PPD-20 P.3. Retrieved on April 23, 2017 from https://fas.org/irp/offdocs/ppd/ppd-20.pdf
[65] Ibid.
[66] Ibid.
[67] Ibid. P.9

intelligence, to deter, deny, or defeat ay adversary that seeks to harm U.S national interest in peace, crisis, or war."[68]

Under the guiding principles of how the OCEO is conducted, it is stated that the conduct of OCEO is integrated as appropriate with other "diplomatic, informational, military, economic, financial, intelligence, counterintelligence, and law enforcement options, taking into account effectiveness, costs, risks, potential consequences, foreign policy, and other policy consideration." The OCEO is believed by the U.S government to be able to offer unique and significant consequences; however it would take more time and effort if the tools and access do not exist.

"The United States Government shall identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capability integrated as appropriate with other U.S offensive capabilities."[69]

3.2. The United States Cyber Warfare Doctrine

Despite the fact that cyber warfare is considered a non-kinetic, or a less violent type of warfare, the results actually can actually cause damage to critical infrastructures, despite causing less number of human casualties. The cyber battlefield is considerably different yet its doctrine is necessary in order to posses and acquires the sufficient guidelines in executing cyber-attacks. Doctrine is the fundamental principle of military forces and the elements thereof serve as a guide for their actions in support of national objectives. [70] Doctrines, authoritative in nature, require judgment in the application.[71] Every nation's military doctrine is

[68] Presidential Policy Directive/PPD-20 P.4. Retrieved on April 23, 2017 from https://fas.org/irp/offdocs/ppd/ppd-20.pdf
[69] Ibid. P.9
[70] Andreas, Jason, and Winterfield, Steve. (June 1, 2011)"Cyber Warfare: Techniques and Tools for Security Practitioners."P.37 Retrieved on April 23, 2017
[71] (November 8, 2010) Department of Defense Dictionary of Military and Associated Terms."Joint Publication 01-02" Retrieved on April 23, 2017

under the influence of traditions, guidance, literature, tactics, techniques, as well as procedures. In a deeper understanding, a doctrine represents a set of rules embodied in the government to maintain the standard of procedures.

A comprehensive knowledge of the assets is crucial to create infrastructure that supports the cyber warfare doctrine. The line between cyber warfare and traditional warfare lies on the implemented policy, as the role of information is the central element for both the former and the latter. Military forces heavily rely upon the systems that provide the speed of command so as to achieve the information. Thus, the results of network-centric operations make a significant strategic advantage to cyberspace as a battlefield. Moreover, the Department of Defense (DoD) have defined the importance of Information Operations (IO) of quite a number of reports and paper trails. The DoD have also identified 5 core capabilities of Information Operations (IO), the integration of Electronic Warfare (EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC).[72]

3.2.1. DoD Directive No.3600.1 Information Operations. October 2013

The Department of Defense (DoD) Directive No.3600.1 was reissued in accordance with the DoD authority. Such is a regulation that implemented a directive policy by assigning some responsibilities as well as delegating authority to those working with and in the military. DoD Directive established and described policies under specific programs by also defining missions and assigning more responsibilities.

The DoD policies, under the issue of Information Operation (IO) was written as follows[73]:

[72] February 13 2006. Joint Publication (JP) 3-13 Information Operations. Retrieved on April 23 2017 from http://www.information-retrieval.info/docs/jp3_13.pdf
[73] May 2013. DOD Directive No.3600.1, Information Operations. Retrieved on April 23,2017 from http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf

a. Information Operations (IO) will be the principle mechanism used during military operations to integrate, synchronize, employ, and assess a wide variety of information-related capabilities (IRCs) in concert with other lines of operations to effect adversaries 'or potential adversaries' decision-making while protecting our own.

b. IRCs constitute tools, techniques, or activities employed within a dimension of the information environment (IE) that can be used to achieve a specific end at specific time and place. IRCs can include, but are not limited to, variety technical and non-technical activities that intersect the traditional areas of electronic warfare, cyberspace operations, military information support operations (MISO), military deception, (MILDEC), influence activities, operation security, (OPSEC), and intelligence.

c. The development and management of individual IRCs will be the responsibility of various DoD components and will be brought together at a specific time and in a coherent and integrated fashion for use against adversaries and potential adversaries in support of military operations.

d. DoD IO will be coordinated and, as practicable, integrated with related activities conducted by allied nations and coalition partners.

The Combatant Commanders, whose tasks are to provide command and control of the U.S military services, was assigned to utilize IO as the principles mechanism, as written below[74]:

[74] May 2013. DOD Directive No.3600.1, Information Operations. Retrieved on April 23,2017 from http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf

a. Utilize IO as the principal mechanism to integrate, synchronize, employ, and adapt all IRCs in the IE to accomplish operational objectives against adversaries and potential adversaries.
b. Develop, plan, program, and assess IO as well as IRC execution in support of IO during all phases of military engagement and at all levels of war.

The question on who is in charge and in control of U.S cyberwarfare has been hanging and debatable for several years. Despite all U.S Air Force, Army, as well as the Navy having their own cyber operation divisions, the task of Computer Network Operation (CNO) has been assigned to the U.S strategic Command (USSTRATCOM) and the National Security Agency (NSA). Both of these institutions as assigned to operate the mission of defending all the U.S military networks. THE USSTRATCOM, specifically, has the responsibility to coordinate space operations and cyber space operations, among others, in support of international operations. (IO).[75]

3.2.2. DOD Information Operations Roadmap

The Information Operations Roadmap published on October 30 2003 aimed to provide the Department in helping them advance and achieve the goal of IO as the core of military competency.[76] This roadmap provided a common framework for understanding the Information Operations and the policies to integrate IO. Similar to any other roadmaps, it consolidates oversight, advocacy, and analytic support of IO.

The objective of said roadmap is also set to transform IO into becoming a core military competency on the same level of air, ground, maritime, and special

[75] May 2013. DOD Directive No.3600.1, Information Operations. Retrieved on April 23,2017 from http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf
[76] October 20 2003. Department of Defense Information Operations Roadmap. Retrieved on May 2 2017 from http://nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf

operations. To summarize, three key points of importance were identified, which includes[77]:

a. "We Must Fight the Net". At the time, DoD was building an information-centric force, as networks were becoming an increasingly center of gravity for institutions.
b. "We Must Improve Psychological Operations (PSYOP)". Psyops must be prepared in military forces in order to be consistent with national security objectives as well as national-level messages.
c. "We Must Improve Network and Electro-Magnetic Attack Capability". The DoD believed that in order to be influential in an information-centric fight, they have to dominate the electromagnetic spectrum with attack capabilities. This means, the DoD is fully aware of the support for the implementation of CNA capability with a rapid improvement.

The full spectrum of IO emphasizes the contribution that it provides, especially in military operations during peace, crisis, and war. The main concepts of the function of IO are elaborated as[78]:

a. "Deter, discourage, dissuade and direct an adversary, thereby disrupting his unity of command and purpose while preserving our own."
b. "Protect our plans and misdirect theirs, thereby allowing our forces to mass their effects to maximum advantage while the adversary expends his resources to little effect."
c. "Control adversarial communications and networks and protect ours, thereby crippling the enemy's ability to direct an organized defense while preserving effective command and control of our forces."

[77] October 20 2003. Department of Defense Information Operations Roadmap. P.6-7. Retrieved on May 2 2017 from http://nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf
[78] Ibid. P.8

In addition to the above, when implemented to its full effect, seizing control of the adversary communications and networks could allow control of enemy networks and communication-dependent weapons, infrastructure, as well as command and control of battlespace management functions[79]. This desired effect will achieve operational effects in support of a military deception plan.

3.2.3. Joint Publication (JP) 3-13 Information Operations

The U.S Forces acknowledges the importance of information environment, which is why they have defined information as a "strategic resource, vital to national security, and military operations depend on information and information systems for many simultaneous and integrated activities."[80] In order to succeed, the U.S has a doctrine that provides Joint Force Commanders (JFCs) and their staff to help prepare a plan and execute information operations to support joint operations, as it is necessary to maintain U.S and its allies superiority in the information world.

The JP 3-13 also realizes that the instruments of national power which includes diplomatic, informational, military, economy shall provide leaders with an utmost advantage in dealing with crisis around the world. Being fully-aware of such significance of information-related capabilities, in the case of Stuxnet, the focus of IO is based on the human decision-making or automated decision support systems with specific actions, which is by taking actions to affect the infrastructure that collects, process, and/or store information in support of targeted decision makers. This publication also stated that all IO capabilities can be implemented in both offensive and defensive operations, with the main accomplishment of destroying a system or entity until it cannot perform any basic functions without being entirely re-assembled.

[79] October 20 2003. Department of Defense Information Operations Roadmap. P.8 Retrieved on May 2 2017 from http://nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf
[80] February 13 2006. Joint Publication (JP) 3-13 Information Operations. Retrieved on May 6th 2017 from http://www.information-retrieval.info/docs/jp3_13.pdf

3.3 The United States Cyber Warfare Methods

Today, all political and military conflicts may be inflicted in the cyber dimension. Attackers now have a wide variety of effective cyber warfare strategies and tactics. According to Kenneth Geers, who is based in the Cooperative Cyber Defense Centre in Estonia, state and non-state actors prefer the play on cyber tactics, starting from a well-thought of propaganda to the manipulation of an adversary's critical infrastructure.[81] Globalization and the internet have strengthened the way nation-states control the international conflict as much as they can.

Among the five core capabilities identified by the Department of Defense, Computer network operations (CNO), is comprised of three types of operations, namely Computer Network Attack (CNA), Computer Network Exploitation (CNE), and Computer Network Defense (CND).[82] In relevance to this research, the author will only elaborate on CNE and CNA.

3.3.1 Computer Network Attack (CNA)

Defined as the action taken through the use of computer networks for the purpose of disruption, deny, and destruction of information in a computer network, CNA differs from typical attacks conducted by common hackers. CNA relies on the data stream to execute attacks, that may send a code or instruction to the central processing unit that cause the computer to experience power shortage supply, thereby leaving the computer unusable.[83] Successful CAN depends on the intelligence of its well-defined intention and a clear understanding about the effects from the execution.

---

[81] Geers, Kenneth. (August 27 2008) "Cyber Space and the Changing Nature of Warfare".Retrieved on May 7, 2017 from http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf

[82] February 13 2006. Joint Publication (JP) 3-13 Information Operations. CH. II-4

[83] April 12 2001. Joint Publication 1-02 DoD Dictionary of Military and Associated Terms. Retrieved on May 7, 2017 from http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%2801%29.pdf

There are certain methods of destruction using CNA depending on the intended purpose. The unique feature of CNA offers several implications to the practitioners and policy makers as its potential anonymous nature might cause the user of CNA technique to widely accomplish several political and economic objectives. Computer network attacks could cause the widespread suffering of targeted nation-states, if may be. The result of this is usually a short or long duration of infrastructure shutdown, or any computer-controlled life-support systems.[84]

The act of CNA is a force where the attack can cause physical destruction towards tangible property and harm some foreseeable results.[85] Such techniques of offensive computer network disruption occur without revealing the source or even the method of the attack itself. CNA is largely considered as a non-kinetic environment which is less costly and accessible and has a strategic effect. One of the techniques widely used is the injection of viruses or malwares to the computer network so that it destroys or gathers intelligence for the executor or both simultaneously. Frameworks that establish U.S offensive cyber security strategy is also stated in the following policy directives: In February 2003, the Bush administration also released a national-level guidance known as National Security Presidential Directive 16, to develop guidelines for offensive cyber warfare in regards to CNA[86]. The National Security Presidential Directive 38 (NSPD-38) on 2004, NSPD-54 on 2008, and the Presidential Policy Directive 20 (PPD-20) on 2012 were all the presidential directives issued to authorize cyber security efforts

[84] Dinstein, Y. "Computer Network Attacks and Self-Defense" Retrieved on April 8, 2017 from https://www.usnwc.edu/getattachment/26796276-0919-4699-b2f0-5f15f46cb894/Computer-Network-Attacks-and-Self-Defense.aspx

[85] Michael N. Schmitt. "Computer Network Attack and the Use of Force in International Law" Research Publication 1 Information Series. Retrieved on May 8, 2017

[86] Wilson, C. September 2006. "Information Operations and Cyberwar: Capabilities and Related Policy Issues." Retrieved on May 8, 2017 from https://ipmall.law.unh.edu/sites/default/files/hosted_resources/crs/RL31787_060914.pdf

that included all the initiatives to protect cyberspace and government policy on offensive cyber actions.[87]

3.3.2 Computer Network Exploitation (CNE)

The term Computer Network Exploitation (CNE) is referred to the ability to exploit data or information gathered on a target adversary in support of CNA.[88] CNE prepares an IO through intelligence, surveillance, and reconnaissance, through extensive planning and analysis. This involves actions such as espionage, usually though the penetration of adversary network systems to gain intelligence on enemy vulnerabilities, or with aims to make unauthorized copies of important files.[89] Computer network exploitations are implemented in similar ways as CAN, yet used to collect intelligence, rather than to disrupt critical infrastructures.

The National Security Agency, as the main U.S intelligence agency, has infected, or "implanted" approximately 50,000 computer networks using CNE by installing malicious malwares. [90] The NSA computer attacks are performed by specialized team called the Tailored Access Operations (TAO). These attacks are then designed to compromise routers, switches and firewalls to monitor adversary networks. According to the Washington Post, U.S intelligence services have carried out 231 offensive cyber operations, mostly those of CNE nature[91]. These so-called implants persist through software and upgrades of equipment, which is then used to copy stored data and tunnel into compromised networks from the outside. Nearly three-quarters of the operations were reported to have been carried out upon Iran, Russia, China, and North Korea, whose activities involve

[87] Electronic Privacy Information Center. Epic.org "Presidential Directives and Cyber Security" Retrieved on May 8, 2017
[88] Denning, D. E. "Assessing the Computer Network Operations Threat of Foreign Countries." Retrieved on May 8, 2017.
[89] Wilson, C. September 2006. "Information Operations and Cyberwar: Capabilities and Related Policy Issues." Retrieved on May 8, 2017
[90] Constantin, L. November 25 2013. "NSA infected 50,000 Networks with Specialized Malware." PC World. Web. Retrieved on May 8, 2017.
[91] Gellman, B and Nakashima E. August 31 2013. "U.S Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents show." The Washington Post. Retrieved on May 8 2017.

nuclear proliferation.[92] Despite the documents provided and facts presented by Edward Snowden, the Obama administration treats such cyber operations as covert and refuses to admit to them. Below is the map showing CNE-targeted countries in 2012.

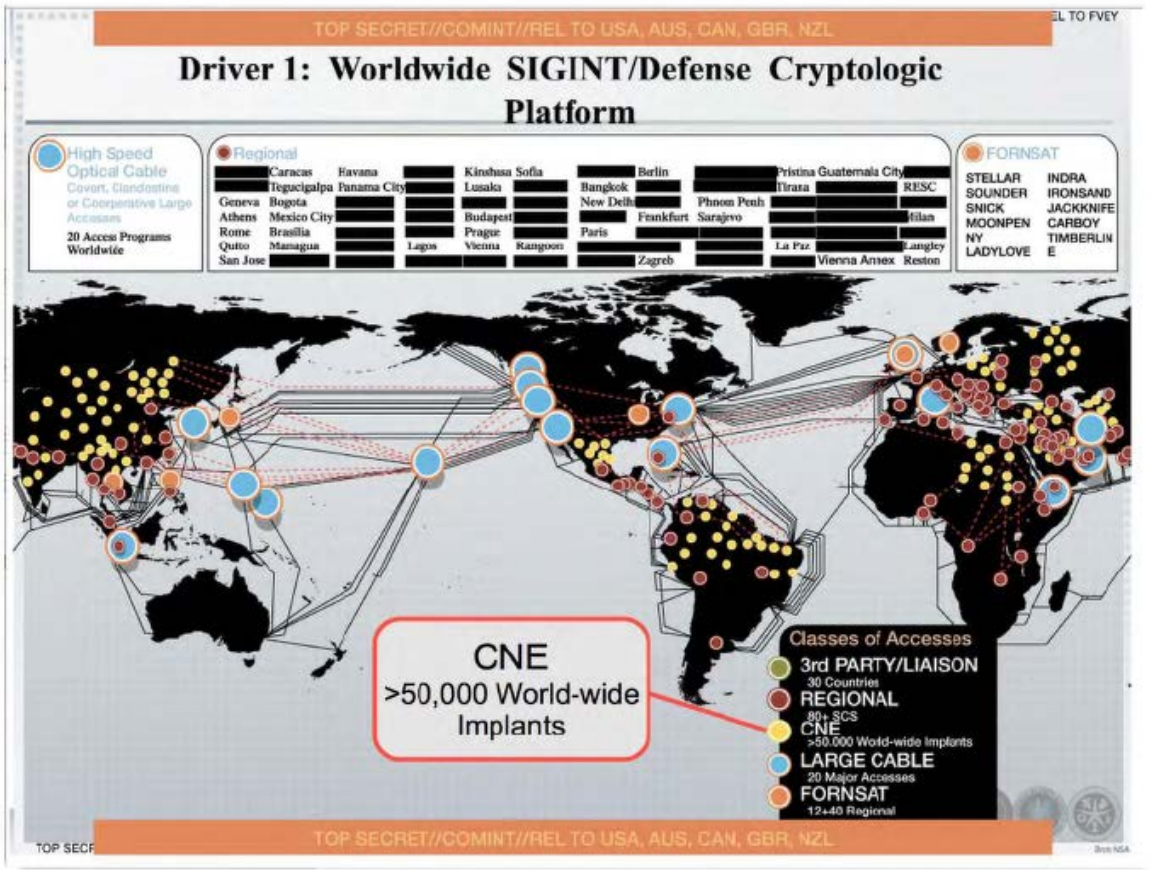

Figure 1: U.S National Security Agency Cyber Operations Year 2012.[93]

The figure above was published by the U.S National Seucirty Agency in 2012, titled the 'Worldwide SIGINT/Defense Cryptologic Platform' and was leaked by former NSA contractor Edward Snowden. It provides a visual

[92] Gellman, B and Nakashima E. August 31 2013. "U.S Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents show." The Washington Post. Retrieved on May 8 2017.
[93] Edward Snowden Foundation, November 23 2013, Worldwide SIGINT/Defense Cryptologic Platform, Retrieved on May 8 2017 from https://edwardsnowden.com/2013/11/23/worldwide-sigintdefense-cryptologic-platform/

representation of how the NSA has infected more than 50,000 computer networks worldwide with malicious software designed to steal sensitive information through CNE, or Computer Network Exploitation. It also documents multiple forms of access to the internet through its FORNSTAT (or Foreign Satellite Collection) program. It identifies “80+” “regional” forms of access in cities around the world via the “Special Collection Service”. The larger blue points indicate the 20 Access Programs worldwide, the red points on the regional forms of access in cities, the orange points indicate the FORNSTAT forms of access, and the yellow points indicate the CNE operations.

CHAPTER IV:

THE IMPLEMENTATION OF THE U.S CYBER WARFARE STRATEGY: OPERATION OLYMPIC GAMES

This chapter will be discussing the Operation Olympic Games (OOG) in detail providing its historical background. The historical background of the three codes addressed in the OOG, namely Stuxnet, Duqu, and Flame, will also be elaborated. The chapter will also mention the timeline of the attacks, which are influenced by the discovery of the United States Offensive Cyber Operations (OCEO) and other supporting documents of U.S cyber warfare doctrines mentioned in the previous chapter.

4.1 Historical Background of Operation Olympic Games

Operation Olympic Games (OOG) was a clandestine and still unacknowledged operation campaign of sabotage using cyberspace to disrupt Iran nuclear facilities. This operation was carried out unnoticed by the general public. According to the U.S Department of Defense Dictionary of Military and Associated Terms, Clandestine Operations [94] is defined as "An operation sponsored or conducted by governmental departments of agencies in such a way as to assure secrecy or concealment. A clandestine and a covert operation differ, in terms of the concealment. A clandestine operation is focused on the concealment of the operations, while covert operations emphasize more on the concealment of identities or sponsors of the operation. On rare occasions such as this, however, an operation can be both clandestine and covert, both focusing on intelligence-related activities.

[94] Joint Publication JP 1-02, January 5 2017, "DoD Dictionary of Military and Associated Terms" Retrieved on May 9 2017 from http://marineparents.com/downloads/dod-terms.pdf

The OOG is also considered a covert operation (CoveOps) that is conjointly done with Israel. In general, Covert operations are intended to create political effects that might have implications in the military, intelligence, as well as law enforcement. The implementation is intended to achieve the desired effect without letting any parties know who sponsored or carried out the operations.

In June 2002, while giving out a speech in New York, former U.S President George Bush stated that the spread of chemical, biological, as well as nuclear, along with ballistic missile technologies were becoming the U.S and its allies' gravest danger.[95] Hence, as per written on the U.S National Security Strategy in 2006, Iran was considered a nation that preserved tyrannical political system, and a sponsor of terrorism; in addition to that, Iran also had hidden many of its nuclear developments with the international community, all the while failing to comply with international obligations with the International Atomic Energy Agency (IAEA) an access to its nuclear facilities[96]. All these issues threatened the U.S national security. Leaked information told by officials in the U.S National Security Agency stated that cyber weapons had been designed since 2006, during the Bush administration. The U.S and Israel had developed the sophisticated cyber weapon with aim of slowing Iran's ability in developing nuclear weapons.[97] This effort involved the likes of institution such as the National Security Agency, the CIA, and Israel's military.[98] One of former U.S high-ranking intelligence officials also admitted that the cyber weapons were to prepare the battlefield for future possible covert actions.[99]

At the beginning of the operation, dating back to 2006, the U.S during Bush's tenure seemed to acknowledge a few good options in dealing with Iran,

[95] June 1 2002, "Text of Bush's Speech at West Point". New York Times. Retrieved on May 9 2017 from http://www.nytimes.com/2002/06/01/international/text-of-bushs-speech-at-west-point.html
[96] March 2006, "National Security Strategy of the United States of America." Retrieved on May 9 2017 from https://www.state.gov/documents/organization/64884.pdf
[97] Nakashima, E, Miller G, and Tate J. June 19 2012, " U.S, Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say. " The Washington Post. Retrieved on May 9 2017.
[98] Ibid.
[99] Ibid.

but was left with limited options, after just having had accuse Iraq falsely of the reconstitution of its nuclear program.[100] Being left with only a few options, Vice President Dick Cheney at the time urged the current President to consider launching a military strike against Iran's nuclear plantation facilities, however, the Bush administration came to a conclusion that the region was already amidst a war and another military attack would further worsen the region and have unfortunate results. [101]

Despite International efforts and sanctions, Iran kept resuming its uranium enrichment at its Natanz nuclear facility. Iran's leader at the time, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described his great ambition of installing around 50,000 centrifuges in the facility.[102] This ambition caused a great deal of concern for U.S and other major countries in Europe, and more significantly, Israel. The uranium enrichment ambitions had then raised tremendous insecurity and suspicions to the rest of the countries.

Initially, The Central Intelligence Agency had been trying to introduce faulty systems and designs into Iran's systems but caused relatively little effect. The United States Strategic Command then established a small cyber operation, led by General James E. Cartwright, proposed an idea to the President, such of a sophisticated cyber weapons far more advanced than the U.S had ever designed before. [103]

In order to develop this program to its full potential, the U.S didn't work alone. It had collaborated with Israel's Signal Intelligence, Unit 8200, whose technical expertise and cyber skills was as equivalent; if not more than the NSA's itself[104]. Moreover, Israel's involvement in this operation was due to Israel

[100] Sanger, David. (1 June 2012) "Obama Order Sped Up Wave of Cyber Attacks Against Iran." The New York Times. Retrieved on May 9 2017.
[101] MacAskill, E. and Borger, J. (16 July 2007)"Cheney Pushes Bush to Act on Iran". The Guardian. Retrieved on May 9 2017.
[102] Sanger, David. (1 June 2012) "Obama Order Sped Up Wave of Cyber Attacks Against Iran." The New York Times. Retrieved on May 9 2017.
[103] Ibid.
[104] Ibid.

having vital information about the Natanz power plant, as well as to persuade Israel from deploying a military attack from air against Iranian nuclear facilities.[105] In order for Israel to be convinced, they had to be absolutely sure that the cyber weapon they develop was working. The so-called cyber weapon was a form of malware called "the Bug", but was later dubbed "Stuxnet".

This ultimate goal of this operation was to sabotage the uranium enrichment facility of Iran by reprogramming the command and control of the fast spinning centrifuges, which would result in destroying the vulnerable centrifuge rotors. [106] What had been a weapon designed to a specific action, was now spread to the internet, leading to the investigation of its origins by experts. The Stuxnet worm had become public due to a programming error and has spread outside Natanz power plant and became widespread on the internet, targeting other countries, as well. The ambitious attempts to deliberately slow the progress of Iran's nuclear program also in turn was comprised of three different codes of worms, each respectively having its own functions, namely Stuxnet, Flame, and Duqu.

4.2 Operation Olympic Games Timeline

The timeline of the Operation Olympic Games could be traced back to 2006, to when the U.S was still under Bush administration. Below is the timeline of the events on when the attack was deployed.[107][108]

Table 2: Timeline of the Operation Olympic Games

No.	Time of Discovery	Description
1.	2006	Iran resumes uranium enrichment at

[105] Sanger, David E. (2 June 2012) "Mutually Assured Cyberdestruction?" The New York Times. News Analysis. Retrieved on May 9 2017.
[106] Lendvay, R. (March 2016) " Shadows of Stuxnet: Recommendations for U.S Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack." California Naval Post-Graduate School. Retrieved on May 9 2017.
[107] Jim Finkle, (December 2 2011), "Factbox: Cyberwarfare Expert's Timeline for Iran Attack." Reuters, Retrieved on May 9 2017.
[108] Guilbert, G. "How a Secret Cyber Program Worked" New York Times. Retrieved on May 9 2017.

		Natanz after negotiations with European and American officials flounder. U.S military and intelligence agencies propose top-secret cyber war program against Iran.
2.	May 2006	First components of Stuxnet attack code developed.
3.	Early 2007	Code name Operation Olympic Games begin. A replica of the Natanz facility was built in the U.S, all while in collaboration with Israel.
4.	Early 2007	Duqu deployed to electronically map Natanz networks.
5.	Late 2007	Engineers write the code for "digital bomb component of Stuxnet that would damage sensitive equipments when attack is executed.
6.	2008	Centrifuges begin crashing at Natanz nuclear facility. Engineers at the plant under the assumption that programming went wrong. Initial breakdowns are designed to seem like small random accidents, with different code variations having different breakdowns.
7.	2009	As President Bush was leaving office, he urges President Obama to continue Olympic Games, in which Obama complied.
8.	April 2009	Stuxnet attack begins on 30th anniversary of the Iranian Islamic Republic.

9.	Late 2009	IAEA cameras captured workers removing broken centrifuges
10.	Early 2010	The NSA and Israel's Unit 8200 decide to target the critical array of centrifuges composed of 1,000 machines, if succeeded, would cause a huge setback to Iran.
11.	June 2010	Computer security firm VirusBlokAda first identifies Stuxnet presence in Iran.
12.	July 2010	Stuxnet had spread to the Internet, being quickly replicated. In weeks, news of the virus that exploits a hole in the Windows operating system was widespread. Obama decided not to stop the program, with a subsequent attack taking out around 1,000 Iranian centrifuges, 1/5 of those operating.
13.	November 2010	President Ahmadinejad publicly discloses that a cyberweapon had damaged its centrifuges at his nuclear facilities.
14.	September 2011	The Budapest University of Technology and Economics analyzed a new worm, named Duqu, to be related to Stuxnet.
15.	November 2011	The head of Iran's civil defense organization, Gholam Reza Jalali, told news agencies that infected computers were all being checked and Iran had also developed a special software to combat such attacks.

16.	May 2012	The new malware, "Flame" was discovered, although different from Duqu and Stuxnet, it also infects through usb drives.
17.	June 2013	Leaked 18-page Presidential Policy Directive 20 on Offensive Cyber Effect Operations published on the Internet.

4.3 Stuxnet

On January 2008, Israel sought permission from the U.S to bomb Iran by approaching former President Bush to launch an air strike against the Iranian uranium enrichment facility. Israel believed that the attack would hinder Iran a three-year setback, the request, however, was refused by the U.S.[109] On April 2008, Iran began installing 6,000 centrifuges to enrich uranium at its main nuclear plant in Natanz, of which the capacity were five times greater than the ones that were already made.[110]

An IAEA report released on September 2010 stated that around 160 centrifuges in Iran's facility had been taken offline without giving any specific reasons for being shut down. However, at that time, Iran's officials refused to admit that Stuxnet have had anything to do with the on-going delays of the Iran's nuclear programs. [111] Security response at Symantec also reported that 60% of Stuxnet targets Iran's nuclear critical infrastructure, which are Bushehr nuclear power plant and the Natanz nuclear facility.

Firstly discovered in June 2010 by a Belarusian cyber security firm named "VirusBlokAda", this unclaimed malware had been specifically engineered to

[109] Zetter, K. (7 November 2011) "Stuxnet Timeline Shows Correlation Among Events." Wired. Retrieved on May 10, 2017 from https://www.wired.com/2011/07/stuxnet-timeline/
[110] (8 April 2017) "Iran Installing New Centrifuges" BBC News. Retrieved on May 10, 2017
[111] (22 November 2010) " Stuxnet 'Hit' Iran Nuclear Plans" BBC News. Retrieved on May 10, 2017

target Siemens computer components, of which the centrifuges in Iran's Natanz nuclear facility was comprised. Unlike other malwares that have already existed, the newly discovered worm did not aim for a corporate or financial advantage like they usually do [112]; instead, the code was programmed to target the supervisory control and data acquisition (SCADA) system, reprogram the Programmable Logic Control (PLC) [113] and destroy the centrifuges of the facility. [114] Stuxnet was considered a cyber attack which caused significant physical damage to a critical infrastructure of the facility.[115] Ralph Langer, the man who discovered the existence of Stuxnet, spent three years studying its code, coming up with the analysis that Stuxnet was not about sending a message proving a concept, but destroying its targets with utmost determination in military style.[116]

Stuxnet's rate of success was also due to the insider threat of system access at the facility. It was initially spread through, according to Symantec, either a willing or unknowing third party, such as a contractor who perhaps had access to the facility, or an insider. The malware's propagation method was through the infection of USB removable devices, replicating itself into the computer systems each time it was used, from one computer into another.

A report made by Symantec in 2010 stated that the "concentration of infections in Iran likely indicates that this was the initial target for infections and was where infections were initially seeded." Below is a figure that indicated Iran

[112] Kushner, D. (February 26 2013) "The Real Story of Stuxnet". Retrieved on May 10, 2017 from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
[113] O'Murchu, researcher at Symantec. PLCs are programmed to turn on and off motors, monitor temperature, and turn on coolers if a gauge goes over a certain temperature.
[114] Sanger, David. (1 June 2012) "Obama Order Sped Up Wave of Cyber Attacks Against Iran." The New York Times. Retrieved on May 10 2017.
[115] Lendvay, R. (March 2016) " Shadows of Stuxnet: Recommendations for U.S Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack." Retrieved on May 10, 2017.
[116] Broad, W. J, Markoff, J., and Sanger, D. (January 15 2011) " Israeli Test on Worm Called Crucial in Iran Nuclear Delay" The New York Times. Retrieved on May 10, 2017

was the initial target, with other infections likely being the "collateral damage".[117]

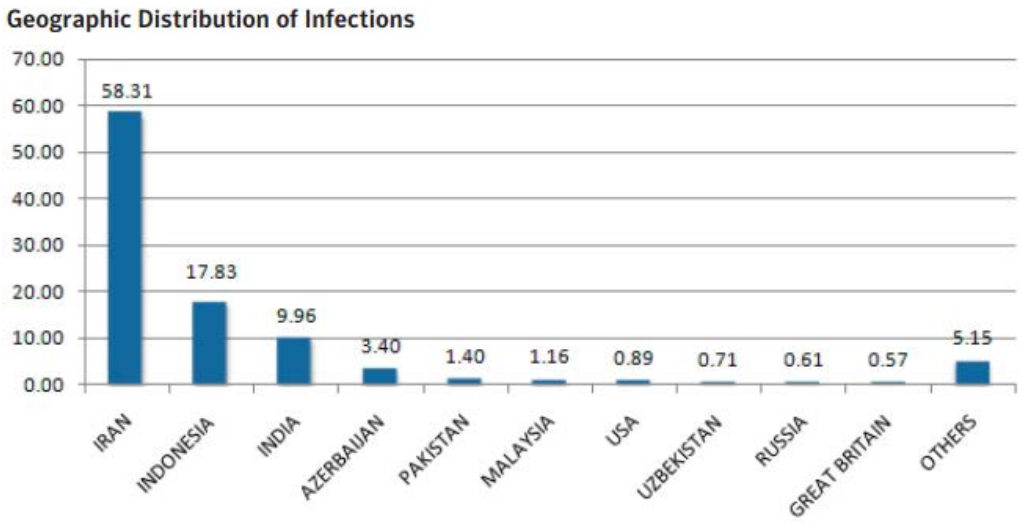

Figure 2: : Geographic distributions of infections with the percentages of affected computers.[118]

According to Ralph Langer, in his stuxnet analysis called "To Kill a Centrifuge, Stuxnet is a highly complex cyber weapon which required resources that of a nation-state level for intelligence gathering, infiltration, and testing during its development.[119] This is due to the fact that building a fully functional replica of a uranium enrichment facility would be beyond the reach of organized crime rings or terrorist organizations.[120] What made Stuxnet unique was also the fact that it was the first malicious software to have exploited four "zero-day" vulnerabilities, compromise two digital certificates, and was able to infect

[117] Falliere, N., O'Murchu, L., and Chien, E. (February 2011) "W32. Stuxnet Dossier" Retrieved on May 10 2017 from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
[118] Falliere, N., O'Murchu, L., and Chien, E. (February 2011) "W32. Stuxnet Dossier" Retrieved on May 10 2017 from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
[119] Langner, R. (November 2013) "To Kill a Centrifuge" Retrieved on May 9th 2017 from http://bruteforcelab.com/wp-content/uploads/To-kill-a-centrifuge.pdf
[120] Ibid. p.20

industrial control systems and hide the code from the operator.[121] A "zero day" refers to a vulnerability or exploitable gap in a computer program unknown to the developers, in which hackers may exploit this gap until the developers become aware and fixes it with a security patch. He also believes that Stuxnet has opened a "Pandora's Box" for cyber threats and that in the future, Stuxnet will serve as a blueprint for a more dangerous, and difficult to neutralize next generation of malware.[122]

4.4 Duqu

On September 1 2011, a collection of malware was discovered which was thought to be connected to the Stuxnet worm. The Laboratory of Cryptography and System Security (CrySyS Lab) of the Budapest University of Technology and Economics analysed the threat and wrote an extensive report, naming the threat Duqu. Duqu is considered a Trojan horse which was written by the same parties who also created Stuxnet. The purpose of these two malwares was different, however. Unlike Stuxnet, Duqu was created to perform industrial sabotage by collecting intelligence regarding its targets. The intelligence includes passwords, taking screenshots, user keystrokes, in order to spy on the user's actions and steal various documents.

The announcement of Duqu discovery was also on the Symantec website, saying that a similarity was found between Duqu and Stuxnet's original programming, especially its source codes and keys, the only difference being that Duqu was more sophisticated.[123] The similarity between those two was distinguished after the identification that the Duqu worm could not have been written without having access to the original programmer's instructions. Unlike Stuxnet, Duqu's purpose was to gather intelligence from the industrial control

[121] Falliere, O'Murchu, and Chien (February 2011) "W32. Stuxnet Dossier" Retrieved on May 10 2017.`
[122] Nakashima, E. (October 2 2010) "Stuxnet Malware is Blueprint for Computer Attacks on U.S" Washington Post, Print Edition. Retrieved on May 10, 2017.
[123] Rapoza, K. (October 21 2011) "'Duqu' Virus Likely Handiwork of Sophisticated Government, Kaspersky Lab Says." Forbes. Retrieved on May 10, 2017

system manufacturers, replacing it with general remote access capabilities,[124] possibly, to simplify the execution of future attacks. The program was designed to stay within 36 days and remove itself after infecting the system. The way it propagates and infects was through an infected Microsoft word document, allowing the virus to modify the computer's security protections.[125]

In November 2011, the head of Iran's civil defense organization, Gholamreza Jalali, said that some of its computer systems had been infected with the Duqu Troja, however, computers at all the main nuclear sites were being checked and that Iran already had software ready for combating the virus. [126] According to Symantec, Iran was one of eight countries targeted by this attack.[127] Below is a figure showing the geographical distribution of the Duqu-infected organizations in eight countries. These countries include France, Netherlands, Switzerland, Ukraine, India, Iran, Sudan, and Vietnam.

[124] (November 23 2011). "W32.Duqu: The Precursor to the Next Stuxnet" Symantec Retrieved on May 11 2017 from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf
[125] (November 23 2011). "W32.Duqu: The Precursor to the Next Stuxnet" Symantec Retrieved on May 11 2017 p. 2
[126] Jaseb, H. (12 November 2011), "Iran Says has Detected Duqu Computer Virus" Reuters. Retrieved on May 11 2017
[127] "W32.Duqu: The Precursor to the Next Stuxnet." Symantec. P.3

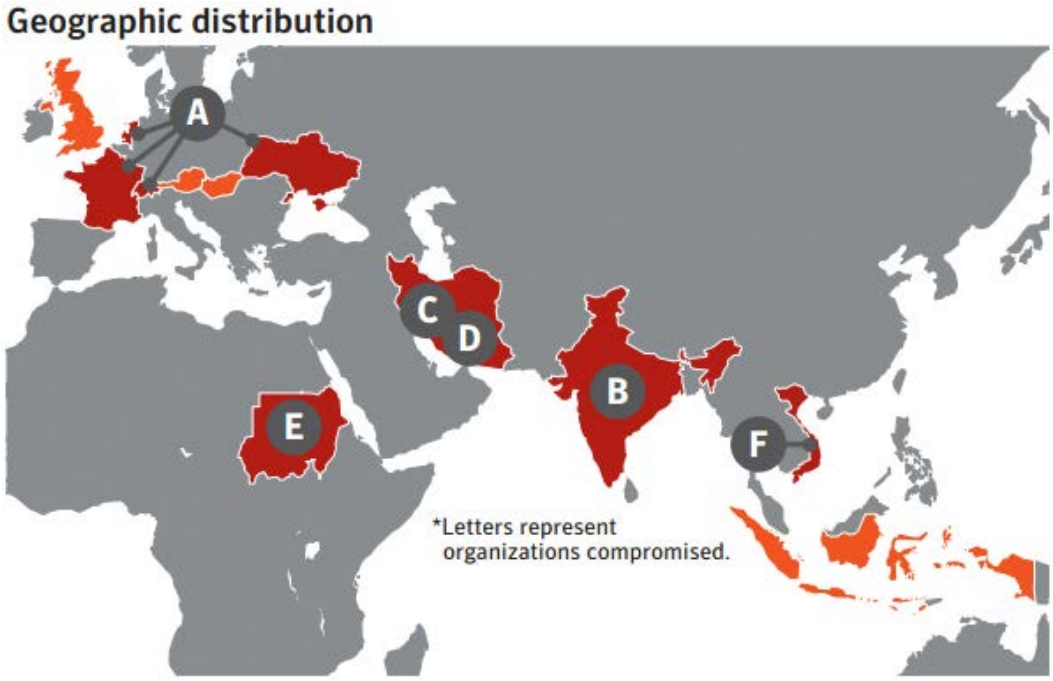

Figure 3:Countries with the most Duqu infections.[128]

4.5 Flame

In the following year, 2012, another malware named Flame was found and discovered within many Middle Eastern computer systems, Including Iran.[129] This malware was discovered by Iran's MAHER Center of National Computer Emergency Response Team (CERT), Kaspersky lab, and the CrySyS Lab of Budapest Technology University and was considered as the most complex and sophisticated malware ever found. [130]

[128] (November 23 2011). "W32.Duqu: The Precursor to the Next Stuxnet" Symantec Retrieved on May 11 2017 P.3
[129] Zetter, K. (May 28 2012) " Meet "Flame", the Massive Spy Malware Infiltrating Iranian Computers". Wired.com. Retrieved on May 12 2017
[130] (May 31 2012) "sKyWIper: A Complex Malware for Taregted Attacks). Technical Report by the Laboratory of Cryptography and System Security. Retrieved on May 12 2017.

The malware was detected in computers belonging to the Iranian Oil Ministry and the Iranian National Oil Company.[131] According to Kaspersky, Flame had existed since February 2010 and was involved in the disruption of Iran's nuclear program. Researchers also claim that the Flame malware may be developed by the same nation-state that was sponsoring the development of Stuxnet and Duqu, ruling out the involvement of cyber criminals. The purpose of Flame was also different than Stuxnet, Flame's programming was purely for espionage purposes. Using a method called Sinkholding[132], the virus mainly targeted PDFs, text files, recorded conversations, and keystrokes. Aside from this, after the system is infected, the malware is able to tweak and add new functionalities to the system. Like Stuxnet, Flame has the ability to spread by infecting USB sticks. However, unlike its counterparts, flame has a kill module, or an elimination function that removes all traces of malware on the system, so that nothing is left and it will not be easily detected. [133] Flame also had remained undetected until 2012 due to its ability to masquerade as a routine Microsoft update.[134]

Although the fundamental function of Flame was generally the same as other malware component, such as recording keyboard activities, Flame was 20 times more complicated than Stuxnet ever was. The size of Flame was over 20 MB, and the way Flame gathers information was quite comparable to Duqu, as it has the ability to record audio if a microphone is attached to the infected system, screen capture and transmit visual data, including personal messages.

---

[131] Zetter, K. (May 28 2012) " Meet "Flame", the Massive Spy Malware Infiltrating Iranian Computers". Wired.com. Retrieved on May 12 2017

[132] Vitaly Kamluk, Senior researcher for Kaspersky " Sinkholding is a procedure when we discover a malicious server- whether It is an IP address or domain name – which we can take over with the help of the authorities or the domain registrar."

[133] Zetter, K. (May 28 2012) " Meet "Flame", the Massive Spy Malware Infiltrating Iranian Computers".

[134] Nakashima, E., Miller, G., and Tate, J. (June 19 2012) " US, Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say." The Washington Post. Retrieved on May 13 2017.

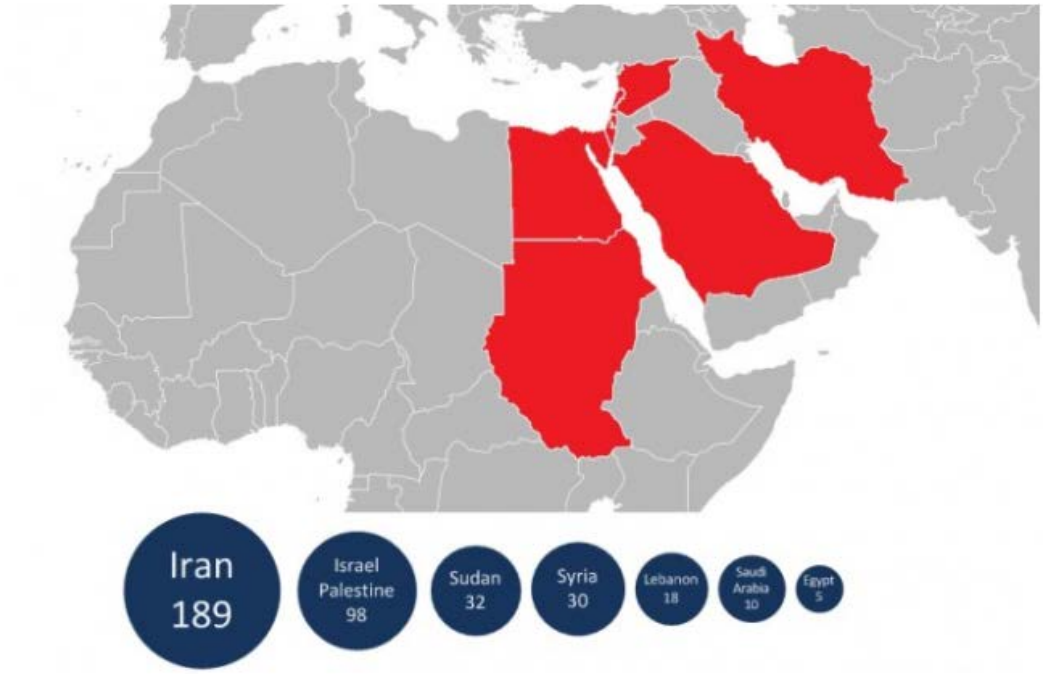

Figure 4: Number and geographical location of Flame Infections detected by Kaspersky Lab.[135]

Based on the data gathered by Kaspersky, a Russian-based cyber security firm, as of May 2012, Flame had infected approximately 1,000 machines, with targets including governmental organizations, educational institutions, as well as private individuals. Besides Iran being the country with the most attacks, countries like Israel, Palestine, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt were also attacked, as shown above.[136] Despite this, Iran's MAHER National Computer Emergency Response alerted the media that the detection and clean-up tool was finished within the same year.

[135] Zetter, K. (May 28 2012) " Meet "Flame", the Massive Spy Malware Infiltrating Iranian Computers". Wired.com.
[136] Zetter, K. (May 28 2012) " Meet "Flame", the Massive Spy Malware Infiltrating Iranian Computers".Wired. Retrieved on May 13 2017.

4.6 Implications for Government and Private Sectors

As quoted by the Department of Homeland Security,

"Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks."[137]

The implication of the Stuxnet attacks towards government as well as private sectors are very much intertwined, in terms of consequences, as it shows the vulnerability that an operational infrastructure possess. It may also create damage, threaten lives, or interfere with crucial services of civilians. [138] According to the U.S Government Accountability Office, the U.S private sectors own 85% of the critical infrastructure in the country[139], so impacts of a cyber attack on industrial control systems could very well have physical, economic, and social effects. Physical impacts include personal injury, loss of lives, and property and environmental damage, especially in the healthcare, food and agriculture, and transportation systems sectors. Negative effects to the local, regional, and national economy are also a result from the physical impacts, which include the energy reactors, financial services, and critical manufacturing sectors; as this could also affect the short-term profits of those companies. Lastly, social impacts of such attacks could also induce the lack of trust by the public society

[137] (September 27 2016) "Cybersecurity Overview," U.S. Department of Homeland Security, Retrieved on May 14 2017 from http://www.dhs.gov/cybersecurity-overview.
[138] Ibid.
[139] U.S Government Accountability Office, "Critical Infrastructure Protection – Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics" P. 1 Retrieved on May 14 2017.

towards the company or government operating the infrastructures impacted by such attacks. [140]

The predominant view of many security observers appears to be that the recent emergency of the Stuxnet worm may be a new type of threat that could potentially lead to short and long-term adverse global security consequences. The stuxnet worm is unique because the software code appears to have been designed to infiltrate and attack an Industrial Control System (ICS) often used by critical infrastructures in facilities in order to cause long term physical damaged to them. Although the full extent of damage caused by the Stuxnet worm is unknown, the potential implications of such a capability are numerous in that the worm's ability to identify specific ICSs and wait for a time to launch an attack could have catastrophic consequences on any nation's critical infrastructures, especially the United States.

4.7 The United States Cyber Warfare Results

The Olympic Games operation is perceived to be successful, as Stuxnet has broken new malware ground because of its complexity and designs. Its sole purpose was to sabotage high-frequency critical infrastructure in Iran's Natanz nuclear facilities. This event made the first known cyber operation to have disrupted physical equipments and machineries. The virus managed to delay Iran's uranium-enrichment program by 18 months to 2 years, due to the virus disabling 1,000 out of the 5,000 functioning centrifuges. [141] Former Head of National Security Agency and CIA Director under George Bush, General Mike Hayden, also stated, as quote "We have entered a new phase of conflict in which we use a cyber-weapon to create physical destruction, and in this case, physical

[140] Lendvay, R. (March 2016) " Shadows of Stuxnet: Recommendations for U.S Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack." P. 71-76 Retrieved on May 16, 2017

[141] Burton, J. (May 13 2015) "Cyber Warfare – A new Strategic Reality " Retrieved on May 15 2017 from https://natlib.govt.nz/blog/posts/cyber-warfare-a-new-strategic-reality

destruction to someone else's critical infrastructure."[142] Implied in this statement, the researcher believes, is the acknowledgement of accomplishment, however, it has also paved new vulnerabilities to the U.S itself, since the coding of the virus can easily be replicated or reprogrammed to be stronger, and could be used as retaliation.

[142] Kroft, S. (June 04 2012) "Stuxnet: Computer Worm Opens New Era of Warfare." CBS News. Retrieved on May 15 2017

CHAPTER V:

CONCLUSION

The cyber warfare strategy was that conducted by the U.S towards Iran under the Operation Olympic Games is just another fundamental way of the U.S to politically exercise its means of achieving national objectives. This also can be understood as part of the U.S diplomacy in interacting with Iran. The way the U.S dealt with Iran's nuclear program was at the time, the utmost concern. The U.S seeks to overcome this concern through something that does not result in casualties; effective yet invisible. Israel, on the other hand has become the U.S closest ally in the Middle East. Israel has also grown to become suspicious of Iran's ability to acquire uranium and its nuclear development program. Bilateral relationship between the two countries was also at mutual distrust and has been for decades. Moreover, Israel was also struggling and competing with Iran over regional influence. Hence, launching the Olympic Games Operation was an alternative and a very much preferred option compared to Israel's plan to launch an air strike over Iran's nuclear facilities. Therefore, the theory of neo-realism is in line with the development of cyber security as a new global threat, as this topic greatly discussed the reality of non-conventional warfare as a new dynamics in international relations.

In the history of cyberwarfare, experts viewed Operation Olympic Games as a game changer. It is now recognized as the first politically motivated cyber attack; a borderless weapon that caused physical damages to the critical infrastructure of a country. In this case, the United States strategy of conducting offensive cyber operations was deemed very effective. Aside from the economic sanctions as well as oil embargo that the U.S and its allies have imposed towards Iran, they do not seem to be effective to stop Iran from developing its uranium enrichment program. That way, the implementation of its cyber warfare strategy was very much necessary in suppressing Iran's regional influence. From the

aforementioned chapters that have elaborated how the operation was conducted, we can see the effect that the attacks had on Iran's nuclear facilities, and the damage it has faced; damaging thousands of Iran's uranium centrifuges at both Natanz and Bushr nuclear facilities. It is also addressed in this research how the industrial control system (ICS) of a critical infrastructure is very vital and vulnerable to cyber attacks. Its disruptions could also hamper the government's ability to provide domestic and international security, safety, and essentials for a period of time. The results of such attacks in Iran have also caused the degradation of Iran's ability to maintain national security goals and thereby make the nation more vulnerable to a variety of foreign and domestic threats.

Cyber threats to national critical infrastructure have raised several flags, which include the need to raise governmental role in protecting critical infrastructures and the reality of cyber "threats" as a growing international security issue. The growth of cyber warfare have also forced nation states to strengthen their development of cyber power so they would not become victims of other states with more advanced cyber capabilities. This is especially so, as it was already mentioned in the second chapter, many infrastructures and control systems were not engineered and programmed to withstand advanced cyber threats. The relation

In conclusion, cyber space has provided a new battle field for cyber warfare, a fifth dimension aside from air, land, maritime, and space.

BIBLIOGRAPHY

ARTICLES

" Stuxnet 'Hit' Iran Nuclear Plans" 22 November 2010.BBC News.

"Burma Hit by Massive Net Attack Ahead of Election". 11 August 2008. BBC News.

"Cyber War: War In the Fifth Domain" 1 July 2010. The Economist.

"Estonia Fines Man for CyberWar". BBC. 25 January, 2008

"Hackers Behind Ukraine Power Cuts, Says US Report." 26 February 2016. BBC News.

"Iran Installing New Centrifuges". 8 April 2008. BBC News.

"Russia Accused of Unleashing Cyber War to Disable Estonia" , 16 May 2017. The Guardian.

"Tallinn Tense After Deadly Riots" 28 April 2007. BBC News.

"Text of Bush's Speech at West Point". 01 June 2002. The New York Times.

Brewster, T. (20 March 2014) "There are Real and Present Dangers around the Internet of Things." The Guardian.

Broad, W. J, Markoff, J., and Sanger, D. (January 15 2011) " Israeli Test on Worm Called Crucial in Iran Nuclear Delay" The New York Times.

Constantin, L. November 25 2013. "NSA infected 50,000 Networks with Specialized Malware." PC World. Web.

Davis, Joshua. August 21, 2007. " Hackers Take Down the Most Wired Country in Europe", Wired.

Fildes, Jonathan. "Stuxnet Virus Targets and Spread Revealed." BBC News.

Gellman, B and Nakashima E. August 31 2013. “U.S Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents show.” The Washington Post.

Gellman, Barton. (December 24, 2013). “Edward Snowden, After Months of NSA Revelations, Says his Mission’s Accomplished” The Washington Post.

Greenwald, Glenn, MacAskill Ewen (June 7, 2013) “ Obama Orders U.S to Draw Up Overseas Target List of Cyber-Attacks. The Guardian,

Greenwald, Green and MacAskill, Ewen, ” (7 June 2013) “Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks, The Guardian.

Guilbert, G. “How a Secret Cyber Program Worked” New York Times.

Jaseb, H. (12 November 2011), “Iran Says has Detected Duqu Computer Virus” Reuters.

Jim Finkle, (December 2 2011), “Factbox: Cyberwarfare Expert’s Timeline for Iran Attack.” Reuters,

Kroft, S. (June 04 2012) “Stuxnet: Computer Worm Opens New Era of Warfare.” CBS News.

MacAskill, E. and Borger, J. (16 July 2007)”Cheney Pushes Bush to Act on Iran”. The Guardian.

MacAskill, E. and Borger, J. (16 July 2007)”Cheney Pushes Bush to Act on Iran”. The Guardian.

McElroy, Damien; Williams, Christopher (28 May 2012). Flame: World’s Most Complex Computer Virus Exposed”. The Daily Telegraph

Nakashima, E, Miller G, and Tate J. June 19 2012, “ U.S, Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say. “ The Washington Post.

Nakashima, E. (October 2 2010) “Stuxnet Malware is Blueprint for Computer Attacks on U.S” Washington Post, Print Edition.

Nakashima, Ellen, 2010, “Stuxnet Malware is Blueprint for Computer Attacks on U.S” The Washington Post.

Rapoza, K. (October 21 2011) “’Duqu’ Virus Likely Handiwork of Sophisticated Government, Kaspersky Lab Says.” Forbes.

Rizzo, J. (02 August 2012) “Cybersecurity Bill Fails in Senate.” CNN.

Rohan, B. (August 11 2008). ”Georgia Says Russian Hackers Blocked Government Websites”. Reuters.

Sanger, David E. (1 June 2012). “Obama Order Sped Up Wave of Cyberattacks against Iran”. The New York Times.

Sutherland, JJ (November 4 2010) “Myanmar’s Internet Under Cyberattack.”

Traynor, Ian, (17 May 2007) “Russia Accused of Unleashing Cyber War to Disable Estonia”, The Guardian.

Zetter, K. (7 November 2011) “Stuxnet Timeline Shows Correlation Among Events.” Wired.

Zetter, K. (May 28 2012) “ Meet “Flame”, the Massive Spy Malware Infiltrating Iranian Computers”. Wired.

Zetter, Kim. March 11, 2014, “ An Unprecedented Look at Stuxnet, The World’s First Digital Weapon”. WIRED.

BOOKS

Andreas, J. and Winterfield, S. “Cyber Warfare: Techniques and Tools for Security Practitioners.” Second Edition. Syngress Publications, October 30 2013.

Clarke, Richard A. & Knake, Robert K. “Cyber War: The Next Threat to National Security and What to do About it.” Harper Collins, New York, 2010.

Kothari, C.R (2004) Research Methodology: Method and Techniques (Second Revised Edition) New Delhi: New Age International Ltd.

JOURNALS

Boaru, G. and Badita, G., Romanian National Defense University, 2008. “Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems.”

Dana A. Shea 2004“Critical Infrastructure: Control Systems and the Terrorist Threat” Congressional Research Service.

Denning, D. E.(2007) “Assessing the Computer Network Operations Threat of Foreign Countries.” California Naval Postgraduate School, Center of Terrorism and Irregular Warfare

Kozlowski, Andrzej, (February 2004) “Comparative Analysis of Cyberattacks on Estonia, Georgia, and Kyrgyzstan” Retrieved on April 29, 2017 from http://www.eujournal.org/index.php/esj/article/viewFile/2941/2770

Kuehl, Daniel T. 2009 “From Cyber Space to Cyber Power: Defining the Problem.” In *Cyber Power and National Security*. Washington DC.: National Defense University Press.

Langner, R. (November 2013) “To Kill a Centrifuge” Retrieved on May 9th 2017 from http://bruteforcelab.com/wp-content/uploads/To-kill-a-centrifuge.pdf

Lendvay, R. (March 2016) “ Shadows of Stuxnet: Recommendations for U.S Policy on Critical Infrastructure Cyber Defense Derived from the Stuxnet Attack.” California Naval Post-Graduate School.

Michael N. Schmitt. “Computer Network Attack and the Use of Force in International Law” Research Publication 1 Information Series.

Shane M. Coughlan, (30 September 2003)“Is There a Common Understanding of What Constitutes CyberWarfare?” The University of Birmingham School of Politics and International Studies.

Strinde, Gabriel, Lund University, 2011. “Cyberwarfare: Connecting Classical Theory to a New Security Domain.” Peace and Conflict Studies.

Stucke, Kaisa, (June 23, 2015) “Cyber Attacks, Security, and Terrorism: Case Studies” Retrieved on April 29, 2017 from http://www.valuewalk.com/2015/06/cyber-attacks-security-and-terrorism-case-studies/?all=1

Villeneuve, N. and Crete-Nishita, M. “Control and Resistance: Attacks on Burmese Opposition Media” Retrieved on April 29, 2017 from http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-08.pdf

ONLINE SOURCES

“Cyber War: War In the Fifth Domain” 1 July 2010. The Economist.

“Duqu: A Stuxnet-like Malware Found in the Wild, Technical Report”. Laboratory of Cryptography of Systems Security (CrySyS).
“SkyWiper: A Complex Malware for Targeted Attacks”.31 May 2012. Budapest University of Technology and Economics.
“W32.Duqu – The Precursor to the Next Stuxnet (Version 1.4)”. Symantec Security Response Team. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

"What is a DDoS Attack?" Retrieved from http://www.digitalattackmap.com/understanding-ddos/

Bradley, Nicolas "Cyberterrorism is Real—is it? " Retrieved from http://www.lowlandssolutions.com/downloads/talent/Cyberterrorism%20-%20Nicholas%20Bradley.pdf

Christensson, P. (2006) "Malware Definition" Retrieved from https://techterms.com/definition/malware on April 23, 2017

Curran, Paul, (May 04, 2016) "Cyber Terrorism – How Real is the Threat?" Retrieved from https://www.checkmarx.com/2016/05/04/cyber-terrorism-real-threat-2/

Dinstein, Y. "Computer Network Attacks and Self-Defense" Retrieved on April 8, 2017 from https://www.usnwc.edu/getattachment/26796276-0919-4699-b2f0-5f15f46cb894/Computer-Network-Attacks-and-Self-Defense.aspx

Electronic Privacy Information Center. Epic.org "Presidential Directives and Cyber Security"

Falliere, N., O'Murchu, L., and Chien, E. (February 2011) "W32. Stuxnet Dossier" Retrieved on May 10 2017 from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Gordon, Sarah; Ford, Richard. "Cyberterrorism?" Retrieved from http://www.symantec.com/avcenter/reference/cyberterrorism.pdf .
Kushner, D. (February 26 2013) "The Real Story of Stuxnet". Retrieved on May 10, 2017 from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

M., Cereijo. May 16, 2006 "Cuba The Threat II: Cyberterrorism and Cyberwar"
Saputra, Y. M. "*Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare"* Retrieved from http://download.portalgaruda.org/article.php?article=349381&val=6444&title=P

ENGARUH%20CYBER%20SECURITY%20STRATEGY%20AMERIKA%20SERIKAT%20MENGHADAPI%20ANCAMAN%20CYBER%20WARFARE

OFFICIAL SOURCES

(February 12 2017) “The Ministry of Energy and Coal Industry Ukraine: *"Міненерговугілля має намір утворити групу за участю представників усіх енергетичних компаній, що входять до сфери управління Міністерства, для вивчення можливостей щодо запобігання несанкціонованому втручанню в роботу енергомереж”* Retrieved on April 30, 2017 from http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109

(November 8, 2010) Department of Defense Dictionary of Military and Associated Terms.”Joint Publication 01-02” Retrieved on April 23, 2017

(September 27 2016) “Cybersecurity Overview,” U.S. Department of Homeland Security, Retrieved on May 14 2017 from http://www.dhs.gov/cybersecurity-overview.

“Identification of a New Targeted Cyber-Attack.” Iran Computer Emergency Response Team. 28 May 2012.

April 12 2001. Joint Publication 1-02 DoD Dictionary of Military and Associated Terms. Retrieved on May 7, 2017 from http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%2801%29.pdf

Burton, J. (May 13 2015) “Cyber Warfare – A new Strategic Reality “ Retrieved on May 15 2017 from https://natlib.govt.nz/blog/posts/cyber-warfare-a-new-strategic-reality

Edward Snowden Foundation, November 23 2013, Worldwide SIGINT/Defense Cryptologic Platform, Retrieved on May 8 2017 from https://edwardsnowden.com/2013/11/23/worldwide-sigintdefense-cryptologic-platform/

February 13 2006. Joint Publication (JP) 3-13 Information Operations. Retrieved on April 23 2017 from http://www.information-retrieval.info/docs/jp3_13.pdf

GAO, February 2013, "Cyber Security: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." Retrieved from http://www.gao.gov/assets/660/652170.pdf

Geers, Kenneth. (August 27 2008) "Cyber Space and the Changing Nature of Warfare".Retrieved on May 7, 2017
from http://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf
Keith Stouffer, National Institute of Standards and Technology, 2014 "Guide to Industrial Control Systems Security."Retrieved
from http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

March 2006, "National Security Strategy of the United States of America." Retrieved on May 9 2017
from https://www.state.gov/documents/organization/64884.pdf
May 2013. DOD Directive No.3600.1, Information Operations. Retrieved on April 23,2017 from http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf

Obama, Barack, January 2012, "Sustaining U.S Global Leadership:Priorities for the 21st Century Defense."

October 20 2003. Department of Defense Information Operations Roadmap. Retrieved on May 2 2017
from http://nsarchive.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf
Presidential Policy Directive/PPD-20. Retrieved from https://fas.org/irp/offdocs/ppd/ppd-20.pdf

The Department of Defense Cyber Strategy, April 2005, Retrieved
from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

The DoD Cyber Strategy “Department of Defense Cyberspace Policy Report, November 2011.

Wilson, C. September 2006. “Information Operations and Cyberwar: Capabilities and Related Policy Issues.” CRS Report for Congress. Retrieved on May 8, 2017 from https://ipmall.law.unh.edu/sites/default/files/hosted_resources/crs/RL31787_060914.pdf