



**THE COMPETITION OF SHOWING ABILITY: THE
POTENTIAL DANGERS OF HACKER IN US CYBER
SECURITY (2009 – 2014)**

By

KRESNA ADITYA

016201500194

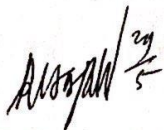
**A thesis presented to the Faculty of Humanities President University
In partial fulfilment of the requirements for Bachelor Degree in
International Relations Major in Diplomacy Studies**

2019

THESIS ADVISER RECOMMENDATION LETTER

This thesis entitled " **THE COMPETITION OF SHOWING ABILITY: THE POTENTIAL DANGERS OF HACKER IN US CYBER SECURITY (2009-2014)** " prepared and submitted by Kresna Aditya in partial fulfillment of the requirements for the degree of Bachelor of Arts 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, January 2019



Teuku Rezasyah, Ph.D

Thesis Adviser



Anggara Raharyo S.I.P., MPS


Thesis Adviser



DECLARATION OF ORIGINALITY

I declare that this thesis, entitled " **THE COMPETITION OF SHOWING ABILITY: THE POTENTIAL DANGERS OF HACKER IN US CYBER SECURITY (2009-2014)**" 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, January 2019

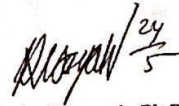


Kresna Aditya

PANEL OF EXAMINER

APPROVAL SHEET

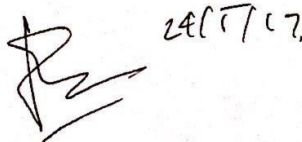
The panel of Examiners declare that the thesis entitled "The Competition of showing ability: The Potential Dangers of Hackers in US Cyber Security (2009-2014)" that was submitted by Kresna Aditya majoring in International Relations from the Faculty of Humanities was assessed and approved to have passed the Oral Examination on 6 February 2019.



Teuku Rezasyah, Ph.D
Chair – Panel of Examiners
Thesis Adviser I



Anggara Raharyo S.IP., MPS
Thesis Adviser II



Hendra Manurung, S.IP., MA.
Examiner I



ABSTRACT

The development of information technology has provided a significant shift from the concept of security. At present, a country is not limited to interact physically in real space but also extends to cyberspace. Consequently, the state must adapt to this development. Nowadays the concept of cyber security should be established as one of the "territory" of the state which should be safeguarded as the state's obligation to secure its borders. Now the interaction between the actors of international relations is not only in the land, sea and air. The interaction between the actors also performed in the virtual space into other options to achieve the interests. This study aimed to see the importance of cyber security strategies policy of the United States. Where the United States in the last 10 years is very intense spawned a cyber security strategy. This study uses qualitative research methods and use a secondary data to the problems studied. The results showed that the United States has put cyber security as one of four priorities in National Security. It is clearly mentioned in official documents and US security strategy. The United States realizes that it needs a comprehensive strategy to safeguard its national interests in the global world. Threats that come in massive threatening sovereignty of United States, requires the U.S government issued a policy to overcome this phenomenon, because of the threat of this kind can have an impact on many things, one of which impact on the economy, to deal with these problem the United States including establishing specific force and military equipment in order to reinforce the cyber security, and also issued direct instructions and orders from president to handle the cyber security issues.

Keywords: Cyber Strategy, Cyber Security, Cyber Warfare, National Interest, Policy, United States

ABSTRAK

Perkembangan teknologi informasi telah memberikan perubahan signifikan dari konsep keamanan. Saat ini, suatu negara tidak terbatas untuk berinteraksi secara fisik di ruang nyata tetapi juga meluas ke dunia maya. Akibatnya, negara harus beradaptasi dengan perkembangan ini. Saat ini konsep keamanan dunia maya harus ditetapkan sebagai salah satu "wilayah" negara yang harus dijaga sebagai kewajiban negara untuk mengamankan perbatasannya. Sekarang interaksi antara aktor hubungan internasional tidak hanya di darat, laut dan udara. Interaksi antara aktor juga dilakukan di ruang virtual ke dalam opsi lain untuk mencapai kepentingan. Penelitian ini bertujuan untuk melihat pentingnya kebijakan strategi keamanan cyber Amerika Serikat. Di mana Amerika Serikat dalam 10 tahun terakhir sangat intens melahirkan strategi keamanan siber. Penelitian ini menggunakan metode penelitian kuantitatif dan menggunakan data sekunder untuk masalah yang diteliti. Hasil penelitian menunjukkan bahwa Amerika Serikat telah menempatkan keamanan cyber sebagai salah satu dari empat prioritas dalam Keamanan Nasional. Ini jelas disebutkan dalam dokumen resmi dan strategi keamanan AS. Amerika Serikat menyadari bahwa diperlukan strategi komprehensif untuk melindungi kepentingan nasionalnya di dunia global. Ancaman yang datang secara besar-besaran mengancam kedaulatan Amerika Serikat, mengharuskan pemerintah AS mengeluarkan kebijakan untuk mengatasi fenomena ini, karena ancaman semacam ini dapat berdampak pada banyak hal, salah satunya berdampak pada ekonomi, untuk menghadapi hal tersebut. masalah Amerika Serikat termasuk membentuk pasukan khusus dan peralatan militer untuk memperkuat keamanan siber, dan juga mengeluarkan instruksi dan perintah langsung dari presiden untuk menangani masalah keamanan siber.

Kata kunci: Strategi Cyber, Keamanan Cyber, Warfare Cyber, Kepentingan Nasional, Kebijakan, Amerika Serikat

ACKNOWLEDGEMENT

First of all, I am very grateful for the gift that Allah ﷻ has given me. He has given a life full of precious values. Shalawat and Salam, I offer to the Prophet Muhammad ﷺ who taught all humans to have good morals through his words.

A very big thank you goes to my parent who have given their whole lives to their children. Their struggle behind the journey of my life is very important. For my mother Dini Berliana, I want to make my mom's proud to me. And also for my father Yusda Elfani, I want to prove that I will be the great man he wanted to. I also want to make him happy and give him the best of me, just as he did for me. You are great parents that I am very proud of.

Secondly, for my sister and brother, thank you for giving a best supports to me, thank you very much for the enthusiasm that you have given me. Thank you very much to my only great thesis advisor, Drs. Teuku Rezasyah, MA., Ph.D. and Mr. Anggara Raharyo, S.IP., MPS who has guided me very patiently and meticulously in the process of doing this thesis which even I do not have clear instructions, unless he who gave me direction.

Then I thank all the lecturers at President University who have given many lessons and helped me during my studies. Thanks to Mr. Bustanul Arifin, who was willing to provide valuable and important information related to the topic of the thesis that I wrote.

And further, I thank all my friends and close friends, Ryano Rahmanza, Imanael Sakti, Darma Putra Purba, Fauzan Nivo Erlangga, M. Fadhil Saminan, Ghifarie Aglis, Putri Syaiftia, Jeffira Ridhany, Frisca Nazhiera, Thristina Tiara Yusticia, Amsallah, Samuel Pintor Timothy and the others that I can't mention. Thank you for giving enthusiasm and motivation while I was in college, you are very valuable to me.

For the last, I thank all those who have helped me directly or indirectly. No matter how much your help, it is very valuable to me because we are social beings who live side by side and help each other. I hope all of us are always under Allah's protection.

Cikarang, January 2019

Table of Contents

THESIS ADVISER RECOMMENDATION LETTER.....	1
DECLARATION OF ORIGINALITY	Error! Bookmark not defined.
PANEL OF EXAMINER	Error! Bookmark not defined.
APPROVAL SHEET.....	Error! Bookmark not defined.
ABSTRACT	4
ABSTRAK.....	5
ACKNOWLEDGEMENT	6
Table of Contents.....	8
CHAPTER I.....	11
INTRODUCTION	11
1.1 Background of Study	11
1.2 Problem Identification	18
1.3 Statement of Problem	22
1.4 Research Objectives	22
1.5 Significance of Study.....	23
1.6 Literature Review	23
1.7.1 Time Span	27
1.7.2. Scope	27
1.7.3. Study Limitation.....	28
1.8 Theoretical Framework.....	28
1.8.1 Concept of Security Strategy.....	29
1.8.2 Policy Planning Process	31
1.8.3 Securitization Theory.....	32
1.8.4 Neorealism	34
1.9 Research Methodology & Thesis Structure	37
1.10 Thesis Structure.....	37
CHAPTER II.....	39
Literature Review.....	39

II.1 Understanding Cyber Space.....	42
II.1.1 Internet	44
II.1.2 Web Surface and Deep Web.....	45
II.2 Cyber Warfare.....	47
II.3 Cyber Security Challenges.....	50
II.3.1 Policy	51
II.3.2 The Process.....	51
II.3.3 Technique	52
II.3.4 Skill	53
II.3.5 Humans	53
II.3.6 Organizations.....	53
II.3.7 The Core of all challenges	54
II.4 Understanding Cyber Threats through Threat Models	54
CHAPTER III.....	57
Cyber Security in the United States Security System.....	57
III.1 The Nature of Global Cyber Security Competition.....	61
III.2 The Significant of Cyber Security Strategy.....	63
III.2.1 Cyberspace Policy Review.....	64
III.2.2 International Strategy for Cyberspace.....	66
III.2.3 Presidential Proclamation - National Cybersecurity Awareness Month, 2014 ...	70
III.3 United States Executive Orders Agenda	71
III.3.1 Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information	72
III.3.2 Executive Order 13636 - Improving Critical Infrastructure Cyber Security	73
III.4 The United States Cyber Security Strategy Implementation	74
III.5 The Structure of Role Model Cyber Security Agencies in the United States Administration	75
III.5.1 Department of Defense as the Strategic Level Agency.....	75
III.5.2 US Strategic Command (USSTRATCOM) as an Operational Level Agency	76

III.5.3 US Cyber Command (USCYBERCOM) as a Military Cyber Defense Agency .	77
III.5.4 National Security Agency (NSA) as the Protector of Vital Information and Infrastructure.....	78
CHAPTER IV.....	79
The Nature of Cyber Security Attack and United States Responses.....	79
IV.1 Cyber Security and United States-China Relations	79
IV.2 Cyber Security and United States-Russia Relations	86
CHAPTER V.....	91
Conclusion	91
Bibliography.....	94
Appendix:	99

CHAPTER I

INTRODUCTION

1.1 Background of Study

Internet usage has been highly increased since the development of the technology era. All of the technology systems are connected to the Internet. The internet has brought a fundamental change by the engagement of nations and their citizens in global economic activity, manage critical infrastructure, and communicate with one and another. The hyper-connectivity of the modern world brings a wealth of benefits for governments, enterprises, and individuals in that the information exchange is no longer dependent on physical constraints and is available immediately regardless of the distance.¹

Hackers become easier conducting criminal activity on the Cyber Space until pointing to the more serious activities like theft the secret nation's primary data and theft the nation's infrastructures. The United States potentially adversaries may seek to exploit, disrupt, deny, and degrade the networks and systems. It threatens the United States personal, financial data, and leads the nation's economic stability and prosperity.² Without strong investments in Cyber Security and Cyber Defenses data systems are remain open tend to rudimentary and dangerous forms of exploitation attack. Malicious actors use Cyber Space to steal data and intellectual property for economic and political goals, an actor in one region of the globe can use cyber capabilities to strike directly at a network within a thousand of miles range away, destroying any data, disrupting businesses, or shutting off critical infrastructures systems. State and non-state actors conduct cyber operations to achieve a variety of

¹ Klaus Schwab, *The Fourth Industrial Revolution 2016 Chapter 3.3.3 International Security. World Economic Forum*® Page 77.

² Isle of Man, *National Cyber Security Strategy 2018-2022*. GD 2018/0029. Page 0008.

political, economic, or military objectives, they may strike at a nation's values as well as its interests or purposes.³

Cyber Space has become a way in order to achieve certain interest which also known as Cyber Power.⁴ The Connectivity has fundamentally advanced the way people to travel, communicate and also conducting a business.⁵ Convenience is a just one click away. News, ideas and information buzz around the globe has become easily to access. Networks store a whole host of information. From medical and financial records, personnel employment data, private records, tax information, school records, Social Security numbers, to government data, the list goes on about the sensitive data stored on networks. Connectivity furthers the nation forward.⁶ The United States is committed to an open, secure, interoperable, and reliable the Internet have enables prosperity, public safety, and the free flow of commerce and ideas.⁷ These qualities of the Internet have reflected a core of American values which are freedom of expression and privacy, creativity, opportunity, and innovation. These qualities have allowed the Internet to provide a social and economic value to a billion people.⁸

The United States is one of the major countries that have the capability to utilize the internet in daily life and in the state. The internet has been ingrained for an

³ US Department of Defense. *The Department of Defense Cyber Strategy*, April 2015.

⁴ David J. Betz and Tim Stevens. *Cyberspace and the State, Toward a strategy for cyber-power*. https://assemblingsecurity.files.wordpress.com/2013/05/betz_stevens_cyberspace-and-the-state-2011.pdf

⁵ Zaryn Dentzel. *How the Internet has changed everyday life*. <https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/>

⁶ Darrell M. West. *Technology and the Innovation Economy*. October 19, 2011. <https://www.brookings.edu/research/technology-and-the-innovation-economy/>

⁷ Department of Defense. *DoD Cyber Strategy (April 2015)*. 2015. <https://www.hsdl.org/?abstract&did=764848>

⁸ Daniel Rostrup. *Applying Connectivity to deliver the United States sustainable development goals*. 24 October 2018. <https://www.avantiplc.com/blog/applying-connectivity-to-deliver-the-unsustainable-development-goals/>

American⁹; every sector both from a small sector to vital infrastructure has relied heavily on this network-based technology. This dependence on massive network technology certainly has a few drawbacks caused by the vulnerability of cyberspace and at any time can be infiltrated by other parties both individually in the country. This will be a threat to the United States cybersecurity because confidential data and information stored digitally can be stolen, spying, destroyed or changed by other parties. Digital attacks will also be widespread and blatant if cybersecurity is not properly addressed and will lead United States to cyber war that will threaten the vital sector, infrastructure, and US sovereignty. Moreover, the Internet will lead to an exponential number of devices being connected to the network. As a result, the economic and political incentives to exploit the network for malicious purposes have expanded, and cybersecurity has become to head-of-state-level consideration¹⁰. In parallel, publications on the topic by academic, policy, industry, and military institutions have multiplied.

Scholars within the International Relations (IR) discipline and its subfields of security studies and strategic studies increasingly focus on the technology's implications on national and international security. This includes studying its effect on related concepts such as power, sovereignty, global governance, and securitization. Meanwhile, the meaning of cybersecurity has been highly contested. From the common to the phenomenal, networks and connectivity is a significant part that US necessity in order to develop the United States power. The great domains are land, sea, air, space and now cyberspace. Cybersecurity has become a topic of concern over the past decade as private industries, public administration, commerce, and communication have gained a greater online presence.

⁹ Polaris. *Cyberspace as American Culture*. <http://polaris.gseis.ucla.edu/pagre/sac.html>

¹⁰ Hannes Ebert & Tim Maurer. *Cyber Security*. January 2017. DOI: 10.1093/OBO/9780199743292-0196 <HTTP://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0196.xml>

The US Cybersecurity Policies and Strategies for Cyberwarfare Prevention serve as an integral publication on the latest legal and defensive measures being implemented to protect US infrastructure and another secret governance data from cyber threats¹¹. In the information age, the state (or non-state) of the ruling country is no longer a country that has a strong military force, but also a country that has the best narrative. It is difficult to measure the balance of power, especially how successful a survival strategy is. The States will remain the main actor on the world stage. However, the country will get a stage that is more crowded and difficult to control.

*According to the United Nations, cybercrime is an enterprise that exceeds a trillion dollars a year in online fraud, identifies theft and lost the intellectual property. The crime affects millions of people around the world, as well as businesses and governments worldwide.*¹²

However, it is unavoidable that the rate of development of the Internet is also widely used for various counter-productive, even destructive goals, either by non-state actors, groups, and state actors. They exploit information to spread their influence and dominance in information warfare (Information Warfare / Cyber Warfare). In the currently cyber era, the mastery and use of the destructive Internet are basically also a threat to national security. The inability to face the cyber era can be a threat if a nation and state do not have the capability or ability to utilize the Internet properly, correctly and effectively. As a result, cyber security and cyber defense are needed in a country. Cyber Security has different from ordinary security because cyber threats cannot simply be entered into traditional security categories.¹³ In addition to originating from within the country, Cyber Threats also come from

¹¹ White House. *National Cyber Strategy*. 2018. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

¹² United Nations. 2016. *Cybersecurity Demands Global Approach*. <http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demandsglobal-approach.html>

¹³ Wallace, I. 2013. *The Military Role In National Cybersecurity Governance*. Brookings. <http://www.brookings.edu/research/opinions/2013/12/16-military-role-national-cybersecurity-governance-wallace>

abroad. However, this threat rarely reaches the level that requires a military response because whatever the government will do in response to this cyber threat will have domestic and international implications.

The earnestness of the United States in defying this cyber-attack can be seen with the issuance of US International policy details for cyberspace. The point by point and complete arrangement of how US strategies deal with different cases concerning cyberspace. Various policies of arrangement in the face of threats that come from cyberspace including:

1. The National Strategy to Secure Cyberspace, issued in February 2003.
2. Cyberspace Policy Review, issued in 2009.
3. International Strategy for Cyberspace, issued in May 2011.
4. Department of Defense Strategy for Operating in Cyberspace, issued in July 2011.

A number of strategy formulations for cybersecurity were made by the US not without cause. A number of good events that directly hit the US and that did not directly affect the US affected the birth of the cybersecurity strategy. These event is enough to widely open the eyes of the world, including the US itself, that cyber threat is not only a discourse anymore; it even demands military handling for countermeasures.

The Chinese military hacked into a Pentagon computer network in June in the most successful cyber attack on the US defense department, say American -officials.¹⁴

Not only the state, a number of private companies such as Multinational companies, including US property, also do not escape from cyber-attacks. Google and Adobe system were recorded as victims of the operation Aurora in 2009. In 2010, the attack on the Stuxnet malware virus also became a global conversation

¹⁴ Demetri Sevastopulo in Washington September 4, 2007. *Chinese hacked into Pentagon*. *Financial Times*. <https://www.ft.com/content/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac>

because it was able to knock out the Bushehr power plant. Stuxnet was a malicious computer worm that had used to attacks Iran's SCADA (Supervisory control and data acquisition) system and causing substantial damage to Iran's nuclear program. SCADA is system software and hardware element that are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime.¹⁵ Stuxnet was the first cyber weapon that could destroy a real-world target. Stuxnet working to manipulated system software, that makes human operator thought everything was running fine, while it destroyed the uranium, enrichment, and centrifuges. Living on the era of a new arms race where a malicious piece of 'code' can threaten an untold number of human lives. The US is also often reported to experience a fairly threatening cyber-attack national interests and security.

The dangers of cyber threat can be seen through cyber-attack events that had occurred in Ukraine in **2015** which has cut power 200,000 residents for several hours.¹⁶ If a major US region was left without power, it is certain that it will turn off everything from water filtration systems to aviation safety software such as a large-scale power outage with severely crippled law enforcement, banking, and life-saving services. Malware implants can attack computer systems in the simplest of ways. Servers can be forced to record unnecessary data. Malware causes all the free memory to be used for accelerated rates, ultimately leading to a system crash which causes military and civilian networks to be brought down this way.

¹⁵ SCADA's Official website. *What is SCADA*.

<https://inductiveautomation.com/resources/article/what-is-scada>

¹⁶ Takepart journalism observation. *Here's what a Cyber Attack would like in America*. August 23, 2016. <https://www.youtube.com/watch?v=ZkoenqCGiOs>

Nitro Zeus is a cyber weapon developed by the Defense Department was created to break the havoc on the country's infrastructure.¹⁷ This weapon can shut down communication systems, power grids and water defenses without the use of bombs or bullets. As with the nuclear arms race, cyber warfare is immense. Despite this malware is highly secretive practice, there has been a little dialogue or international diplomacy aimed at governing the use of cyber weapons. During the Stuxnet attack, the viruses were escaped on computers worldwide and left the blueprint for creating Stuxnet like Cyber weapons to everyone.¹⁸

President Barack Obama and administration officials have expressed concern about troubling activity by adversaries, including those who have breached US nation's critical infrastructure. The threat that against US networks is a constant. Officials have mentioned the names are China, Russia, Iran, and North Korea as nation states that have infiltrated US cyber targets. Many experts have warned the possibility of a major cyber-attack. The consequences could be dire if a rogue nation or cyber terrorists struck US critical infrastructure. In an executive order addressing the dangers and vulnerabilities in cybersecurity, President Obama declared a "national emergency to deal with this threat".¹⁹ China and Russia are the countries are most often accused by the US of espionage and even hacking into information systems both government infrastructure and private companies.

¹⁷ Langner. *When will we see Stuxnet & Nitro Zeus attack against Iran*. October 8, 2018. <https://www.langner.com/2018/10/when-will-we-see-another-stuxnet-nitro-zeus-attack-against-iran/>

¹⁸ George Aquila. *The Stuxnet Worm - The Nexus of Cyber Security and International Policy*. <http://www.cs.tufts.edu/comp/116/archive/fall2013/gaquila.pdf>

¹⁹ Hirschfeld, Julie Davis, and David Sanger. Obama and Xi Jinping of China Agree to Steps on Cybertheft. The New York Times. September 25, 2015. <http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-whitehouse.html? r=0>

1.2 Problem Identification

According to the background of the problem, the author will explain the problem has found that the United States is intimately interwoven in the cyberspace which all the technology that the United States had have dependent to the cyberspace. Since the United States and companies rely on Cyber Space for everything from financial transactions to the movement of military forces. The examples are from the everyday social interactions to the banking and financial industries, to the critical infrastructure on which the nation relies, and to the sophisticated national security apparatus that protects the nation. Even those who are not connected could still feel the impacts of cybercrime, including through increased costs, or if their personal information gets stolen, or if terrorists struck the nation's critical infrastructure. Therefore, the United States gains tremendous economic, social, and military advantages from cyberspace. However, the United States pursuit of these advantages has created extensive dependencies on highly vulnerable information technologies and industrial control systems. As a result, US national security is at an unacceptable and growing risk.

According to the 2015 (ISC) Global Information Security Workforce Study (GISWS), 60 percent of the over 1,800 US federal government respondents say that they do not have enough information security personnel to meet the demands of their mission; a 2 percent increase over the 2013 survey findings.²⁰

This personnel shortage is especially alarming considering the daily barrage of attacks against DoD networks. Eric Rosenbach, who serves as the Principal Cyber Advisor to the Secretary of Defense, recently testified before the US Senate Committee on Armed Services on this topic.

²⁰ U.S. Department of Defense Cyber Strategy: One of five strategic goals to building and maintaining the Cyber Workforce http://blog.isc2.org/isc2_blog/2015/05/us-department-of-defense-cyber-strategy-one-of-five-strategic-goals-to-building-and-maintaining-the.html

“External actors probe and scan DoD networks for vulnerabilities millions of times each day, and over one hundred foreign intelligence agencies continually attempt to infiltrate DoD networks. Unfortunately, some incursions – by both state and non-state entities – have succeeded,” said Rosenbach.²¹

Bases on Director of National Intelligence (DNI) research, the author will underline that the United States has been subjected to cyber-attacks and costly cyber intrusions by various actors, including most cyber capable adversary states that have identified.²²

For example:

- During 2012–2013, Iran conducted distributed denial of services attacks on Wall Street firms, disrupting operations and imposing tens of millions of dollars in remediation and cyber hardening costs.²³
- In 2014, North Korea hacked Sony Pictures in an effort to suppress the release of a movie depicting a plot to assassinate North Korean leader Kim Jong Un, causing direct and indirect financial damage in the process.²⁴
- For at least 10 years,²⁵ China conducted a massive cyber theft of U.S. firms’ intellectual property (IP); since President Xi Jinping committed in September 2015 that China would not undertake such theft; reportedly Chinese cyber IP theft has reduced but not stopped.

²¹ Statement for the Record, The Honorable Eric Rosenbach. Assistant Secretary for Homeland Defense and Global Security and Principal Cyber Advisor to the Secretary of Defense, U.S. Department of Defense.

²² The Honorable James R. Clapper, Director of National Intelligence. *Senate Select Committee on Intelligence – IC’s Worldwide Threat Assessment Opening Statement*. February 9, 2016. https://www.dni.gov/files/documents/2016-02-09SASC_open_threat_hearing_transcript.pdf

²³ Department of Justice press release “*Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector*”. 24 March 2016. <https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged>

²⁴ U.S. Department of State. *The North Korean Threat: Nuclear, Missiles and Cyber*. 13 January 2015. testimony before the House Foreign. <https://www.state.gov/p/eap/rls/rm/2015/01/235888.html> Affairs Committee by the Special Representative for North Korea Policy

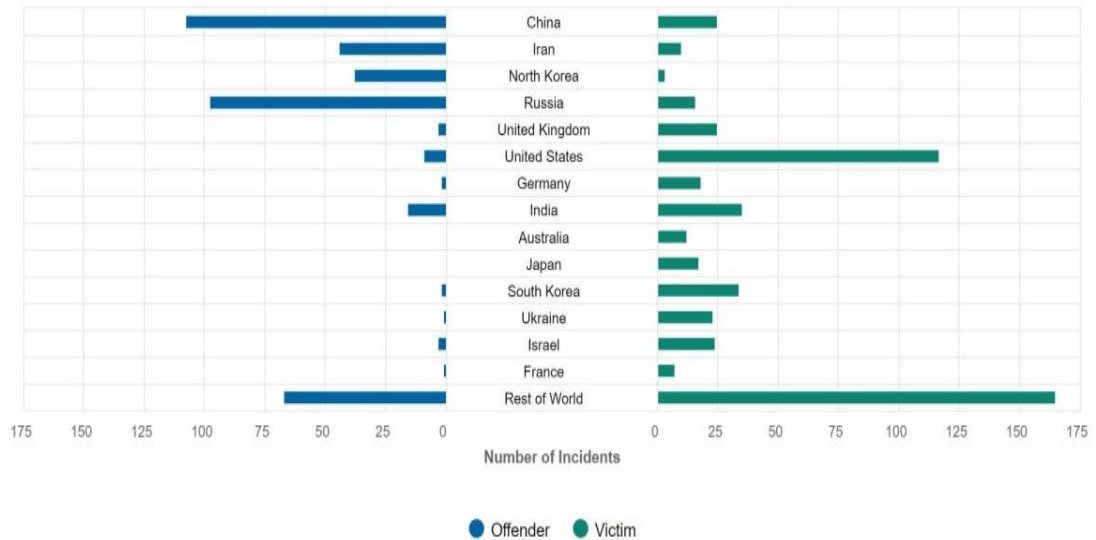
²⁵ Director of National Intelligence. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07*. Additional reports are located at the website of the National Counterintelligence and Security Center.

Each of the above examples stands out from the constant barrage of cyber intrusions that occur in the United States and globally on a daily basis, including those conducted by nations as part of their cyber espionage programs. Such actions qualify as cyber attacks (Iran’s Distributed Denial-of-Service Attack (DDoS) and North Korea’s Sony hack) or costly cyber intrusions (China’s intellectual property (IP) theft and Russia’s hack of political parties to facilitate information operations) because their impact goes beyond data collection, to impose some form of harm on the United States. Of critical importance, known cyber-attacks on the United States to date do not represent the “high-end” threats that could be conducted by U.S. adversaries today – let alone the much more daunting threats of cyber-attack the Nation will face in coming years as adversary capabilities continue to grow rapidly. A large-scale cyber-attack on civilian critical infrastructure could cause chaos by disrupting the flow of electricity, money, communications, fuel, and water.

The arrival of the digital age has also created challenges for the Department of Defense (DoD) and the Nation. The open, transnational, and decentralized nature of the Internet that seeks to protect creates significant vulnerabilities. Competitors deterred from engaging the United States and allies in an armed conflict are using cyberspace operations to steal US technology, disrupt US government and commerce, challenge US democratic processes, and threaten the US critical infrastructure.

Significant Cyber Incidents

Based on publicly available information on cyber espionage and cyber warfare, excluding cybercrime. Long-running espionage campaigns were treated as single events for the purposes of incident totals. Tallies are partial as some states conceal incidents while others fail to detect them.



CSIS Technology Policy Program | Source: CSIS & Hackmageddon

Figure 1. Timeline records significant cyber incidents since 2006.

Source : <https://csis-ilab.github.io/js-viz/tech-policy/cyber-incidents-bar/index.html> accessed on 18 November 2018.

From figure 1 of the Center for Strategic & International Studies (CSIS) data, United States has become a victim of Cyber Attacks which has mostly attackers and hackers. This data was focusing on cyber attacks on government agencies, defense, and high tech companies, or economic crimes with losses of more than a million dollars. The United States was engaged in long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose a long-term strategic risk to the Nation as well as to the US allies and partners. China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltration sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence the United States population and challenge the democratic processes.

Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm the US citizens and threaten US interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every essential civilian and military function makes this an urgent and unacceptable risk to the Nation. The Department must take action in cyberspace during the day-to-day competition to preserve U.S. military advantages and to defend US interests. The author will be focusing on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia.

1.3 Statement of Problem

Topic: The Implement of US Cyber Security Strategy in facing Cyber Warfare from 2009 – 2014.

Research Question:

How did the United States implement their Cyber Security Strategy in 2009-2014?

1.4 Research Objectives

The objective of this research is to describe analytically from the current issue using scientific methods. In accordance with the explanation above, this research objective is to find out and analyze about how Cyber Security becomes one of four National security priorities of threat for the United States and the implement of US Cyber Security Strategy, based on available official data, statement, statistic, report and journal regarding to the topic and writer analysis.

1.5 Significance of Study

This research is meant to give valuable knowledge, information, and problem solution to the reader, about US Cybersecurity strategy on facing a Cyber Space. The significant of study is providing analysis and data for the reader related to the research is done to describe and analyze how Cybersecurity becomes National security priority of US Government. Afterward, how the US facing incoming threats from another States or even a terrorist attacks thru the cyberspace. Therefore, through this research, the writer's will able to give information about the strategy of US government (Department Of Defense and Department of Homeland Security), and US Military (US Cyber Command) in facing incoming threats from another States or even a Terrorist attacks thru the cyberspace (Cyber Terrorism).

Thereafter, the writer will be able to implement the theory, concept, and knowledge in International Relations, which has been learning in President University. This research also gives the experience to the writer in order to write the research and to get deeper knowledge.

1.6 Literature Review

A literature review is a list of references from all kinds of references such as books, journal papers, articles, dissertations, theses, thesis, hand-outs, laboratory manuals, and other scholarly works cited in proposal writing.

1. The Basics of Cyber Warfare, Understanding the Fundamentals of Cyber Warfare in Theory and Practice

This book has made by Steve Winterfeld and Jason Andress, published in 2011 in the United States. The book is designed an introduction to the strategic, operational, and tactical aspects of the conflicts in cyberspace. This book was increasing the author knowledge according to how big Cyber Attack could affect the Nation's Security in a higher level of view material in

Cyber Warfare techniques, tactics, and tools for security practitioners. The book shares two very different perspectives of the two authors on what many are calling cyber warfare today. One comes from a commercial background and the other brings the military viewpoint. The book is designed for explaining the essentials of what is happening today, as well as provide a strong background on the issues we are facing. The unique in the books is provides the information in a manner that can be used to establish a strategic cybersecurity vision for an organization but it is also designed to contribute to the national debate on where cyber is going.²⁶

2. The United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?

The thesis that has made by Lieutenant Commander William K. Tirrell, USN, The George Washington University, Fort Leavenworth, Kansas, December 2012. A thesis presented to the Faculty of the US Army Command and General Staff College. Through an exhaustive review of recurring and stand-alone strategic cybersecurity strategy and policy documents and a detailed assessment of the United States cyber organization within the Department of Homeland Security, Department of Defense, and Department of Justice, the United States is indeed vulnerable to a cyber attack.

Despite the recent emphasis on cyber-attacks against private and governmental organizations, the genesis of American interest and awareness of cyber threats began during the Clinton Administration. While progress has been made on many fronts, cybersecurity strategy, policy, and organization

²⁶ Steve Winterfeld and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. ISBN-13: 978-0124047372 ISBN-10: 0124047378. 2011. <https://www.amazon.com/Basics-Cyber-Warfare-Understanding-Fundamentals/dp/0124047378>

have not incorporated some of the lessons the Intelligence Community learned from the 9/11 experience. Because of this shortfall, the United States is potentially vulnerable to a devastating cyber-attack.²⁷

3. Internet Security Threat Report (ISTR)

The book by Symantec has convened a working group on Cyber Security. Symantec has established the most comprehensive source of Internet threat data in the world through the Symantec Global Intelligence Network. This book has much attention focused on cyber-espionage, threats to privacy and the acts of malicious insiders in 2013. However, the end of 2013 provided a painful reminder that cybercrime remains prevalent and that damaging threats from cybercriminals continue to loom over businesses and consumers. Eight breaches in 2013 each exposed greater than 10 million identities, targeted attacks increased and end-user attitudes towards social media and mobile devices resulted in wild scams and laid a foundation for major problems for end users and businesses as these devices come to dominate people lives. ISTR once again covers the wide-ranging threat landscape, with data collected and analyzed by Symantec's security experts.

4. Handbook of System Safety and Security Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber-Physical Systems

This book has made by Edward Griffor, National Institute of Standards and Technology (NIST) the United States, 2017. The book was explaining how the system and the concept of the system working, including

²⁷ U.S. Army Command and General Staff College. *United States Cyber security Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?*. ISBN:1500750247 9781500750244. USA, 2014. <https://dl.acm.org/citation.cfm?id=2692572>

Cyber-Physical Systems / CPS, commonly known as the Internet of Things. CPS are systems that include both logical operations (such as control and feedback) and physical interactions (such as gathering information from the physical realm using sensors or actuating or taking an action that impacts the physical realm). Also discussing the perspectives on Safety and Security when faced with constantly changing conditions under which a system must continue to deliver its function, the author's attempt to model those conditions and test their design against the model. In order to assess systems and determine their overall risk, their overall security posture, design countermeasures, and then re-assess systems to determine the effectiveness of countermeasures in a provable, reproducible, repeatable quantitative manner, we must be able to model the security, vulnerability, and risk of these systems. In this chapter, the authors introduce new modes of modeling for security adversaries and discuss some basic foundations for adversary modeling. The book has also discussed how the connectivity of systems increases the complexity of system interactions. These complexities also need to be identified and modeled to understand the derivative effect on the overall security posture.²⁸

5. Developing a National Strategy for Cybersecurity. Foundations for Security, Growth, and Innovation

This Microsoft Corporation's journal delivering the vulnerabilities of legal framework cybersecurity regulation of any governments around the world including the US Government, by Cristin Flynn Goodwin and J. Paul Nicholas, October 2013. Its Microsoft's view that such a framework should

²⁸ Edward Griffor. *Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems*. ISBN-13: 978-0128037737 ISBN-10: 0128037733. <https://www.amazon.com/Handbook-System-Safety-Security-Management/dp/0128037733>

be based upon a principled national strategy that sets a clear direction to establish and improve cybersecurity for the government, academics, enterprises, consumers, and the ICT companies who serve those communities. Microsoft strongly supports governments taking steps to protect their most essential information and ICT systems which those needed to support national security, the economy, and public safety.

A national cybersecurity strategy is critical for managing national-level cyber risks and developing appropriate legislation or regulation to support those efforts. As a global software company, Microsoft has observed dozens of national approaches aimed at addressing cyber risk and has developed views about what makes for an effective national cybersecurity strategy. This document contains recommendations for policymakers for developing or improving a national security strategy.²⁹

1.7 Scope and limitation of the study

1.7.1 Time Span

This research will describe five years range for this research, starting from the establishment of Cyber Policy Review 2009 and International Cyber Strategies for Operating in Cyberspace in 2011 under the Barack Obama's presidential periods; will mark the limitation of the time frame of this research.

1.7.2. Scope

This research made to discuss US Cyber Security in facing incoming threats from another States or even terrorist attacks thru the cyberspace. Focusing on the United States confronting Cyber-attack challenges from another States under the United States Department of Defense (DoD) and the Military agencies.

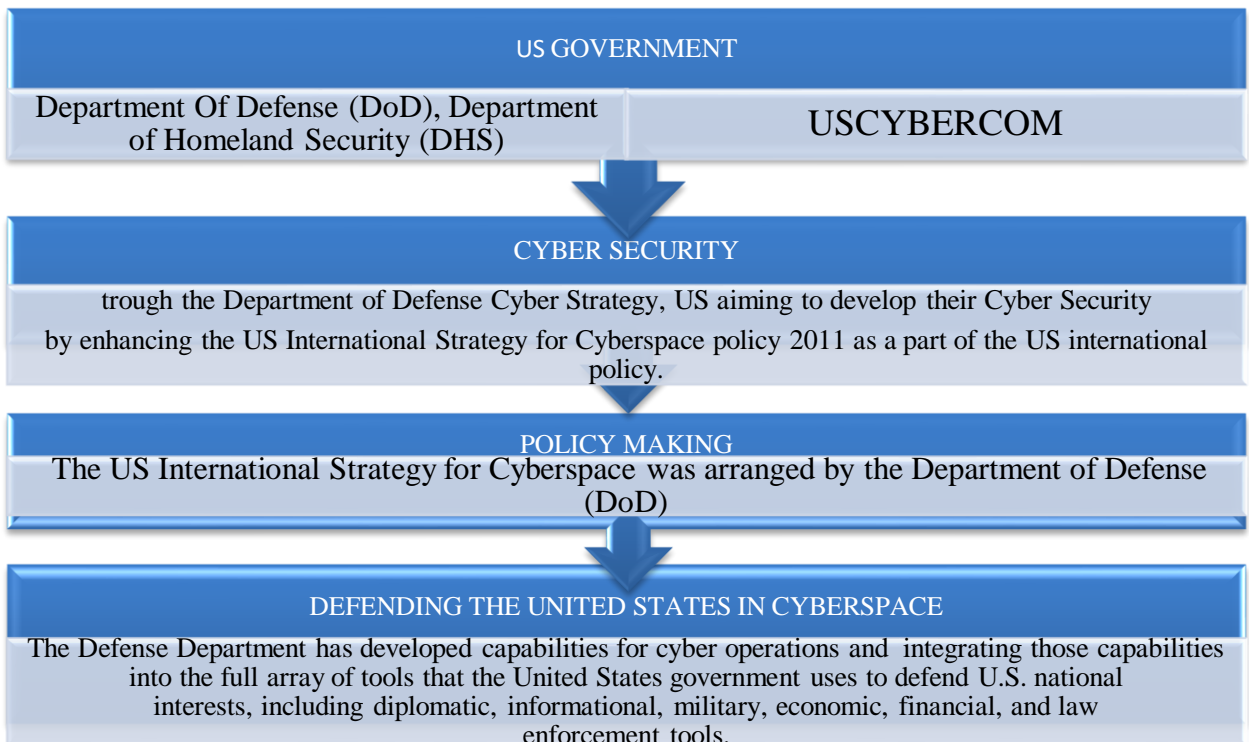
²⁹ Cristin Flynn Goodwin and J. Paul Nicholas. *Developing a National Strategy for Cybersecurity*, Foundation for Security, Growth, and Innovation. October 2013.
http://download.microsoft.com/download/b/f/0/bf05da49-7127-4c05-bfe8-0063dab88f72/developing_a_national_strategy_for_cybersecurity.pdf

1.7.3. Study Limitation

This research will focus on the strategy of the US Government and Military in facing incoming threats from another States or even a terrorist attacks thru the cyberspace and the implement of US Cybersecurity strategy.

1.8 Theoretical Framework

In order to explain how the US government effort in making a cyber-security strategy does become a National security priority of the US government, the author has made the chart as presented below:



The framework of this research will put the focus on the efforts of the US Government in developing their cybersecurity using cybersecurity framework by implementing International Strategy for Cyberspace that arranged by the US Department of Defense (DoD).

1.8.1 Concept of Security Strategy

International security assessments have experienced significant developments. Understanding the concept of security after the cold war is no longer narrow as a relationship of conflict or cooperation between countries, but also centered on security for society.³⁰ Arnold Wolfers in Perwita & Yani defines security as follows,

"Security, in any objective sense, measures the absence of acquired values and in a subjective sense, the absence of fear that such values will be tacked".³¹

Steven Spiegel and Winarno said that the expansion of the definition of national security has the consequence of increasing threats: nuclear, economic, social and cultural. The concept of security can be described as follows:³²

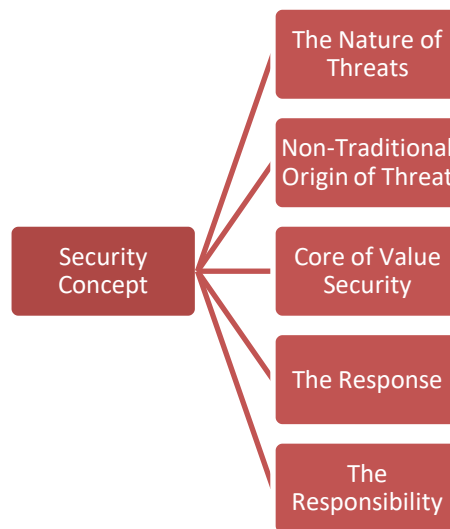


Figure 2 Security Concept

Source: *Concept of Security Threats, Challenges, Vulnerabilities*

https://www.springer.com/cda/content/document/cda_downloaddocument/9783642177750-c1.pdf?SGWID=0-0-45-1068963-p174086661

³⁰ Perwita, Anak Agung Banyu & Yani, Yanyan A. *Pengantar Ilmu Hubungan Internasional*. 2005. Page 119.

³¹ Ibid. Page 121.

³² Sujarweni, V. Wiratna. *Metode Penelitian: Lengkap, Praktis, dan Mudah Dipahami*. 2014. Page 10.

From Figure 2 above shows that if viewed from the dimensions of the origin of threats, the threat can come from domestic such are primordial issues related to race, ethnicity, group, and religion. Threats can also come from the global environment, carried out by state and non-state actors. The next dimension is Nature of threats if the threat to traditional security is military. But along with the development of the era of threat, it becomes much more complicated not only military in nature, but also a threat that is non-military in nature, or related to aspects of the economy, social culture, environment, human rights, and other more comprehensive security issues.³³ Meanwhile, Strategy by John P. Lovell³⁴ is interpreted as "a series of steps or decisions that were designed beforehand in a competitive situation where the end result is not mere chance. The strategy is a method used to achieve a goal or interest by using available power, including military force. In foreign policy, the strategy is a pattern of planning used by decision-makers to advance and achieve their national interests accompanied by efforts to prevent other countries from colliding or hindering the achievement of that interest.

There are three assumptions from strategy theory:³⁵

1. The foreign policy behavior of a nation-state must be directed as a step to achieve one or several objectives of that interest.
2. A decision makers always try to maximize the acquisition of their countries by examining various alternative actions, each of which is assessed based on cost and outcome analysis.
3. In this world interdependent so that decisions must take into account the goals and strategies of other nation-states.

³³ Winarno, Budi. *Dinamika Isu-isu Global Kontemporer*. 2014. Page 11.

³⁴ Mas'oeed, Mochtar. *Studi Hubungan Internasional, Tingkat Analisis dan Teorisasi*. 1989. Page 90

³⁵ Ibid. Page 90-91

1.8.2 Policy Planning Process

The policy planning process is preceded by analytical and/or political activities (analysis, generation of options, bargaining, etc.) and followed by equally important planning activities (implementation, assessment, and possible redesign). Policy analyses are a welcome addition to the physical therapy literature. Such analyses are critical to advance the understanding of the impact of various federal, state, local, and organizational policies on the provision of physical therapist services across the continuum of care and to advance the profession's various policy agendas. The translation and application of the rich and extensive literature on theories of policy-making and methods for policy analysis to physical therapy are still in its infancy. At the same time, the evaluation of policy implementation, the development of systems models to explain the multiple factors that influence policy-making and the advancement of knowledge within specific policy areas are redefining the field of policy analysis.³⁶

Although consensus regarding best practice remains elusive, there appears to be little disagreement that policy analysis is complex. Moreover, there is growing recognition that analytical approaches are situational and require an understanding of the context within which the analysis is conducted. The closer move towards concrete cybersecurity issues, the more shown that the specific roles of various actors and the need for a multistakeholder approach. Any of the actors itself – including the most powerful states – cannot ensure Internet security without the broader participation of many: from individuals to corporations. On the decision-making level, governments need to be able to decide on policies and share operational resources and also defend themselves (and even attack) – in accordance with international law. Nevertheless, they also have a responsibility not to militarise

³⁶ Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 30, <http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf>

cyberspace by cyber-armament and exclusive policies. Instead, they need to create inclusive policy-shaping environments that define the roles and the responsibilities of other stakeholders and enable them to perform their perspective roles.

Government actions: Support inclusive multistakeholder policy processes, invest in evidence-based policymaking, raise general awareness, and build capacity.

1.8.3 Securitization Theory

In security discourse, an issue is dramatized and presented as an issue of supreme priority; thus, by labeling it as security, an agent claims a need for and a right to treat it by extraordinary means. For the analyst to grasp this act, the task is not to assess some objective threats that ‘really’ endanger some object to be defended or secured; rather, it is to understand the processes of constructing a shared understanding of what is to be considered and collectively responded to as a threat. The securitization approach serves to underline the responsibility of talking security, the responsibility of actors as well as analysts who choose to frame an issue as a security issue. They cannot hide behind the claim that anything in itself constitutes a security issue.³⁷

‘Security’ can be framed in other ways than the specific frame implied by securitization. The Copenhagen school assumes that the connotations of security are givens (existential threats requiring emergency measures) and that only the threats and the core values of security are variables. There are indeed cases in which threat framing has exactly these consequences, especially when issues are perceived as threats implying hostility and antagonism. Theoretically, however, there is a reason to expand the conception of possible connotations beyond the negative and limited ones associated with securitization. The need for doing so is evidenced by the political success of alternative concepts like ‘common security’ and ‘cooperative

³⁷ Barry Buzan, Ole Wæver and Jaap De Wilde *Security A New Framework For Analysis* Lynne Rienner. 1998. <http://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0091.xml>

security’.³⁸ Not all threat frames fall into the life-and-death category of existential threats, and extraordinary ‘hard power’ measures that sidestep democratic procedures are not always legitimized by a certain threat frame.³⁹

More specifically, this framework focuses on frame characteristics, framing actors, and contextual conditions. For each of these aspects, that is concerned with patterns of continuity and change. Frame characteristics concern what is considered a threat, what is considered to be threatened (core values and referent objects), and what connotations are implied by both of these aspects. A threat frame, like any frame, can be restricted as well as elaborated (Snow and Benford 1992), specific and diffuse, and be about antagonistic actors, structural problems, or particular events (Eriksson 2001b). It can be expected that the securitization hypothesis about legitimating extraordinary measures is more likely to be valid when an antagonistic threat is identified than when a threat is characterized as a structural problem. Feelings of fear are greater when we perceive that someone intentionally wants to harm us, in comparison with threats associated with structural conditions or accidents (Dewey 1929; Johnson 1997). This is probably an important reason why war and terrorism gain such prominent positions on the policy agenda, although health problems and traffic accidents kill more people. Yet even fearing the unknown is about some imagined danger, though in this case, it is the very diffuse or unspecific nature of this that produces the sense of threat (Dewey 1929; Johnson 1997). If we are not certain about the ways in which a newly discovered pandemic is transmitted, then panic is not far away.

This theory was pioneered by Barry Buzan⁴⁰, this theory holds that security problems are the result of construction. That is an issue becomes a security problem because there are actors who discuss it by saying that the issue is an existential threat

³⁸ Chilton 1996; Stern 1999:133–4; Wyn Jones 1999: 157–8.

<https://issuu.com/arabianman/docs/international-relations-and-securit>

³⁹ Johan Eriksson & Giampiero Giacomello. *International Relations and Security in the Digital Age*. 2007.

⁴⁰ Buzan, Barry. *Security: A Framework for Analysis*. Boulder: Lynne Rienner Publishers. 1998.

for an entity. Buzan's theory has three models⁴¹ in specifically examining the cyber sector, namely:

1. Hypersecuritization: Buzan was introduced to describe the threats and dangers of securitization of a country's network above the normal level. Because the damaged network will result in the collapse of various systems and many sectors that will be attacked such as the financial and military sectors;
2. Everyday Security Practice: intended to secure actors, including private organizations and businesses, mobilize "normal" individuals in two ways: securing individual partnerships and fulfillment in maintaining security networks and making hyper-securitization scenarios more reasonable by combining threat and experience scenario elements which are already familiar in daily life;
3. Technification: use tools in the field of cyber technology that will play a large role in hyper-securitization.

1.8.4 Neorealism

This theory has four key assumptions: 1) states are the main actors in the system; 2) all states are rational, unitary actors; however, 3) interests are defined by security, not power; and, 4) power is the means to security, not the end goal itself.⁴²

The central tenet of Neorealism is The Security Dilemma, which holds that one state's increased security decreases that of others. This compels other states to compete to 'keep pace,' e.g., via arms races, with an implicit long-term, pan-systemic pressure on states not to lead or lag the others. As a result, the international system's nature leads to states' general-power-matching behavior. Further, as with Classical Realism, the International system is anarchic, meaning that states must look to

⁴¹ Hansen, Lene. *Digital Disaster, Cyber Security, and the Copenhagen School*. International Studies Association. 2009.

⁴² Waltz, Kenneth N., *The Origins of War in Neorealist Theory*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 615-628, <http://sites.google.com/site/casaroos/Waltz-OriginsofWarinNeorealistTheory.pdf>

themselves to cope with both internal and external problems.⁴³ Also, all states are functionally similar, and thus, all states seek the same goal, namely, to maximize their security. Thus, when threats arise, states try to counter them by balancing, by either or both of two methods:

- 1) Internal balancing, either via military and/or economic means; or,
- 2) External balancing (alliances.) External balancing (alliances) in particular, leads to the formation of international structures: ‘don’t seek too much power, or others will balance against you.’⁴⁴

There are two types of alliances in Neorealism. The first of these is called Balancing, in which states join together to match a common threat (e.g. NATO.) This type of alliance is defensive in nature, and it results in a more stable system. The second type of alliance is called Bandwagoning, in which lesser states join with a greater power, firstly, to prevent being attacked by that greater power, and secondly, to benefit from the ‘spoils’ (such as conquests) of the greater power’s successes.⁴⁵

1.8.4.1 Neorealism’s Relevance for Cyber Security

Neorealism has some relevance to Cyber Security, as in the physical world. Neorealism also shares its primary realworld shortcomings in overlooking the ambitions of some nation-states, and actors, in the cyberspace realm. For instance, aside from limited assistance and protection provided by federal agencies such as the DOD, DHS and NSA, there is little active defense/protection of all US individuals and organizations from cyber attack. The international system may be unipolar, in

⁴³ Walt, Stephen M., *International Relations: One World, Many Theories*, Foreign Policy, (Spring 1998), pg. 32, <http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124Readings/WaltOneWorldManyTheories.pdf>

⁴⁴ Waltz, Kenneth N., *The Origins of War in Neorealist Theory*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 619, <http://sites.google.com/site/casaroos/Waltz-OriginsofWarinNeorealistTheory.pdf>

⁴⁵ Waltz, Kenneth N., *The Origins of War in Neorealist Theory*, Journal of Interdisciplinary History, Vol. 18, No. 4, (Spring 1988), pp. 620-623, <http://sites.google.com/site/casaroos/Waltz-OriginsofWarinNeorealistTheory.pdf>

that the US may be the most dominant power in cyberspace; however, there are significant challengers, both from other nation-states, and from organizations (cybercriminals, in particular) that threaten the US and its constituents of all sizes. Indeed, China, Russia, Iran and North Korea are making significant efforts to undermine and take advantage of US cyberspace-based assets and vulnerabilities.⁴⁶

Interestingly, one outstanding example of the fruits of international cooperation towards cyberspace security is STUXNET, a joint US Israeli cyber warfare program/operation carried out against Iran's Natanz and Isfahan nuclear-weapons development facilities, allegedly dating back to 2010.⁴⁷ However, this is a relatively isolated event in international cooperation; there is precious little else ongoing, at least, not in the open-source world. Tellingly, STUXNET was an offensive cyber security program and operation, supporting the previous assertions about the realist, anarchic, offense-dominant nature of cyberspace and Cyber Security operations. Nonetheless, STUXNET serves as a powerful example of the potential benefits of international cooperation in cyber security. Also, and more ominously, there is cooperation between Iran and Hezbollah, Iran's Lebanon-based terrorist proxy organization, in carrying out cyber warfare operations against the US and elsewhere.⁴⁸ While this implies that there are at least some advantages to be obtained by 'balancing' or alliance formation among states (and perhaps, all levels of entities within cyberspace) in Cyber Security, and that this IR Theory has at least some potential benefits to offer, Neorealism nonetheless holds little overall insight into the international system in cyberspace.

⁴⁶ Tadjdeh, Yasmin, *Fears of Devastating Attacks on Electric Grid, Critical Infrastructure Grow*, National Defense Magazine, October 2013, <http://www.nationaldefensemagazine.org/archive/2013/October/Pages/FearsofDevastatingCyberAttacksOnElectricGrid,CriticalInfrastructureGrow.aspx>

⁴⁷ Barnes, Ed, *Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Ambitions*, FoxNews.com, November 26, 2010, <http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclearambitions/?test=latestnews>

⁴⁸ Staff, *Iran's global cyber war-room is secretly hosted by Hizballah in Beirut*, DEBKAfiles.com, 10-21-12 <http://www.debka.com/article/22459>

1.9 Research Methodology & Thesis Structure

The research methodology is a process or scientific way to obtain data that will be used for research purposes. The methodology is also a theoretical analysis of a way or method in this thesis; by using Qualitative research methods with secondary data. Through this research, it is expected to obtain a relevant information and data to answer what the main interests of the United States are to develop cybersecurity strategies and how those strategies are implemented. This research method is focuses on a Web Surface and Deep Web shutter. The results have showed that the United States has put cybersecurity as a National security priority. The developments of information technology have provided a significant shift from the concept of security. At present, countries are not limited to interact physically in real space but also extended to cyberspace.

Consequently, the state must adapt to this development. The concept of cybersecurity should be established as one of the domains of the state which should be safeguarded as the state's obligation to secure its borders. Now the interaction between the actors of international relations is not only in the land, sea, and air. The interaction between the actors also performed in the virtual space into other options to achieve the interests. This study aimed to explain what has the US already done with cybersecurity strategies in the Domestic, Regional, and International of the United States. Where the United States in the last 10 years is very intense released a cyber-security strategy.

I.10 Thesis Structure

• Chapter I – Introduction

The first chapter of this thesis will introduce the reader on the issue and critical information as well as the background of the analysis. This chapter is intended to be the basis of the writing and also to provide general insight into the thesis. This

chapter will examine the reason why U.S. Cyber Security has become a National security priority on US Government.

• **Chapter II – Literature Review**

The second chapter of this thesis will describe an explanation from a literature book about Cyber Security as a National Security Interest to US National Security. This chapter will describe furthermore about the cyber space, criminal activity and Cyber Warfare in Cyberspace, Cyber Security Challenges the United States, including the threats models as the basic knowledge for a decision making (US Government) for consider a threat for implement and improving a US Cyber Security.

• **Chapter III – Cyber Security in the United States Security System**

The third chapter of this thesis will explain about US Cyber Security. It includes an explanation of US Cyber Security Strategy Policy through the worldwide. It will also describe a brief history what have US effort to implement a Cyber Security Policy from Obama's era. It will contain about the implement of both US Government and Military. In this chapter also describe more about the US Cyber Security strategies, developments and preparations in deterring Cyber Warfare.

• **Chapter IV – The Nature of Cyber Security Attack and United States Responses**

The fourth chapter of this thesis will explain about bilateral relations of United States with China and Russia. It will also describe what have US effort to keep relations on International. It includes some Cyber Security Experts commends.

• **Chapter V – Conclusion**

The fifth chapter of this thesis is the conclusion of the fourth chapter. This chapter will conclude all the US Cyber Security in enhancing National Security through US Cyber Security Strategy and Policy.

CHAPTER II

Literature Review

Cyber Security is defined as prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.⁴⁹ On the national and transnational levels, the matters of cyber security primarily concern criminal matters. The main issues are highlighted by the fragmentation of national criminal laws (substantive and procedural) and the need for their harmonization. The diversity of national laws is one of the main reasons for the global cybercrime vulnerabilities, as such diversity does not allow for the development of a single legislative response to the global phenomenon. Many countries, especially developing countries, do not have criminal laws that specifically address cybercrime. Neither do they have adequate capacity to enforce the laws.⁵⁰

On the international level, Cyber Security is concerned with the application of international law to the realities of network and computer technologies, including the possibility of their use in modern warfare.⁵¹ The attribution of the conduct – distinguishing the offender between state or non-state actors – and identification of the offender jurisdiction are significant challenges. With all these challenges in hand, the effective legal regulation of the internet presumes creation of the viable policy

⁴⁹ Department of Defense. *Cybersecurity and the Risk Management Framework*. <https://www.slideserve.com/yერიel/cybersecurity-and-the-risk-management-framework>

⁵⁰ Webology. *International Actions against Cybercrime: Networking Legal Systems in the Networked Crime scene*. September 2007. <http://www.webology.org/2007/v4n3/a45.html>

⁵¹ Artur Appazov. *Legal aspects of Cybersecurity*. 2014. http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspublikationer/Legal_Aspects_of_Cybersecurity.pdf

that can adequately address the substance of the problem and its technical complexity on various levels, including legislative interventions in the form of criminalization and harmonization; international cooperation; collaboration with the private sector; professional educational and capacity building in terms of technical support and assistance, especially in the developing countries.

The Government of the United States (US) has shown its seriousness in building its information security system. This is of course closely related to the enormous dependence of the US government on information system security networks. Cybersecurity has become a priority for US domestic political policy given its very vital existence. The US government is building a network of information security systems in the fields of military, agrarian, traffic control systems, water, and sanitation, energy and transportation. This vital aspect is very dependent on the role of computers and cyberspace. The US government is renewing the standardization of cyber security. If the information security system is hacked, the US state will automatically be paralyzed and cause serious impacts. The seriousness of the US to build a cyber security system, especially in the era of Barack Obama's leadership, was the government's response to the input and criticism of US society about even though the network information security system in the superpower country is the second strongest cyber security (based on UN reports⁵²) but still have vulnerabilities. This condition can be seen from the record of cyber attacks experienced by the US in the last 10 years. These include retaliatory attacks on Sony Pictures Entertainment, Anthem Insurance, Target, Home Depot, eBay and JPMorgan Chase. The federal government has also experienced cyber attacks, including crackdowns of unclassified computers in the White House and the Department of Foreign Affairs and hacking of Twitter and YouTube accounts belonging to the US military command.

⁵² Bloomberg BNA. *U.S. Has second strongest Cybersecurity in the World, UN Reports*. July 14, 2017. <https://www.bna.com/us-second-strongest-b73014461766/>

The United States has enough reasons to put cyber security as one of the country's main security priorities. Judging from the cyber-attack data experienced by the United States since 2009 - 2014 the highest percentage of attacks occurred in government areas and the world of industry; of course this is a vital area of the country.⁵³ Meanwhile, the world of an industry that is most often the target of cyber crime attacks is in the financial services sector; this is, of course, a very big concern considering financial services hold a very strategic area in the United States industry.

Another thing that makes cyber security a very important concern is the level of difficulty in mitigating it. Forms of attacks that range from the form of viruses, attacks on sites, hackers and so on are a challenge for the Department of Defense in creating security because it deals with an enemy that is difficult to identify, the source of the attack and the form of some attack.

This research will explain the influence of the United States Cyber Security Strategy in securing and maintaining important digital data and vital infrastructure of the United States from the threat of cyber warfare. Whether the Cyber Security Strategy successful in securing important digital data and vital infrastructure depending on its implementation.

Cyber elements include all digital automation, including those used by the Department of Defense (DoD) and its industrial base. Includes the information technology (IT) embedded in weapons systems and their platforms; command, control, and communications (C3) systems; intelligence, surveillance, and reconnaissance (ISR) systems; logistics and human resource systems; and mobile as well as fixed infrastructure systems. "Cyber" applies to, but is not limited to, "IT" and the "backbone network," and it includes any software or applications resident on

⁵³ Pew Research Center. *Cyber Attacks Likely to Increase*. October 29, 2014. <http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/>

or operating within any DoD system environment, which is commonly collectively referred to as information and telecommunication technology (ICT).⁵⁴

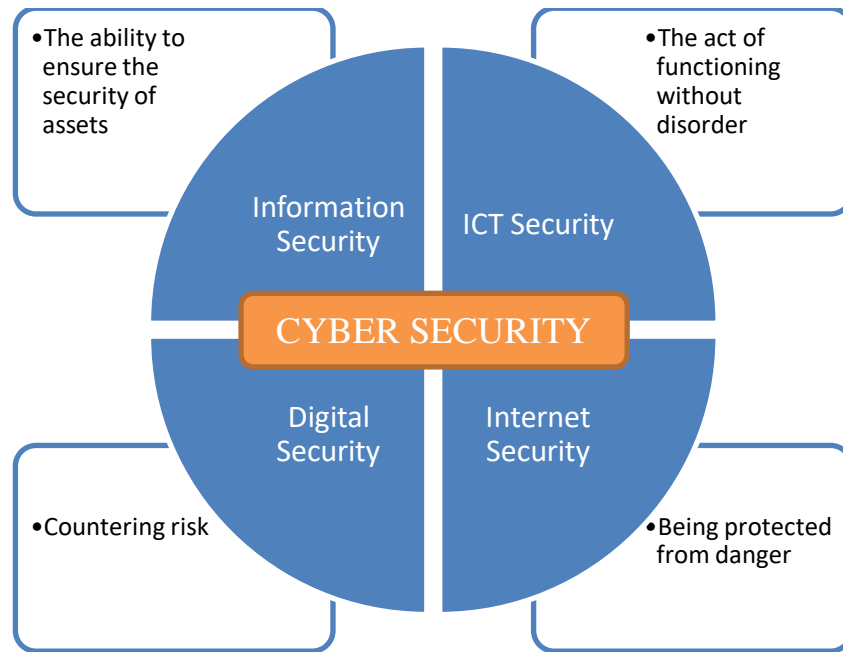


Figure 3. Concept of Cyber Security

Source: Book of *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* <https://www.igi-global.com/book/cyber-security-threats/190539>

II.1 Understanding Cyber Space

There are many terms associated with Cyber Security which are information security, critical infrastructure, information assurance, standards, security baselines,

⁵⁴ DSB Task Force on “Resilient Military Systems and the Advanced Cyber Threat;” January 2013. <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

security risk management, information systems, and more. Understanding the relationships between these terms and disciplines is essential. The cyberspace is a virtual space formed from the results of the union between humans and technology.⁵⁵ Literally, the concept of cybersecurity no longer only touches the technology area but has become a threat to national security. Cybersecurity has become a priority for governments around the world. Major cyber-attacks, data losses, and compromised networks fill the headlines, and governments, the private sector, and citizens all recognize the need for action to improve cybersecurity. Governments worldwide are struggling with questions around how to do this while balancing privacy, civil liberties, and cost. Over the past decade, national governments have been developing strategies to address emerging security issues associated with the rapidly expanding use of information and communications technology (ICT).

These “cyber security” issues have developed into significant national-level problems that require government consideration, including the protection of assets, systems, and networks vital to the operation and stability of a nation and the livelihood of its people. Threats against these vital assets target corporations and citizens and include cybercrime such as identity theft and fraud, politically motivated “Hacktivism,” and sophisticated economic and military espionage.⁵⁶ Previously, discussions about national security were very rarely associated with technology. However, the increasing threat of domestic and international cyber attacks on US public and private infrastructure after the passing of the 9/11 incident, awareness emerged to popularize that cybersecurity is not just a simple password protection issue. Further cybersecurity requires a series of strategies because it involves national interests. The development of information technology has also provided significant changes regarding the concept of security, now the space for interaction cannot be limited to physical but also extends to cyberspace. Consequently, the state must adapt

⁵⁵ Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidang*. 2012. Jakarta: PT. Tatanusa.

⁵⁶ Cristin Flynn Goodwin & J. Paul Nicholas (Microsoft). *Developing a National Strategy for Cybersecurity, Foundation for Security, Growth, and Innovation*. October 2013. Page 3

to this development the concept of cyberspace security is time to be established as one of the regions for a state that safeguards its security as the state's obligation to secure its territory.

Moreover, cyber-attacks not only occur in public institutions but also attack government institutions. Cybersecurity is aimed at information security issues for government, organizations and individual affairs associated with ICT technology, and specifically with internet technology.⁵⁷ Cybersecurity cannot be abstracted too far from its application area and socio-cultural environment. The terminology of "information security" and "cyber security" are two different concepts. In certain contexts, there is a common understanding if it is associated with asset protection or resistance to industrial and economic espionage, resistance to terrorism or economic crime, resistance to prohibited content.⁵⁸ In other contexts, the two concepts have differences. Cybersecurity includes everything related to computer surveillance, monitoring to very strict control or the struggle for fundamental human rights. While information security relates to broader issues, such as state sovereignty, national security, protection of important infrastructure, security of visible and invisible assets, and protection of personal data.⁵⁹

II.1.1 Internet

The history of the Internet began in the 1960s, namely when Levi C. Finch and Robert W. Taylor began conducting research on global networks and interoperability issues.⁶⁰ In 1969, Robert Taylor was newly promoted as head of the information processing office at DARPA (Research Agency The United States Armed Forces) intends to implement the idea of creating a network system that is

⁵⁷ Ghernaouti, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. 2013. Page 329. Lausanne: EPFL Press.

⁵⁸ *Ibid* Page 330.

⁵⁹ *Ibid* Page 330.

⁶⁰ Internet Society. *Brief History of the Internet*. 1997.

<https://www.internetsociety.org/internet/history-internet/brief-history-internet/>

interconnected. Together with Larry Robert of MIT, Robert Taylor began a project which came to be known as the ARPANET.⁶¹ Soon the project developed rapidly in all regions, and all universities in the country wanted to join, making it difficult for the ARPANET to manage it. Therefore the ARPANET was broken down into two, namely "MILNET" for military purposes and the smaller "ARPANET"⁶² for non-military purposes such as universities. The combination of the two networks was finally known as DARPA Internet, which was later simplified to become the Internet. However, the rapid development of the internet has not only given birth to a positive side, but also has a negative side or a dark side that is behind the shadows of the advanced civilizations of the world of technology today. The side is called the Underground Internet / deep web, which refers to sites that are not indexed by standard search engines like Google / Yahoo / Bing. In fact, we cannot access it on the basic World Wide Web (WWW) search engine. This is because these sites are dynamic, which will only be formed by specific searches.⁶³

II.1.2 Web Surface and Deep Web

The internet is divided into two sides, namely the Web Surface and the Deep Web.⁶⁴ The Surface Web is all information contained on the Internet and can be searched by ordinary search engines, while the Deep Web is all information contained on the Internet but not detected by ordinary search engines. Moreover, all information contained on the internet from general to confidential 96% is stored / placed on the Deep Web. It is through the Deep Web that all kinds of cyber attacks are launched. Any country, group or individual who can control and control Deep Web will have a huge influence in the world of international cyber.

⁶¹ Britannica. *ARPANET; United States Defense Program*. <https://www.britannica.com/topic/ARPANET>

⁶² Taylor and Francis Online. *Cybersecurity and Cyber Defence: national level strategic approach*. <https://www.tandfonline.com/doi/full/10.1080/00051144.2017.1407022>

⁶³ Ghernaouti, Solange. 2013. *Cyber Power : Ghernaouti, Solange. Cyber Power :Crime, Conflict and Security in Cyberspace. Lausanne: EPFL Press. 2013. Page 126.*

⁶⁴ Martin, Jeremy. *The beginner's Guide to The Internet Underground*. Information Warfare Center. 2013.

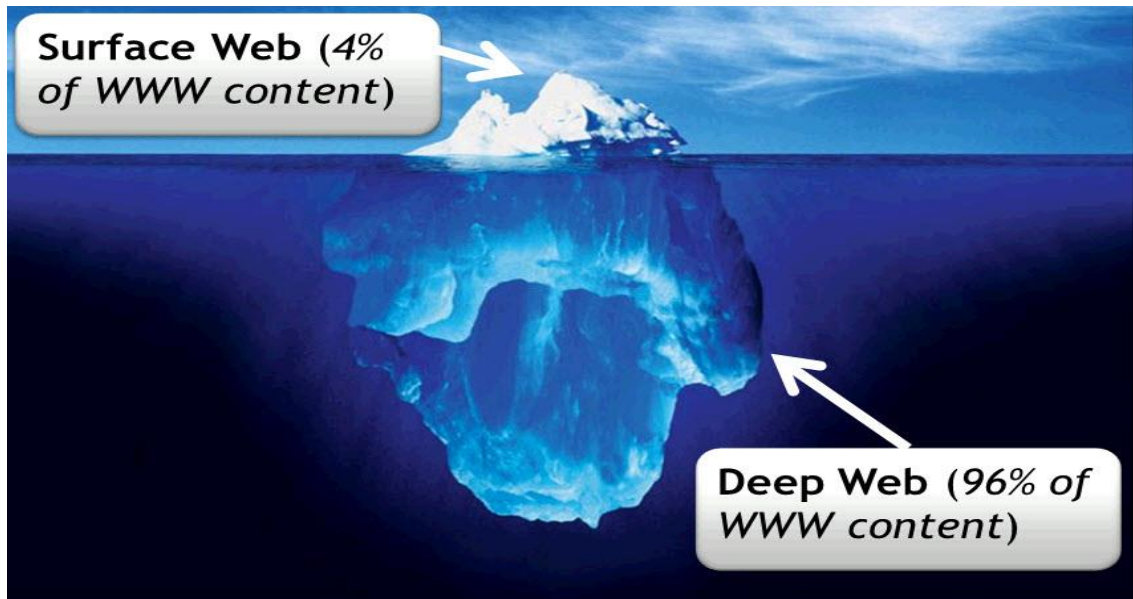


Figure 4. Surface Web and Deep Web

Most of the deep web content contains a wider scale databases from the results of research conducted by academic institutions and government institutions as well as personal sites. This may be one of the causes of "hidden" sites on the deep web because it is not for general consumption. But in some deep webs, there are also unusual sites. For example, the site where drug trafficking, illegal pornography, contract killer services, illegal experiments in humans, hacking services, and sales of credit card information. Some people think that sites on the deep web that provide contract killer services and illegal experiments are untrustworthy. A transaction in the deep web is using a Bitcoin as a payment method.⁶⁵ In fact, public information on the web is 400 -500 times larger than that on a regular web, or the Deep Web indexed has as much as 7500 TB (terabytes) of information compared to 19 TB of information on the regular web, or indexed there are around 550 billion confidential or public documents on the Deep Web compared to 1 billion documents that are on

⁶⁵ Bitcoin. <https://bitcoin.org/en/>

the regular web, or which are indexed by more than 200,000 active websites and can be accessed without encryption.⁶⁶

The quantity of deep web information is greater than the websites that have been indexed in standard search engines (Because all files are confidential) more than 95% of information from websites that are on DEEP WEB can be accessed without registration or payment. The Deep Web is the biggest category of the Internet, bigger than what has been indexed in search engines, plus all that is on the Deep Web is, the real identity of international hackers, scientists engaged in non-humanity, international drug kingpin, contract killer, astronomers, psychic expert, revolutionary, member Government, police, terrorists, intruders, data thieves, kidnappers, exact sociologists who are crazy, pedophiles, and others. The Deep Web is a place where all things that people generally don't expect will exist and are real. Just like the Deep Sea which is very difficult to penetrate light, as well as the Deep Web, there are many bad and dark sides of the Deep Web, because the good side is only a little. That's why it is called the Deep Web.

II.2 Cyber Warfare

Cyber warfare and telematics crimes are detrimental to many countries because they are wars that have used computer networks and the internet or cyberspace in the form of defense strategies or attacks on opponents' strategy information systems.⁶⁷ Cyber warfare refers to users of World Wide Web (WWW) and computer networks to carry out wars in cyberspace. Cyberwar is also defined as a war that uses electronic equipment and computers to destroy or interfere with electronic equipment and communication lines of opponents. Cyberwar can be in the form of conflict between countries, as well as involving non-state actors. It is very

⁶⁶ Darkwebnews. *Deep Web: What is it and how to access it?* <https://darkwebnews.com/deep-web/>

⁶⁷ UNODC. *Cybercrime as a Transnational Crime*.
<https://www.unodc.org/unodc/en/cybercrime/index.html>

difficult in a cyber war to direct the right and proportional power, the target can be military, industrial, or civilian, or it can be only a server room which is in charge of various clients, with only one of them being targeted.

In the development of Cyber Warfare, the use of information system technology is also used to support the interests of communication between soldiers or command lines facilitated by a modern military control command system, namely the Network Centric Warfare (NCW) system. Network Centric Warfare or NCW is a modern military operation concept that integrates all military components or elements into one NCW military computer network based on satellite technology and a military secret internet network called the SIPRNet (Secret Internet Protocol Network Router).⁶⁸ NCW technology supported by SIPRNet infrastructure as military components or military elements can be connected online and real-time systems, so that the presence of opponents and friends can be known through visualization on a computer or laptop screen. This NCW technology has been owned and applied by the United States military. The threat actors can come from countries (state actors) or non-government (non-state actors) so that the perpetrators can come from individuals, groups, and other organizations that can come from their own country, or between countries. Sources of threats can come from inside or outside, social conditions, human resources, and technological developments. Source of cyber threats can come from various sources, such as:

- Foreign intelligence service;
- Dissaffected employees;
- Investigation of Journalists (investigative Journalists);
- Extremist Organization;

⁶⁸ Military Factory. *Secret Internet Protocol Router Network Definition (US DoD)*.
https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=4771

- Activities of Hackers (Hacktivists);
- Organized Crime Group (Organized Crime Groups).

American prosperity, liberty, and security rely on open and reliable access to information. The Internet have engages American and enhances their lives by providing ever-more prominent access to new knowledge, businesses, and services. Computers and network technologies support U.S. military war fighting superiority by empowering the Joint Force to gain the information advantage, strike at long distance, and exercise global command and control. The arrival of the digital age has made challenges for the Department of Defense (DoD) and the Nation. The open, transnational, and decentralized nature of the Internet that DoD and the Nation seek to protect creates significant vulnerabilities. Competitors discouraged from engaging the United States and allies in an armed conflict are using cyberspace operations to steal technology, disrupt the government and commerce, challenge the democratic processes, and threaten the critical infrastructure.

The United States are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to incorporate persistent battles in and through cyberspace that present long-term strategic risk to the Nation as well as to United States allies and partners.⁶⁹ China is eroding U.S. military overmatch and the Nation's economic vitality by persistently exfiltration sensitive information from U.S. public and private sector institutions. Russia has used cyber-enabled information operations to influence United States population and challenge the democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests. Globally, the scope and pace of malicious cyber activity continue to rise. The United States' growing dependence on the cyberspace domain for nearly every

⁶⁹ CHIPS. *CIWT Assumes Cyber Mission Force Training Role*.
<https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=10830>

essential civilian and military function makes this an urgent and unacceptable risk to the Nation.⁷⁰

II.3 Cyber Security Challenges

The United States government develops challenges in cybersecurity into three main components, namely policy, technical, and human. The three components of the challenge are related to each other so as to form new challenges, namely the process, skills, organization, and the core of all challenges (Steve Winterfeld and Jason Andress). The following chart shows the relationship between the challenges that exist in cybersecurity.

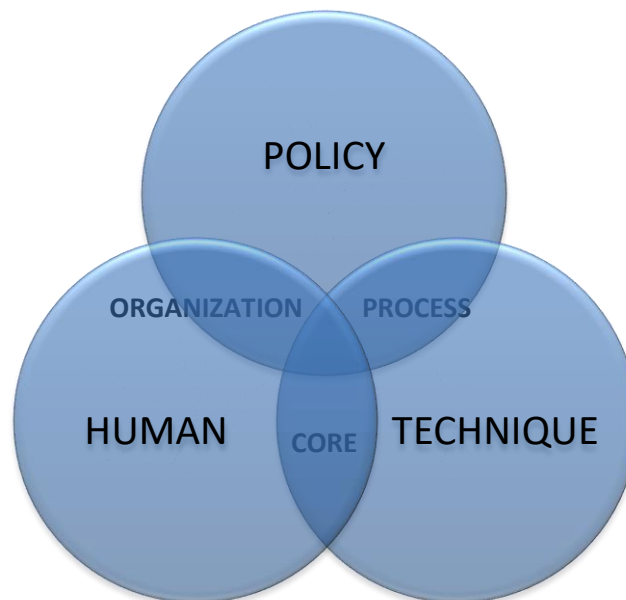


Figure 5 Chart of Cyber Warfare Challenges: *Techniques, Tactics, and Tools for Security Practitioners*. Sources: Jason Andreas and Steve Winterfeld (2009).

⁷⁰ Department of Defense, *Department of Defense Cyber Strategy Summary 2018*. Page 1

II.3.1 Policy

The policy is what can provide a beacon in this storm of cyber risk and help an organization put in place multi-level, in-depth defenses. The policy is a core element of the cyber security management system. Without it, extensive implementations of routers, firewalls and intrusion detection systems are misguided. Indeed, policy steers the application of technology within this system. What is meant by policy in the United States includes legal issues, national security, and privacy. Some challenges related to policy in America are:

(a) there is no common vision relating to the cyber war doctrine; (b) there is no standard procedure for responding to cyber attack⁷¹ (whether technically, legally or diplomatically); (c) even if the rules have been prepared, each institution has different applications, depending on the culture of each state institution. Often information exchange between state institutions is difficult.

II.3.2 The Process

The challenge in the process is about auditing. The audit is a structured and routine evaluation of the cyber personnel system and the process of activities carried out in a company. The audit process is an example of the stage of measurement of a continuous security improvement program. The cyber audit is part of cybersecurity programs. Cyber audits will identify more than 600 vulnerabilities, delivered a number of 202 vulnerabilities with high-risk classifications. To anticipate these things, the United States feels the need to develop a set of standards that can be used by the government and industry sectors. The US has various audit standards, such as the Information Systems Audit and Control Association (ISACA), and Control Objectives for Information and Related Technology (COBIT). Both are international

⁷¹ According to the results of the interview with Dr. Yono Reksoprodjo, this context has caused the cyber domain to fall into the "asymmetrical" category.

organizations that make rules for standardization to regulate information security. The audit is carried out using (a) Information Technology Infrastructure Library (ITIL); (b) Capability Maturity Model Integration (CMMI); and (c) Six Sigma. However, the audit by working in such a manner is no longer suitable to be applied in situations that can quickly obtain results, therefore the audit system must be sought automatically so that the results can be obtained at the same time as the audit process (real time) In line with this automation idea, America currently has a set of accreditation and certification standards, namely: (a) DIOD Information Assurance Certification and Accreditation Process (DIACAP), and (b) Director of the Central Intelligence Directive (DCID) 6/3. These two systems process the Federal Information System Management Act (FISMA) which has now been carried out in all government institutions.

II.3.3 Technique

The technical aspects consist of resilience, supply chains, mobile devices, trust chains, data protection, management identity/characteristics, virtual systems, and interference detection systems. A system is designed to have toughness with the aim of being able to repair itself without human intervention. In the cyber context, cyber systems must be able to provide information thoroughly. For example, information that accesses cannot be authorized. To ensure equitable distribution in cyber systems, an important aspect related to reliability is the ability of the system to fit certain functions in carrying out rejection if there is a 'service attack'. Reliability is an attribute that must be owned by cyber systems. The challenge is how to develop systems that have reliability and are specifically designed for the industry level.

II.3.4 Skill

The challenges in terms of skills are too much data and lack of face-to-face (poor interfaces). Too much data collected can be a challenge so it needs to be stopped and start selecting existing data. The main problem that often occurs in storing data is how much data can be selected because data storage requires a fee. Lack of face to face is a problem that often occurs in every system. Most existing systems still need human assistance in their operation, without human assistance, the system cannot carry out its functions properly. The American government needs a security system that has intuition and can carry out analysis to develop and regulate its data investigation, rather than just accepting what has been provided.

II.3.5 Humans

Care for danger needs to be fostered in every user of the Cyberworld. They must be aware of the immediate activities carried out because maybe their unwitting activities can cause crime. The surrounding environment is often a severe threat. Every user of the Cyberspace needs to specify who can access their personal data. In an effort to answer the scarcity of skilled workers in securing the cyberspace, since March 2010 the US Government held the National Initiatives for Cybersecurity Education (NICE) and the Center of Academic Excellence in Information Assurance Education. But the efforts made cannot be followed by the whole community, only in certain regions (Andress and Winterfeld).

II.3.6 Organizations

Organizations in a broad scope, such as a country, tend to limit the spread of information. Information dissemination can only be done within the organization and the spread of information outside the organization is prevented. The organization

builds a network system that can be separated from other organizations or groups as cybersecurity efforts. The actions taken by the US Government against acts of Chinese espionage are one example. The US government closes all important information that is owned by its country and does not allow other parties, in this case, China know that information. An organization against cyber attacks requires training so that they can be familiar with the situation and know what actions need to be taken.

II.3.7 The Core of all challenges

The core of all the challenges put forward by Andress and Winterfeld are (a) determining the perpetrators who committed or were responsible for crimes in the cyberspace; (b) conduct a study of cause and effect, which is to implement long-term thinking about the impact caused if an action is taken; (c) improve the ability to make decisions based on understanding the situation that occurred at this time or before; (d) equating understanding of the context discussed so that there is no misperception; (e) instill the spirit of sharing information, because what is happening now is that both the private sector and the government tend to cover up the information they have on the grounds of competition with other parties and national security; (f) continue to carry out a needs analysis to measure any cyber activities that have a negative impact; (g) integrating all systems within the organization so that activities that threaten cyber security will be quickly tracked.

II.4 Understanding Cyber Threats through Threat Models

The United States places a Cyber Security as one of four National security priorities. The director of the Federal Bureau of Investigation (FBI) added that cyber threats have a potential to equal or surpass the threat from terrorism in the future. Four types of actors are characterized: criminal hackers, organized criminal groups,

terrorist networks and advanced nation-states.⁷² In order to establish National cyber security priorities, a risk framework must reflected on the motives of threat actors; potential avenues for attack or exploitation; and the key assets or functions that could be targeted by criminals, non-state actors, and state-sponsored organizations.⁷³ When developing national threat models, governments should see the input from a variety of sources, including government and law enforcement agencies, the private sector, and academia. Counseling a wide range of stakeholders equips national governments to prioritize their defensive efforts. The prioritization of threats will differ between countries, given factors such as ICT penetration, levels of economic development, and also geopolitical considerations.

According to big company of Operating System which is Microsoft, they have identified four major categories of cyber threats to simplify the threat model used in the assessment process.⁷⁴ Categorizing the threats in this manner makes it easier to assess them more clearly and then develop preventive and reactive strategies. Categorization can also help reduce the paralysis that may occur when governments attempts to design a single strategy for the myriad of threats that involve information technology.

The four major categories of cyber threats are:

1. Conventional cybercrimes. These crimes include cases in which computers are targeted for traditional criminal purposes, or used as tools to commit traditional offenses including fraud, theft of intellectual property or financial instruments, abuse or damage of protected information technology systems, and even damage of critical infrastructure. These crimes span those

⁷² The RAND. *Cyber-security threat characterization*. 2013.

https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR235.pdf

⁷³ Erica Borghard. *Protecting Financial Institutions Against Cyber Threats: A National Security Issue*. September 2018. <https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324>

⁷⁴ Cristin Flynn Goodwin & J. Paul Nicholas. *Developing a National Strategy for Cybersecurity*, *Foundation for Security, Growth, and Innovation*. October 2013. Page 4.

committed by individual hackers through those committed by organized crime entities.

2. Military and political espionage. These attacks include instances in which nation-states intrude into and attempt or succeed to exfiltrate large amounts of sensitive military data from government agencies or the military-industrial base, or use third parties to do so on their behalf.
3. Economic espionage. This category applies to governments (or third parties that are acting on their behalf) stealing intellectual property that was created in other nations, or tolerating domestic companies stealing information from foreign competitors.
4. Cyber conflict or cyber warfare. Asymmetric warfare has significant implications for cyber-attacks, since the Internet makes it possible for anonymous and difficult-to-trace individuals or organizations with slight resources to engage a nation-state in cyber conflict. Recently, 15 governments including China, Russia, and the United States agreed that the United Nation charter applies in cyberspace and affirmed the applicability of international law to cyberspace.⁷⁵

These kinds of threats that has described can have serious implications for critical infrastructures, including the theft of sensitive data, damage to business or operational systems, disruption of services, and other scenarios that could result in substantial financial loss and compromise public safety or National security. Each of these four areas should be included in the threat model for the national strategy.

⁷⁵ Patrick. *US, China Among 15 Countries agreeing UN Charter Applies in Cyberspace*. 2013. <http://cnsnews.com/news/article/us-china-among-15-countries-agreeing-un-charter-appliescyberspace#sthash.y9G5beB4.dpuf>

CHAPTER III

Cyber Security in the United States Security System

There is no relenting in the cyber war that happens every day against government targets. Networks are bombarded with Cyber Attacks, with attempts at breaching the fortified systems growing more and more sophisticated.⁷⁶ The threats against U.S. critical infrastructure and the economy are constant (Department of Homeland Security 2014). With the United States relying so heavily on connectivity, officials have warned just how damaging an attack could be. Leaders at all levels, all the way to the president of the United States, have repeatedly voiced concerns about the possible impacts a Cyber Attack could have on the nation.

The United States is a superpower in various fields including information and communication technology. The author examines that the United States has have advanced information and communication technology and is supported by well implemented policies taken by the head of state to protect cyber space security from the threat of cyber warfare. But it needs to be underlined, no matter how advanced the capabilities are, as good as any implemented policy, the name of this network technology will still have gaps or bugs that can be used as an entry gap to carry out cyber-attacks even if only on a very small scale. The next point will explain the attacks carried out against and by the United States as well as legal regulations regarding cyber warfare owned by the United States. The United States is known as the country that has the second strongest cyber security, but still there are those who try to carry out cyber-attacks against the United States.⁷⁷ This is reinforced by the

⁷⁶ Paletta, Damien. *NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent*. The Wall Street Journal. September 8, 2015.
<http://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-wassophisticated-persistent-1441761541>

⁷⁷ The Cyber Research Databank. *Top 10 Countries Best Prepared Against Cyber Attacks*.
<https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/>

increase in cyber-attacks placing confidential information in danger that will have an impact on federal operations, assets and the American people themselves.

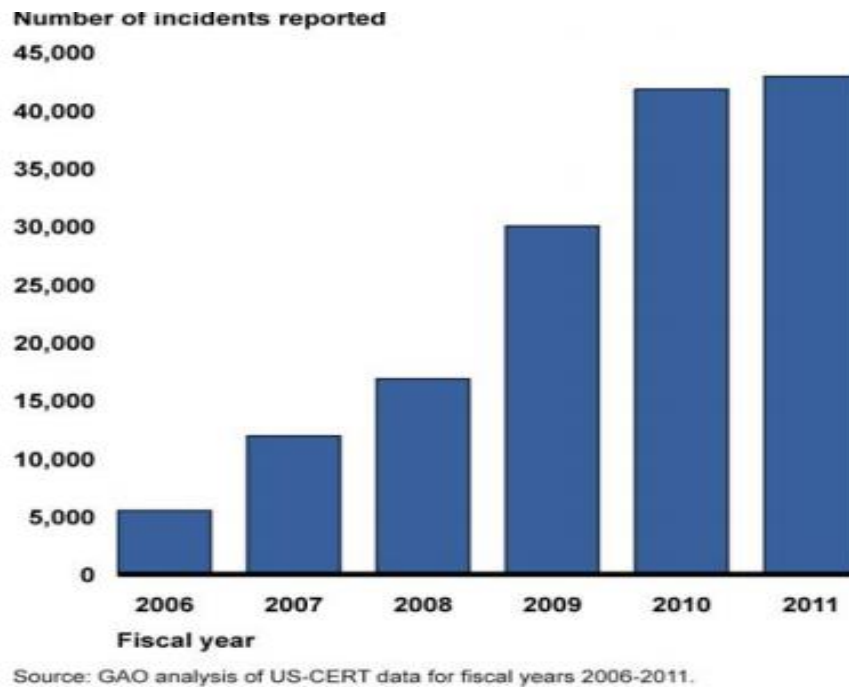


Figure 6 Incidents Reported to US-CERT: Fiscal Years 2006-2011.

In the past 6 years, there has been an increase in the quantity of cyber-attacks from 5,503 cyber-attacks in fiscal 2006 to 42,887 cases in 2011. This increase reached 680%.⁷⁸ Some examples of cases of cyber-attacks on the United States are as follows:

⁷⁸ Wilshusen, Gegory C. *Cybersecurity Threat Impacting the Nation*. GAO Report of US-CERT. 2014.

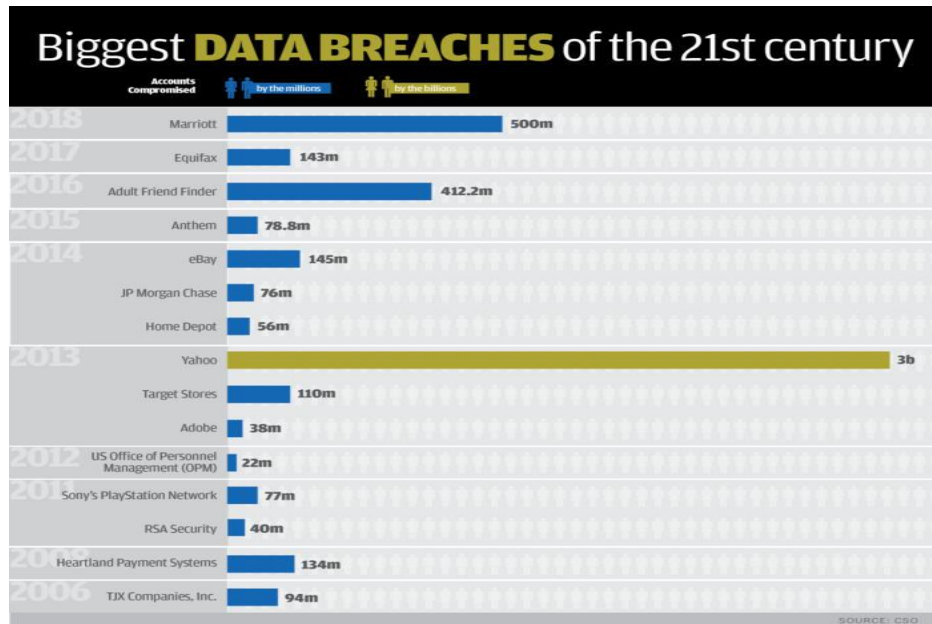


Figure 7 List of United States Companies are hacked from 2006. Source:

<https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html>

- The company's POS system named Michaels was attacked by hackers and 2.6 million customer payment cards were attacked by viruses in May 2013 to January 2014;
- Yahoo's Communications Company was hacked in January 2013 and allegedly 273 million e-mail accounts were hacked;
- 400,000 Aaron Brothers company customer credit and debit card information was stolen by using malware on the POS system;
- User information, including the social security information of AT & T communication company customers accessed by outsiders for 2 weeks in April 2014;
- The eBay company was hit by a cyber attack at the end of February to the beginning of March 2014 which resulted in the inaccessibility of 233 million

customer accounts. Therefore eBay immediately asks customers to immediately change their password;

- Five hackers from China were indicated to be hacking computers and spying on the economy of companies from the United States from 2006 to 2014. The targeted companies are Westinghouse energy company, SolarWorld industry, US Steel industry, Allegheny technology company, Workers Union service company and Alcoa industry;

- According to a report from the Homeland Security Department, a company that is not named has been accessed by hackers by force through an employee password;

- The US Transportation Command Contractor network was attacked up to fifty times between June 2012 and May 2013. At least, twenty attacks originated from China;

- Su bin, a 49-year-old Chinese hacker indicated that he hacked into the Boeing defense industry between 2009 and 2013. He worked with two other hackers with the aim of stealing plans for defense development programs such as the F-35 and F-22 forged jets;

III.1 The Nature of Global Cyber Security Competition

To understand just how technology becomes vulnerable to cybercrime, it helps to first understand the nature of threats and how they exploit technological systems. Technology is vulnerable at all, and the answer is simple: trust. From its inception, the protocols that drive Internet, by and large, were not designed for a future that involved exploitation, there was little expectation at its birth that might need to one day mitigate against attacks such as a distributed denial of service (DDoS), or the things that shelf might need security protocols to prevent it being hacked and used to espionage. In many cases, the idea that a device might be used for nefarious purposes isn't even considered. Cybercrime comes in a variety of forms ranging from denial of service attacks on websites through to theft, blackmail, extortion, manipulation, and destruction. The tools are many and varied, and can include malware, ransom ware, spyware, social engineering, and even alterations to physical devices.⁷⁹

The sheer scope of possible attacks is vast, a problem compounded by what's known as the attack surface: the size of the vulnerability presented. The first step in any analysis of cyber-security must be to chart the range of cyber threats, by which is meant either security challenges made via ICT equipment and networks, or challenges made to those equipment and networks. This can be a difficult undertaking, not least because these two broad categories of security challenge can overlap. Disruption of which could fall into both categories just described.⁸⁰ The transformation of the Internet from an elite research network to a mass communications medium has altered the global cyber-threat equation dramatically. The global ICT system can be exploited by a variety of illegitimate users and can even be used as a tool in state-level aggression. These activities can be organized along a spectrum running from individual action, to the behavior of non-state actors and groups, to plans orchestrated by governments.⁸¹

It is important to note that these diverse users of the Internet do not fall into discrete camps, and least of all into a simple hierarchy of threats. Hacking, for

⁷⁹ P. Cornish, R. Hughes and D. Livingstone, *Cyber-space and the national security of the United Kingdom* (London: Chatham House, forthcoming 2009).

⁸⁰ Let it rise: A special report on corporate IT, *The Economist*, 25 October 2008, page 7

⁸¹ A. Sipress, 'An Indonesian's Prison Memoir Takes Holy War Into Cyberspace', *Washington Post*, <http://www.washingtonpost.com/ac2/wp-dyn/A62095-2004Dec13?language=printer>, 14 December 2004.

example, can have uses in very serious organized crime; organized criminality can be linked to international terrorism; and terrorism can be used a tool of state aggression.

Leadership in the area of cyber security by national governments is manifested largely through the government's national policy-making role. Governmental policy-making in the area of cyber security provides, at the highest level, a common understanding and vision of the problem, allowing for coordinated national action that would realize national cyber security objectives. The preparation of a National Cyber Security strategy is an essential first step in addressing cyber security challenges. Such a statement typically:⁸²

- Highlights the importance of ICTs to the nation (e.g. by providing information on the role of ICTs in the economy, society and national security, and the industrial and governmental processes dependent on ICTs);

- Identifies and evaluates potential risks and threats (e.g. cyber attacks, cybercrime, etc.);

- Establishes cyber security related objectives (e.g. containment of cyber-attacks, detection and prosecution of cybercrime, protection of data resources, etc.);

- Identifies the actions to be taken in order to achieve those objectives (e.g. establishment of incident response centers, adoption of cyber security standards, building consumer awareness, etc.); and

- Sets out the roles and responsibilities of all stakeholders in the process (including a mechanism for information sharing, cooperation and collaboration).⁵

The national cyber security strategy can also place cyber security efforts into the context of other national efforts, such as homeland security and the development of an information society. In many countries, national cyber security strategy is typically promulgated at a high level of government, often by the head of government, in order to get the buy-in of all stakeholders.

⁸² ITU National Cybersecurity/CIIP Self-Assessment Tool, ITU, 2009 <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html>

III.2 The Significant of Cyber Security Strategy

Awareness to develop cyber security and prepare strategies in the face of threats and challenges of cyberspace has long been recognized by the US. However, the intensity of the development of cyber power has been very visible in US government policies in the last 10 years. The following are some of the cyber security policies released by the US government in the last 10 years:

YEARS	DOCUMENT NAME	INSTITUTIONS
2003	The National Strategy to Secure Cyberspace	White House
2009	Cyberspace Policy Review	White House
2011	International Strategy for Cyberspace	White House
2011	Department of Defense Strategy for Operating Cyberspace	US Department of Defense

Table 1 List of US Cyber Security Policies

From the table above it is very clear that the US government is serious in developing cyber security. President Barack Obama in 2009 stated that America's digital infrastructure is a national asset. In May 2010 the Pentagon launched the US Cyber Command (USCYBERCOM) to protect American military networks and carry out attacks. In the government and corporate networks protected by the Department of Homeland Security. To anticipate the cyber war in America was formed DC3 (Defense Cyber Crime Center) in 2008, US Cyber Command (2009), Homeland Security (for non-military), and research to create cyber warfare weapons by DARPA.⁸³

⁸³ Council on Foreign Relations. *Confronting the Cyber Threat*. 2011. <https://www.cfr.org/background/confronting-cyber-threat>

III.2.1 Cyberspace Policy Review

After the expiration of President Bush's administration, Barack Obama took over; Obama became the 56th American President. In the early days of his administration, Obama ordered a comprehensive review of relevant agencies and institutions to maintain information, communication and develop a comprehensive approach to safeguard digital infrastructure. In the United States President Obama in 2009 stated that America's digital infrastructure is a national asset.

The results of a thorough study of the initial administration of President Obama were Cyber Policy Review which was immediately launched that year, which was in 2009. This review analyzes previous policies, observes gaps or shortcomings from the massive to the smallest. As a result, there are still many cybercrime activities both from within the country and abroad. This has resulted in privacy degradation as well as the paralysis of the public sectors where very many people depend on it. For example:⁸⁴

- Critical infrastructure damage: CIA reports that there is dangerous information technology activity that results in disruption to various electric power capacities area;
- Exploitation of public financial services. In November 2008 there were a lot of frauds in transactions through ATM (Automatic Teller Machine) in 49 cities, besides that many US entrepreneurs lost their credit card and debit card identities.
- Systemic losses in the value of the US economy. Industries lost data on intellectual property and estimates a loss of around \$ 1 trillion.

After recognizing these opportunities and challenges, Obama identified that Cyber security was among the top priorities of his administration. This makes sense, because when viewed from this review, Obama is very serious about planning this Cybersecurity Strategy. In this study also discussed what policies will be taken to

⁸⁴ United States of America. *Cyberspace Policy Review. 2009.* Washington: The White House

secure cyber space both from within and outside the country. The strategies of the policy include: ⁸⁵

- Lead through the highest leader;
- Building the nation's digital capacity;
- Sharing responsibilities in cybersecurity;
- Establish an incident response body and share information effectively;
- Encouraging innovation;
- Action plan.

Priority cyber security in the Barack Obama administration includes: ⁸⁶

1. Maintaining the country's important infrastructure and important state information system from cyber threats.
2. Increasing the ability to identify and report cyber events in order to respond at the right time.
3. Inviting the world to promote internet freedom and build support for open, easy to operate, safe and reliable cyber space.
4. Securing the central government network by setting clear security targets and placing accountable government agents to meet these targets.
5. Establish a force that is very understanding of cyber and goes beyond passwords in partnership with the private sector.

⁸⁵ Max Smith. *An Outcome-Based analysis of U.S. Cyber Strategy of Persistence and Defend Forward*. <https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward>

⁸⁶ White House. *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. <https://www.whitehouse.gov/articles/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure/>

In May 2009, the President received a recommendation from the results of this Cyberspace Policy Review, including the selection of a Cybersecurity Executive Coordinator branch that would get full access to the president. Cybersecurity Executive Coordinator will also work with key players in US cybersecurity, including local and state governments, the private sector, Cybersecurity Executive Coordinator will also strengthen public and private cooperation relationships to find new technological solutions to ensure cyber security and prosperity.

III.2.2 International Strategy for Cyberspace

In May 2011, the Obama administration issued an International Strategy for Cyberspace policy: Prosperity, Security, and Openness in a Networked World. This policy is the result of the United States efforts in fight cyber-attacks along with international partners. The principles in this policy are fundamental freedoms, privacy, freedom of information flow which together with the protection of national network security. This policy recommends building norms of international behavior and increasing international cooperation rather than imposing a structure of cyber governance globally. From a series of US policies to secure cyber space, which is very in touch with Foreign Policy is "U.S International Strategy for Cyberspace". This strategy is a special formulation issued by the White House as the US international code of conduct in cyber issues in international relations. The US really understands that the world still does not have a clear arrangement regarding cyber space. This situation is not used by a number of countries to act arbitrarily in cyber space. Some countries detected by the US threaten US national interests through cyber space actions, among others: Chinese and Russian.

This strategy is the first US-issued strategy that connects and ties the US with the rest of the world on a very broad cyber issue. This strategy is also a guide to the US in dealing with all the challenges of information technology security in the cyber space. Therefore in April 2015, the US Department of Defense issued "The

Department of Defense (DoD) Cyber Strategy" to answer what regions and how the US defense agency must succeed the goals and priorities set out in the International Strategy for Cyberspace 2011.

U.S International Strategy for Cyberspace regulates the short and long term US strategy in facing the era of digital war in the world. Through this strategy, the US will pursue international policies for cyber space and empower various innovations that have been proven to drive the progress of the economy and improve the lives of US society and the world community at large. For this reason, the US states that it will stand firm on the basic principles that apply not only to US foreign policy but to the future of the internet itself. Some approaches developed by the US through US cyber space international security strategies include:⁸⁷

Strategic Approach	Building on Successes	The US is committed to maintaining and increasing the benefits of digital networks for society and the economy.
	Recognizing the challenges	The US is aware that the growth of this network has come along with its challenges to the economic security of the State and the global community.

⁸⁷ The White House. *International Strategy for Cyberspace*. May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

	Grounded in Principle	The US will fight all these challenges at the same time also maintain the main principles of the State.
--	-----------------------	---

In order to strengthen the National Strategy, technically the strategy steps have been prepared by the Department of Defense (DoD), which is called the initiative Strategy. This strategy was compiled for cyber security which was the task of the United States Department of Defense. These strategies include;

1. **Strategy initiative 1:** Treat cyber space as an operational area that must be managed, trained and equipped so that the US Department of Defense can exploit the potential of cyber space itself.
2. **Strategy initiative 2:** Develop a new defense operating system to protect the US Department of Defense's systems and networks.
3. **Strategy initiative 3:** Partner with government departments / agencies even with the private sector to implement all cyber space strategies.
4. **Strategy initiative 4:** build strong relationships with US allies and other international partners to strengthen cyber collective security.
5. **Strategy initiative 5:** The Department of Defense will influence the intelligence of the nation with special abilities in the cyber world and very rapid technological innovation (DOD Strategy for Operating in Cyberspace, July 2011).

To support the cyber security mission, the US Department of Defense (DoD) conducts various activities outside the cyber world to develop cyber collective

security and in an effort to safeguard US national interests.⁸⁸ For example, DoD collaborates with government agencies, the private sector, and also with international partners in information exchange, building alliances and partnerships and developing responsible behavioral norms to improve global stability.⁸⁹ In order to support the above activities, 3 (three) main missions of the US Department of Defense for the cyber world are formulated:

1. DoD must maintain its own network, system and information. The Department of Defense must be able to secure its network from attacks and restore the system quickly if security fails.
2. DoD must prepare itself to safeguard the US and all its interests against cyber attacks that give significant importance.
3. By being led by the President and Minister of Defense, DoD must be able to create integrated cyber capabilities to support military operations and plans to be achieved in the future.

These three main missions can be achieved through 5 (five) strategic objectives, including:⁹⁰

1) Strategic Goal I: Build and maintain forces and capabilities to conduct cyberspace operations; To be able to operate effectively in the cyber world, DoD requires the support of individual personnel and soldiers who are trained to high standards. For this reason, DoD must invest heavily in providing training to the army, building effective organizations.

⁸⁸ US Department of State. *Pillars of the International Strategy for Cyberspace*. 2014. <https://2009-2017.state.gov/s/cyberissues/strategy/index.htm>

⁸⁹ The White House. *Launching the US International Strategy for Cyberspace*. May 2011. <https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace>

⁹⁰ US Department of Defense. *Strategic Plan for the next generation of training for the Department of Defense*. http://prhome.defense.gov/Portals/52/Documents/RFM/Readiness/docs/FINAL_NextGenStrategicPlan_23Sep.pdf

2) Strategic Goal II: Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions; DoD must begin by identifying, prioritizing and maintaining the most important networks and data so that they can effectively carry out mission objectives. DoD must continue to develop technology to stay ahead in the face of threats by increasing cyber defense capabilities.

3) Strategic Goal III: Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequences; DoD must work between partners, starting from the private sector, and alliances including partners of other countries to counteract and if necessary cripple cyber attacks that have a significant impact on US interests.

4) Strategic Goal IV: Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages; DoD must establish a cyber system that is sustainable and integrated with relevant institutional plans. DoD will develop cyber capabilities to achieve key security objectives.

5) Strategic Goal V: Build and maintain robust international alliances and partnerships to share shared threats and increase international security and stability.

The three DoD cyber security missions require collaboration with foreign allies and other partners. In attachment to the world of international cyber, DoD must build cooperative capacity in cyber security, cyber defense, and deepen the cooperative relationship.

III.2.3 Presidential Proclamation - National Cybersecurity Awareness Month, 2014

United States President Barack Obama acknowledged that the United States itself is very dependent on information and communication technology both in the

lives of everyday people, the running of government and national defense. Obama is also aware of the dangers posed by this cyber threat, Obama said when American intellectual property was stolen, it would endanger the country's economy, threaten people's lives, state identity, and prevent individual freedom.⁹¹

Judging from the threats and dangers posed by this, Obama as President of the United States proclaimed the month October 2014 as the month of National Cyber security Awareness, so that every level of society can understand and understand information and communication technology not only as users, but also realize the negative impact that can be caused to individuals and countries. On that month of awareness was also supported by cyber security education to the community, so that they would be more sensitive to this network technology.

III.3 United States Executive Orders Agenda

Just as the lives of the collective public have shifted online, so have the systems that power and control the nation's critical infrastructure. In the last 25 years, the move from analog to digital has made work easier and more efficient, according to Michael Assante, director of Industrial Control Systems, Supervisory Control and Data Acquisition Networks. Operators can control systems remotely and oversee various sites, while managers can run refineries and the electrical grid, and control temperatures in nuclear cooling towers, he notes.⁹²

In the same way the everyday individual is at risk for hacking and cyber attacks from a range of actors, so are the systems for the nation's critical infrastructure. National leaders and computer experts warn that it is not a matter of if,

⁹¹ White House. *Presidential Proclamation – National Cybersecurity Awareness Month, 2014*. <https://obamawhitehouse.archives.gov/the-press-office/2014/09/30/presidential-proclamation-national-cybersecurity-awareness-month-2014>

⁹² Assante, Michael. *America's Critical Infrastructure Is Vulnerable to Cyber Attack*. Forbes. November 11, 2014.. <http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructureis-vulnerable-to-cyber-attacks/>.

but when a major cyber attack occurs.⁹³The U.S. government has acknowledged the severity of the threat. In February 2013 President Barack Obama signed an executive order for Improving Critical Infrastructure and Cybersecurity.⁹⁴

III.3.1 Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

In 2011, the US President issued executive orders about structural reforms to improve network security and share responsibility in securing confidential information. There are several parts in this executive order, including:

- Order structural reforms in securing confidential information;
- General agent responsibility;
- Make a senior security committee and share confidential information;
- Build security offices and share confidential information;
- Choose executive security agents and share confidential information on computer networks, in this sections it can be called a spy;
- Hold a task force to deal with threats; According to BBC's report,⁹⁵ which coincides with the announcement of the defense department's new strategy which is also related to the new budget for 2011, that for the military budget in 2011, the US government has budgeted 700 billion dollars, up 2 percent from the previous year.

⁹³ Rainie, Lee, Janna Anderson, and Jennifer Connolly. "Pew Research Internet Project." Pew Research. October 29, 2014. <http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/>

⁹⁴ White House. *Fact Sheet: Cybersecurity National Action Plan*. February 9, 2016. <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.

⁹⁵ Lyne, James. *We Must Resist over-hyping security threat*. 2012. <http://www.bbc.com/news/technology-16320582>

III.3.2 Executive Order 13636 - Improving Critical Infrastructure Cyber Security

After issuing Executive Orders on structural reforms to improve network security and sharing responsibility for securing confidential information, President Obama described the cyber threat as one of the gravest national security dangers.⁹⁶ U.S. national and economic security depend on the nation's critical infrastructure operating in the face of such threats, then in 2013 the US President again issued an Executive Order to increase cyber security in infrastructure that is considered critical / vital. The points of the order include:

- Policy. It is a must for Americans to enhance the security and resilience of the nation's vital infrastructure and keep the cyber environment efficient, innovative, and support the economy, together with promoting security, business confidence, privacy and civil liberties. This goal can be achieved by cooperating with other countries, business owners and infrastructure operators to support cyber security and implement risk-based standards;
- Vital infrastructure. Referring to assets, both physical and virtual, which if exposed to an attack will have an impact on security, national economic security, public health, or a combination of both.
- Policy coordination;
- Share information about cyber security with the country cooperation, between institutions, or with the private sector.
- Privacy and maintaining civil liberties;

⁹⁶ White House. *Executive Order – Improving Critical Infrastructure Cybersecurity*. 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

- Consultative process. The Minister will establish a consultative process to coordinate to improve cyber security;
- Framework for reducing the risk of cyber attacks. The cyber security framework consists of a set of operating standards, methodologies, procedures, and approaches to dealing with the risk of cyber attacks. This framework must also be in accordance with national standards;
- Designing programs that support the adaptation of the cyber security base framework.

III.4 The United States Cyber Security Strategy Implementation

Cyber Attacks can cripple and damage computer and internet network systems so that it has a major impact on the operational continuity of large institutions both state and private. This attack between users of cyberspace is a phenomenon that forms a new war regardless of distance, time, and the culprit actor. Observe the events and phenomena that exist, making countries using cyber networks, especially the United States give a respond by creating organizations to deal with the worst possible consequences of cyber attacks that can cripple and damage network and operational systems.

The formation of cyber organizations is one form of cyber defense strategy and application in anticipation of attacks that can damage and cripple the system. With various strategies issued by the United States related to cyber security, the policy is implemented by several organizations / agencies as an extension of the government in facing the threat of cyber warfare. Many cyber-attacks target the private sector, which does not result in damage to government networks even though the quantity of attacks relatively high.

Supposedly, periodic high-ratio attacks can paralyze a country's information and communication system, for example Estonia and Iran. Estonia and Iran are

examples of countries that were paralyzed by cyber-attacks. The quality of attacks aimed at Estonia and Iran is the same as the attacks that have been carried out in the United States; in fact the quantity is not as high as the attack aimed at the superpower. Estonia and Iran were paralyzed, the United States persisted. With the mastery and utilization of good information and communication technology and supported by its cyber security strategy, the United States has succeeded in securing digital data and its vital infrastructure from the threat of cyber warfare.

The United States cyber security strategy requires cooperation between institutions or agencies both government and private domestic or international cooperation. This collaboration is divided into strategic levels and operational levels. In implementing this cyber security strategy, each agency / agency has their respective roles and functions in the face of cyber warfare threats. This agency / agency have its own task force, operating standards, methods, procedures and programs. So, the success of the United States in securing digital data and its vital infrastructure rests on the performance of these agencies. In fact, the operations of the United States intelligence agencies are a threat to other countries.

III.5 The Structure of Role Model Cyber Security Agencies in the United States Administration

III.5.1 Department of Defense as the Strategic Level Agency

The Department of Defense (DoD) is responsible for running the defense and security of the United States after national policies or foreign policies of the president are established, including defense and cyber security. To create cyber defense and security, DoD as the United States Defense Ministry has five main intelligence agencies called "the big five" and several sub-agencies that run cyber defense and security operations. The five intelligence agencies are independent Central Intelligence Agency (CIA), National Security Agency (NSA), Defense Intelligence

Agency (DIA), National Geospatial Intelligence Agency (NGA) and The National Reconnaissance Office (NRO). The Department of Defense (DoD) serving at the strategic level has five strategic initiatives in cyber defense and security,⁹⁷

1. Treating cyber space as an operational area to coordinate, train and equip themselves so that DoD can take full advantage of the potential of cyber space;
2. Develop a new defense operating system to protect DoD systems and networks;
3. Collaborating with other departments and agencies in the (Department of Homeland Security and some of its subordinate agencies) and the private sector to create intergovernmental cyber security strategies;
4. Building strong relationships with the United States alliance and international partners to strengthen collective cyber security;
5. Give influence to the intelligence of the nation through cyber development and technological innovations that are extraordinarily advanced. The policies taken by this strategic level are policies that are always revised or updated according to the development of cyber warfare threats that will be faced by the United States. Information will be entered as input from intelligence agencies and will then be reviewed and analyzed. If there is a very dangerous threat, a new policy will be issued to overcome the threat. Furthermore, the policies made will be continued and carried out by agencies or agencies that are at the operational level.

III.5.2 US Strategic Command (USSTRATCOM) as an Operational Level Agency

US Strategic Command is a body under the DoD and the parent of the "big five" intelligence agency that runs a level of cyber security and defense operations, USSTRATCOM has duties including:⁹⁸

⁹⁷ Department of Defense United States of America. *Strategy for Operating Cyberspace*. 2011.

1. Carry out the US Department of Defense's Global Information Grid (GIG) operations and defenses;
2. Plan to fight the threat of cyberspace;
3. Supporting the ability of cyberspace;
4. Carry out cyberspace operations;
5. Coordinate with other combatant commands and US government agencies related to problems related to cyberspace.

III.5.3 US Cyber Command (USCYBERCOM) as a Military Cyber Defense Agency

This body is tasked with facilitating the integration of cyberspace operations for military service and synchronizing the defense cyber mission and war effort, and providing support for civil authorities and international partners. In addition to "the big five", elements of US Cyber Command consist of US Army Cyber Command, the Twenty-fourth Air Force / AFCYBER, the US Fleet CyberCommand / US 10th Fleet, and Cyber Command Corps.⁹⁹ The mission from USCYBERCOM is first, planning, coordinating, integrating, synchronizing and carrying out activities for direct operations and defense of the information network of the United States Department of Defense. Second, prepare to be directed towards carrying out full military operations on the cyber spectrum to enable action on all internet domains and ensure the United States and its allies are free from cyber attacks and counteract any cyber attacks from enemies of the United States / Allies.

⁹⁸ GAO. Defense Department Cyber Effort: *DOD Faces Challenges In Its Cyber Activity*. Washington: US Government Accountability Office. 2011.

⁹⁹ PWK International. *Heavy Metals Underpin Asian Arms Buildup*.
<https://pwkinternational.com/page/3/?app-download=blackberry>

III.5.4 National Security Agency (NSA) as the Protector of Vital Information and Infrastructure

The NSA has the duty to collect and analyze communications from other countries, and protect Information belonging to the United States.¹⁰⁰ The NSA coordinates, directs, and carries out very special activities aimed at gathering intelligence information from abroad, especially using cryptanalysis. In addition, the NSA protects government communications and information systems in the US from other agencies, which involve high-level cryptography. The activities of the NSA include tapping and security. NSA intercepts include telephone, Internet communication, radio communications, and other communications that can be tapped. NSA safeguards include military, diplomatic and secret or sensitive communications from the government. The NSA is an organization that employs mathematicians and has the most supercomputers in the world. In cyber warfare, the NSA has a dual role. NSA has a lot of programs and software based on information technology and underground communication that are useful for stealing various data from various parts of the world. One example is XKeyScore.¹⁰¹ XKeyScore is software owned by the NSA to extract information and exploit what you want to know as long as it takes the form of real-time digital data. If you've heard the term "god eye", the eye that can see everything, this XKeyScore is the human version. If a cyber attack occurs, the NSA with all its sophisticated programs and software can counterattack the attacker.

¹⁰⁰ Bulletin of the Atomic Scientists. *Artificial Intelligence and national security*. <https://thebulletin.org/2018/02/artificial-intelligence-and-national-security/>

¹⁰¹ Glenn Greenwald. *Xkeyscore: The NSA files. NSA tool collects 'nearly everything a user does on the internet'*. 2013. <https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>

CHAPTER IV

The Nature of Cyber Security Attack and United States Responses

IV.1 Cyber Security and United States-China Relations

The U.S.-China relationship is among the most important in the world. Both sides draw great benefit from the smooth functioning of the Internet. But the issue of cybersecurity threatens to become a major source of friction. The danger is that the technologies that so connects the world will instead drive these two nations apart. Given what is playing out, it is especially important that Washington and Beijing begin to build the bases for greater mutual understanding, cooperation, and development of common norms in how they deal with the many issues emerging in cybersecurity. Such bilateral efforts certainly should not stand in the way of various multilateral initiatives along similar lines, but focused bilateral dialogue is of great potential value.

There is perhaps no relationship as significant to the future of world politics as that between the U.S. and China. No other two nations play such dominant roles in critical global issues from peace and security to finance, trade, and the environment. How these two powers manage their relationship will likely be a key determinant of not only their own political and economic futures, but also wider global stability and prosperity.

In the web of relationships that have built up between the U.S. and China, no issue has emerged of such importance, and generated such friction in so short a time span, as cybersecurity. Just a generation ago, “cyberspace” effectively did not exist beyond the nascent links among a limited number of university labs’ computer networks. Today, the centrality of cyberspace to our entire global pattern of life is almost impossible to fathom. There are some 4 billion people behind the roughly 50

billion devices that connect to the Internet. They send more than 90 trillion emails a year, and conduct more than two trillion transactions.¹⁰²

Domains that range from commerce to communication to the critical infrastructure that powers and protects our modern day civilization all depend on the safe and secure operation of this globalized network of networks. And yet, concerns over this domain have rapidly moved to the forefront of U.S.-China relations. While both senior policymakers and general publics are struggling to understand the cyber realm's basic dynamics and implications, the issue of cybersecurity is looming ever larger in U.S.-China relations and is seriously affecting threat perceptions on both sides.¹⁰³ Indeed, despite it being such a new issue, the cyber realm is proving to be as challenging as the more traditional concerns that have long dominated the U.S.-China agenda (such as trade, human rights, cross-Strait relations, and regional territorial disputes). The underlying concern is driven by the fact that the malevolent side of cyberspace has increased hand in hand with the growing scale and use of the benevolent side. There are an estimated 55,000 new pieces of malware found each day and another 200,000 computers worldwide turned into "zombies" (compromised computers under the control of an actor other than the owner) each day. These computers are often bundled together into "botnets," chains of thousands and in some cases even millions of computers externally controlled and often used for nefarious activities.¹⁰⁴

But even more important than the growing numbers behind the malicious use of the Internet may be the evolution of the cyber threat landscape from one

¹⁰² "Security in Embedded Devices," McAfee presentation, June 22, 2011.

¹⁰³ Richard D. Fisher, Jr. "Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People's Republic of China (PRC)," Testimony before House Committee on Foreign Affairs, Oversight and Investigations Subcommittee, Hearing on "Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology." April 15, 2011; Larry M. Wortzel. "China's Approach to Cyber Operations: Implications for the United States," Testimony before House Committee on Foreign Affairs, Hearing on "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade." March 10, 2010. Shen Yi, <http://www.globalview.cn/ReadNews.asp?NewsID=22733>

¹⁰⁴ Marc Brown, "Embedded Device Security in the New Connected Era," Electronic Engineering Journal, <http://www.eejournal.com/archives/articles/20110818-windriver/>

dominated by individual hackers, often motivated by a search for attention, to one driven by complex, organized groups, which range from international criminal networks to state-related espionage and military efforts. The result is that just as the positive side of the cyber domain is rippling out into the physical domain with rapid and often unexpected consequences, so too is the negative side.

In any new issue on the international agenda, developing an agreed-upon vocabulary and set of concepts is a requisite step, but one that can require a great deal of time and effort. Whether it is an issue of trade negotiations or nuclear weapons regimes, the basic terms may often seem simple but can prove quite difficult. For example, in one diplomatic meeting between U.S. and Chinese officials, when U.S. representatives first used the term “engagement,” the Chinese were said to be baffled about whether the U.S. meant “marriage proposal” or “exchange of fire.”¹⁰⁵

This issue is even more challenging in the realm of cyber, as it involves both highly technical matters and also concepts where even the most basic terms can be loaded with meaning. There may have been debate about what met the definition of a cruise missile, for example, in talks between the U.S. and USSR, but there was no dispute as to whether it was a weapon or not. The same cannot be said about even such notions as “information” in the cyber realm. The provision of news on protests in the Middle East or the connections built across geographic borders via social networking tools have been described by one side as not just begin, but an essential human right.¹⁰⁶ By contrast, the very same thing has been described by the other side as part of an “information attack” designed to undermine state stability.¹⁰⁷ Similarly, “cyber-terrorism” has been used to describe everything from theoretic use of the

¹⁰⁵ King Jr., N. and J. Dean (Dec. 7, 2005). Untranslatable Word in U.S. Aide’s Speech Leaves Beijing Baffled; Zoellick Challenges China To Become ‘Stakeholder’; What Does that Mean? The Wall Street Journal.

¹⁰⁶ Hillary Rodham Clinton, “Remarks on Internet Freedom,” January 21, 2010, <http://www.state.gov/secretary/rm/2010/01/135519.htm>

¹⁰⁷ Dmitri Alperovitch, and Ralph Langner. Transcript of “Deterrence in Cyberspace: Debating the Right Strategy with Ralph Langner and Dmitri Alperovitch.” Washington, DC, September 20, 2011. Alperovitch references discussions with the Chinese Foreign Ministry where they declared that rumor spreading on Facebook that causes social unrest in China would be considered a cyber attack.

Internet by terrorist groups to cause physical damage (such as by disrupting the operations of an air traffic control network) to the actual use of the Internet by terrorist groups to recruit members and share information on tactics and operational planning.¹⁰⁸

A related problem is in differentiating between activities and intent in this space. Too often, the wide array of cyber activities that differ in nature and should be thought through separately are bundled together in discussions of cybersecurity. Take the notion of what constitutes an “attack.” In both private discussion and public documents, a variety of like and unlike efforts have all been described as “cyber attacks” simply because they involve the technology of the Internet at some point.¹⁰⁹ The parallel for lumping together any and all malicious activity in the digital realm as similar “attacks” would be to treat the threat posed by a teenager with a bottle rocket, a robber with a revolver, an insurgent with a bomb and a state with a cruise missile as the same phenomenon simply because they all involve the same chemistry of gunpowder.

In essence, cyber attacks involve finding vulnerabilities in computers and computer networks, entering into such networks, and then copying and exporting information from such networks, and/or changing information within such networks. The problem is that this relatively simple notion can encompass a very wide array of actions and results. In a “denial of service attack,” the targeted system is not actually penetrated. Rather, it is simply flooded with so many requests from other networks (often botnets manipulating hijacked computers from around the world) that it is overwhelmed and effectively ceases operations. A metaphor would be if the door of

¹⁰⁸ FBI distinguishes mere terrorist use of information technology from a terrorist attack coupled with the use of the Internet—only the later is considered “cyberterrorism.” Evan Kohlmann broadened the definition because, in his view, the online terrorism community overlaps with the real-world one. Keith Lourdeau, “Testimony before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security,” February 24, 2004, <http://www2.fbi.gov/congress/congress04/lourdeau022404.htm> Eben Kaplan, “Terrorists and the Internet,” Council on Foreign Relations, last modified January 8, 2009, <http://www.cfr.org/terrorism-and-technology/terrorists-Internet/p10005>

¹⁰⁹ See for example, William Lynn, “Defending a New Domain,” Foreign Affairs, Oct. 2010, <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-anew-domain>

one's house was never broken down, but so many unwanted people tried to get in that legitimate guests could not make it through.

The cause of such an overwhelming number of requests to enter, though, can vary. It could be anything from unintended poor network management to more purposeful actions like criminal blackmail (groups have threatened such attacks in a form of extortion), political protest (such as recent “Anonymous” group efforts to target companies and institutions it felt were not supportive of Wikileaks)¹¹⁰ or even strategic goals in the context of a more traditional armed conflict (such as the targeting of Georgian websites during its war with Russia, which limited the Georgian government's ability to communicate with its own populace and international parties).¹¹¹ What is more, such denial of service “attacks” are actually one of the most manageable forms of malicious activity, but even they can also serve as part of a broader strategic action—e.g., to multiply the effects of an accompanying attack on infrastructure.

The goals and consequences of attacks that actually enter into a network also widely vary. The goal might be mischief; hackers might be simply “showing off” that they can do so. Or, it might be for criminal reasons, such as to gain components of one's online identity (personal data, passwords, etc.) to use in identity theft crimes, the creation of false accounts and unauthorized transfers of money. A particularly notable area is espionage-like efforts to gain entry into cyber systems in order to monitor activities there and to extract information. Organizations that have suffered from such entries range from governmental diplomatic bodies to international athletic monitoring organizations. In these cases, the information being monitored and stolen has been strategic. Or, the information might be intellectual property, such as a proprietary product or design, which might have great economic or even national

¹¹⁰ Robert Mackey, “‘Operation Payback’ Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks,” New York Times, December 8, 2010, <http://thelede.blogs.nytimes.com/2010/12/08/operation-payback-targets-mastercard-and-paypal-sitesto-avenge-wikileaks/>.

¹¹¹ John Markoff, “Before the Gunfire, Cyberattacks,” New York Times, August 12, 2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html>

security value. Or, it might be companies preparing their negotiation strategy against a foreign, often state-run, company. Entities that have suffered from such attacks range from consumer goods companies that have seen their designs replicated without payment to oil companies that have had their bidding strategy and drilling secrets taken to aerospace companies that have seen designs of combat aircraft stolen.¹¹² In short, the expansion of digital data creation, storage and transmission has created an espionage bonanza for both public and private actors—one that is being exploited to a startling degree.

Indeed, while the focus of U.S. debate is more frequently on fears of a so-called “digital Pearl Harbor,” as described by Secretary of Defense Panetta in his 2011 confirmation hearings, the more serious problem may actually be a long-term economic “death by a 1000 cuts.” Finally, the “attack” might involve not merely entering the system and extracting information, but also changing information within it. Here, too, the goals and consequences might vary widely. Again, the effect might be mere vandalism for mischief or for political purposes, such as defacing a public-facing website of a government institution (which happened in the aftermath of the April 2001 EP-3 incident with China).¹¹³ It might be in the aid or execution of some sort of criminal endeavor, such as changing access or identities to allow criminals through security barriers. Or, it might seek to cause major harm of a strategic nature, such as damaging another country’s ability to implement official decisions, to defend itself, or to provide necessary services to its citizens (such as delivery of electric power, health care, etc.). While relatively untested, the types of harms that might result from serious cyber attacks conceptually range from disrupting the adversary’s electronic systems and what operations they enable (communications, guidance systems, radar capabilities, etc.) to actual kinetic damage accomplished by using cyber tools to cause an adversary’s systems to malfunction or self destruct. A

¹¹² Christopher Drew, “Stolen Data Is Tracked to Hacking at Lockheed,” New York Times, June 3, 2011. <http://www.nytimes.com/2011/06/04/technology/04security.html>

¹¹³ Christopher R. Hughes and Gudrun Wacker, *China and the Internet: Politics of the Digital Leap Forward* (London: Routledge, 2003), 145.

particular worry is those that target infrastructure; for example, actions that remotely open the sluice gates of dams or shut down regional power grids.¹¹⁴ Here too, the intent and the originator of the attack matters. Planting malware that degrades the functioning of a physical plant (the most famous example is the Stuxnet virus against the centrifuges in Iran’s nuclear program)¹¹⁵ has been interpreted as everything from an act of “cyber terrorism,” to an act of “cyber war,” to a lawful activity to enforce international norms in a targeted way that limits loss of life.¹¹⁶ The “attack” remains in the eye of the beholder. Such questions of definitions and terms are hugely important in policy discussion. Actors can use the same terms but with a vastly different meaning (sometimes intentional—such as via the phenomenon of threat hyping by organizations, bureaucracies, companies, and individuals that might benefit from greater levels of investment in cybersecurity).¹¹⁷ But the issue of terms also has importance in domestic and international law. States regularly define the boundaries of criminal activity differently and also attach different degrees of punishment to the same activity. Liberal democracies, for example, tend to view the internet as a place that should maximize freedom of expression, while more authoritarian states do not presume freedom of expression as a basic right. But the issue is even more complex. For example, the democracies of NATO are deeply aligned on many such issues but could not come to agreement in their own talks over a cyber crime treaty. One of the key issues was that to deny the Holocaust online is a crime in many European states, but not in the US. The U.S. and China relationship is critical both to the Internet and its billions of users, as well as to overall global order

¹¹⁴ William J. Broad, John Markoff and David E. Sanger, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay,” *New York Times*, January 15, 2011, <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all>

¹¹⁵ Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 198

¹¹⁶ George R. Lucas, Jr. “Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets.” Presentation at Society of Philosophy and Technology conference, University of North Texas, May 28, 2011.

¹¹⁷ Jerry Brito and Tate Watkins, “Loving the Cyber Bomb: The Dangers of Threat Inflation in Cyber Policy,” *MercatusCenter Working Paper*, April 2011, http://mercatus.org/sites/default/files/publication/WP1124_Loving_cyber_bomb.pdf

beyond the world of cyberspace. If these two nations are to set both realms towards a more positive future, then facing the challenges of cyber security is an imperative today.

IV.2 Cyber Security and United States-Russia Relations

Russian and American experts take different approaches on the problems associated with cyberspace. American notions of “cyber security” and “cyberspace” imply technological understanding; the primary goal of cyber security is to keep technologies safe from disruption, unauthorized access, or other kinds of interference. According to the U.S. International Strategy for Cyberspace, the challenges come in a variety of forms:

Natural disasters, accidents, or sabotage can disrupt cables, servers, and wireless networks on U.S. soil and beyond. Technical challenges can be equally disruptive, as one country’s method for blocking a website can cascade into a much larger, international network disruption. Extortion, fraud, identity theft, and child exploitation can threaten users’ confidence in online commerce, social networks and even their personal safety. The theft of intellectual property threatens national competitiveness and the innovation that drives it.

Cyber security threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace.”¹¹⁸ The Russian position on information security is outlined in recent Russian foreign policy documents:

Russia will act according to its national interests in providing national and international information security, preventing political, economic and social security threats emerging in cyberspace, to fight terrorist and other criminal kinds of criminal activity. Russia opposes military political use of information technologies that contradict international law, including actions aimed at interference in domestic

¹¹⁸ U.S. officials, “International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World,” released by the White House in May 2011, p. 4.

affairs, as well as that kind of using IT that pose threat to international peace, security and stability.¹¹⁹

For Russians, the more common terms, “information security” and “information space,” also have philosophical and spiritual meanings. For instance, the term “noosphere” was introduced almost 100 years ago by the famous Russian philosopher Vladimir Vernadsky to explain the sphere of knowledge and information that exists on Earth along with the biosphere and the geosphere. Technology is one of many elements of Russians’ understanding of information security, and not necessarily the most important one. For Russia, “information security” also aims to keep the nation’s knowledge and culture safe. Indeed, Russia’s 2000 “Doctrine of Information Security of the Russian Federation” does not even contain the word internet. According to the doctrine, information security refers to the maintenance of national security interests, but those interests include the interests of citizens, society, and the government. According to this definition, information security includes the free flow of information that promotes civil society and all kinds of spiritual and educational development and the maintenance of social and moral stability. It also necessitates government engagement in IT development to provide for and protect the constitutional rights of the population. The official Russian position on information security continues to evolve. Russian Presidents Dimitry Medvedev and Vladimir Putin have repeatedly declared that the development of information technologies is a national priority. In a 2008 document, “Information Society in Russian Federation Development Strategy,” Russian government officials stated that they want to make Russia one of the top 20 information societies in the world before 2015.

The Potential for Cooperation

¹¹⁹ The Foreign Policy Concept of the Russian Federation, approved by the President of the Russian Federation Vladimir Putin, February 12, 2013.
<http://mid.ru/bdomp/nsosndoc.nsf/e2f289bea62097f9c325787a0034c255/c32577ca0017434944257b160051bf7f>

The United States has a special role in cyberspace. Due to historical circumstances, the United States leads in the majority of relevant production indicators (global share of patents, technology education, consulting services, etc.) and in the export of information goods and services. It also controls many of the mechanisms for governing the global cyber domain. The importance of the United States in cyberspace is one of the reasons why Russian interests in this area are strongly interconnected with bilateral Russian-U.S. relations, as well as with American global foreign strategy.

According to Russian officials, the United States has long conducted military R & D programs in cyberspace that have raised serious concerns for other international actors, including Russia.¹²⁰ Since the beginning of the twenty-first century, Russia has repeatedly tried to initiate a resolution in the U.N. General Assembly, “Developments in the Field of Information and Telecommunications in the Context of International Security,” aimed at addressing these concerns. The resolution would create an international legal framework, based on the principles of non-use of force, non-interference in domestic affairs, and respect for human rights and fundamental freedoms, and would aim to prevent the use of information and telecommunications in violation of the U.N. Charter. The U.S. has consistently opposed the resolution in part because of “a lack of shared understanding regarding international norms pertaining to State behavior in cyberspace.” This lack of understanding, the U.S. believes, “argues for the elaboration of measures designed to enhance cooperation and build confidence, reduce risk or enhance transparency and stability.”¹²¹ Since President Barack Obama took office, cyber security has remained a national security priority, but Washington has ceased to strive for global information dominance, whereby the United States would pursue both qualitative and quantitative superiority of cyber capabilities, and the ability to govern global

¹²⁰ Interview with Sergey Ryabkov, Deputy Minister of Foreign Affairs, VPK-News, March 14-20, 2012. http://vpk-news.ru/sites/default/files/pdf/VPK_10_427.pdf.

¹²¹ United Nations, “Developments in the Field of Information and Telecommunications in the Context of International Security,” Blue Book Study Series, No. 33, 2001, p. 38.

technological development. Indeed, the Obama administration's adoption of an "International Strategy for Cyberspace," and of multiple bilateral and multilateral initiatives demonstrates Obama's different approach. Among the administration's initiatives is the bilateral Russian-American Agreement on Information Security that is being prepared jointly by high-level U.S. and Russian national security officials.¹²² The very fact that such a document is being discussed on such a high level means that Russia and the United States recognize that they share common interests in cyberspace. Yet, U.S. contributions to the agreement do not address potential military cyber security issues. Given the development of U.S. cyber capabilities, Russia is concerned that U.S. officials consider Russia a primary source of cyber threat. Supporting this notion are comments by U.S. officials. In 2012, Director of National Intelligence James Clapper assessed the cyber threat to the United States, saying, "Among state actors, China and Russia are of particular concern."¹²³

One possible way for Russia and the United States to cooperate in cyber security would be in establishing international norms that would effectively deter other actors from engaging in disruptive, destructive, or illegal behavior in cyberspace. Russian and American decision-makers together face the challenge of adapting to the ever-evolving nature of international politics.

Ensuring national security and maintaining international stability are increasingly defined by factors such as the role of information technologies. Attempts by the United States and Russia to work together to deter cyber-attacks would be complicated by several circumstances:

- Information resources cannot be fully controlled by the governments; in other words, the unauthorized use of cyber weapons is very likely;

¹²² A 2011 joint statement by U.S. cybersecurity coordinator Howard Schmidt and Russian National Security Council Deputy Secretary Nikolay Klimashin outlines some of the work of the group. Joint Statement, "U.S. and Russian Delegations Meet to Discuss Confidence Building Measures in Cyberspace," June 21-23, 2011. http://www.whitehouse.gov/sites/default/files/uploads/2011_klimashin_schmidt_cyber_joint_statement.pdf.

¹²³ James R. Clapper, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community," Senate Select Intelligence Committee," January 31, 2012.

- The potential for nonstate actors' to engage in information warfare can exceed that of states; and
- The lack of regulation containing the military exploration of cyberspace has the potential to turn efforts aimed at protecting economic competitiveness into a cyber-arms race.

Still, Russia and the United States should continue developing their bilateral relations in this area. Establishing reliable cooperation is the only way to counter criminal and terrorist threats in cyberspace, as well as those posed by states.

CHAPTER V

Conclusion

The Cyber Attack can have Long-term and Short-term period's bases on the case. The Department of Defense (DoD) will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. DoD will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. DoD will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. DoD will collaborate with their interagency, industry, and international partners to advance their mutual interests.

Cyber warfare has become a threat that is equally dangerous with the threat of physical warfare for the United States. Attacks carried out through cyber space are able to paralyze vital infrastructure, information systems, so that they can destabilize the government's credibility and ultimately threaten state sovereignty. Demands for cyber security are increasing due to the threat of cyber warfare. To create a cyber security strategy is needed. At this point the United States cybersecurity strategy plays an important role in securing vital infrastructure, assets, banking, and the internet network.

Many cyber attacks launched against the United States can be seen from examples of incidents that have been described before, ranging from the private sector to the government sector but on a smaller scale that is harmless or worrying. The quantity difference of cyber attacks in the private sector and government is due to the implementation of America's cybersecurity strategy that is too focused on the government. The reason is very simple, if a country the size of the United States is easily penetrated through cyber attacks, then the United States is not a country that deserves the superpower's nickname again. America does not want to lose prestige as

a superpower, it will look weak in bargaining positions in the international world and all its secrets will be revealed. So from that the United States emphasized cybersecurity strategy in the government sector. Even though the United States emphasizes cybersecurity in the government sector, it does not mean that the private sector's cyber security is weak. For other countries, it still looks strong to them. It's just that the name cyber technology certainly has a gap even though it's as strong as any security.

The mastery of Underground Information and Communication Technology (ICT) or deep web networking technology and with advanced equipment by the United States as the implementation of the cybersecurity strategy has yielded results. Of the many cyber warfare threats, both threats to the government and private sectors, the United States has succeeded in securing digital data from various vital infrastructures. This can be proven by the absence of big chaos as it should if a vital infrastructure is threatened and there is no paralysis of the government system that impedes the running of the government. On the contrary, the United States is carrying out counter attacks. America implements underground ICT as a tool from the cybersecurity strategy to conduct cyber espionage through its intelligence agency, the big five, brought by USCYBERCOM. The five intelligence agencies comprise the National Security Agency (NSA), Defense Intelligence Agency (DIA), National Geospatial Intelligence Agency (NGA) and The National Reconnaissance Office (NRO) and independent Central Intelligence Agency (CIA).

The five intelligence agencies are the operational level of implementing the strategy, where the strategic level is played by the Department of Defense (DoD). Policies at the strategic level give rise to strategic thoughts in the form of doctrines which are then responded to at the operational level in the form of tactic, technical, and operational actions to control cyber development in the country. Collaboration and integration of these two levels are the main capital in facing the threat of cyber warfare and securing the vital infrastructure of the government itself. It can be said

that this collaboration has a dual role, acting as a United States cyber security guard, also acting as an attacker in cyber warfare.

Bibliography

1. Isle of Man, *National Cyber Security Strategy 2018-2022*. GD 2018/0029. Page 0008.
2. US Department of Defense. *The Department of Defense Cyber Strategy*, April 2015.
3. David J. Betz and Tim Stevens. *Cyberspace and the State, Toward a strategy for cyber-power*.
https://www.academia.edu/1150127/Cyberspace_and_the_State_Toward_a_Strategy_for_Cyber-Power
4. Zaryn Dentzel. *How the Internet has changed everyday life*.
<https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/>
5. Darrell M. West. *Technology and the Innovation Economy*. October 19, 2011.
<https://www.brookings.edu/research/technology-and-the-innovation-economy/>
6. Department of Defense. *DoD Cyber Strategy (April 2015)*. 2015.
<https://www.hsdl.org/?abstract&did=764848>
7. Daniel Rostrup. *Applying Connectivity to deliver the United States sustainable development goals*. 24 October 2018. <https://www.avantiplc.com/blog/applying-connectivity-to-deliver-the-unsustainable-development-goals/>
8. Polaris. *Cyberspace as American Culture*. <http://polaris.gseis.ucla.edu/pagre/sac.html>
9. Aaron Smith, Pew Research Center. *Americans and Cybersecurity*. January 26, 2017.
<http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/>
10. Hannes Ebert & Tim Maurer. *Cyber Security*. January 2017. DOI: 10.1093/OBO/9780199743292-0196
<HTTP://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0196.xml>
11. White House. *National Cyber Strategy. 2018*. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
12. United Nations. 2016. *Cybersecurity Demands Global Approach*.
<http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demandsglobal-approach.html>
 - ˆ Wallace, I. 2013. *The Military Role In National Cybersecurity Governance*. Brookings.
<http://www.brookings.edu/research/opinions/2013/12/16-military-role-national-cybersecurity-governance-wallace>
 - ˆ Demetri Sevastopulo in Washington September 4, 2007. *Chinese hacked into Pentagon*. *Financial Times*. <https://www.ft.com/content/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac>
 - ˆ SCADA's Official website. *What is SCADA*.
<https://inductiveautomation.com/resources/article/what-is-scada>
 - ˆ Takepart journalism observation. *Here's what a Cyber Attack would like in America*. August 23, 2016. <https://www.youtube.com/watch?v=ZkoenqCGiOs>
 - ˆ Langner. *When will we see Stuxnet & Nitro Zeus attack against Iran*. October 8, 2018.
<https://www.langner.com/2018/10/when-will-we-see-another-stuxnet-nitro-zeus-attack-against-iran/>
 - ˆ George Aquila. *The Stuxnet Worm - The Nexus of Cyber Security and International Policy*.
<http://www.cs.tufts.edu/comp/116/archive/fall2013/qaquila.pdf>
 - ˆ Hirschfeld, Julie Davis, and David Sanger. *Obama and Xi Jinping of China Agree to Steps on Cybertheft*. *The New York Times*. September 25, 2015.
http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-whitehouse.html?_r=0
 - ˆ John Markoff, November 9, 2007. *Cyber attack on U.S. nuclear arms lab linked to China*. *The New York Times*. <https://www.nytimes.com/2007/12/09/world/americas/09iht-hack.1.8653712.html>

- USCC.gov. *Report of the U. S. -China Economic and Security Review Commission 2008*. November 2008. Section *The Impact of China's Space Program on U.S. Security* Page 162. https://books.google.co.id/books?id=Cs8dD6Woz4sC&pg=PA162&lpg=PA162&dq=china+20+terabytes&source=bl&ots=372k8RVhbO&sig=dI4J5ZiIA8VkPZNgTxBE2BhQTHQ&hl=en&sa=X&ved=2ahUKEwi_mpb2_OHfAhVJv48KHdGECWAQ6AEwAnoECAGQAQ#v=onepage&q=china%20%20terabytes&f=false
 - Cyber Operations Tracker. *Titan Rain*. August 2005. <https://www.cfr.org/interactive/cyber-operations/titan-rain>
 - Richard Norton-Taylor. *Titan Rain – how Chinese hackers targeted Whitewall*. September 5, 2007. <https://www.theguardian.com/technology/2007/sep/04/news.internet>
 - Josh Rogin. *DOD issues new policy on electronic warfare*. FCW. , February 26, 2007. https://fcw.com/articles/2007/02/26/dod-issues-new-policy-on-electronic-warfare.aspx?admgarea=TC_Policy
 - A Tech Talk Show Record, 25 February, 2007. *Trends in Cyber Warfare*. <http://techtalk.stratford.edu/2007/02/25/show-of-2-25-2007/>
 - RAND Corporation. *The U.S.-China Cyberwarfare Capabilities*, Page 259. 2015. https://www.jstor.org/stable/10.7249/j.ctt17rw5gb.19?seq=1#metadata_info_tab_content_s
 - The White House. *Remarks by the President on Securing Our Nation's Cyber Infrastructure*, May 29, 2009. <https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>
 - Statement for the Record, The Honorable Eric Rosenbach. Assistant Secretary for Homeland Defense and Global Security and Principal Cyber Advisor to the Secretary of Defense, U.S. Department of Defense.
- 13. The Honorable James R. Clapper, Director of National Intelligence. *Senate Select Committee on Intelligence – IC's Worldwide Threat Assessment Opening Statement*. February 9, 2016. https://www.dni.gov/files/documents/2016-02-09SASC_open_threat_hearing_transcript.pdf
- 14. Department of Justice press release “*Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector*”. 24 March 2016. <https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged>
- 15. U.S. Department of State. *The North Korean Threat: Nuclear, Missiles and Cyber*. 13 January 2015. testimony before the House Foreign Affairs Committee by the Special Representative for North Korea Policy - Director of National Intelligence. *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07. Additional reports are located at the website of the National Counterintelligence and Security Center*.
 - Steve Winterfeld and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. ISBN-13: 978-0124047372 ISBN-10: 0124047378. 2011. <https://www.amazon.com/Basics-Cyber-Warfare-Understanding-Fundamentals/dp/0124047378>
 - U.S. Army Command and General Staff College. *United States Cyber security Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?*. ISBN:1500750247 9781500750244. USA, 2014. <https://dl.acm.org/citation.cfm?id=2692572>
 - Edward Griffor. *Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems*. ISBN-13: 978-0128037737 ISBN-10: 0128037733.

<https://www.amazon.com/Handbook-System-Safety-Security-Management/dp/0128037733>

16. Cristin Flynn Goodwin and J. Paul Nicholas. *Developing a National Strategy for Cybersecurity*, Foundation for Security, Growth, and Innovation. October 2013. http://download.microsoft.com/download/b/f/0/bf05da49-7127-4c05-bfe8-0063dab88f72/developing_a_national_strategy_for_cybersecurity.pdf
17. Perwita, Anak Agung Banyu & Yani, Yanyan A. *Pengantar Ilmu Hubungan Internasional*. 2005. Page 119.
18. Perwita, Anak Agung Banyu & Yani, Yanyan A. *Pengantar Ilmu Hubungan Internasional*. 2005. Page 121.
19. Sujarweni, V. Wiratna. *Metode Penelitian: Lengkap, Praktis, dan Mudah Dipahami*. 2014. Page 10.
20. Winarno, Budi. *Dinamika Isu-isu Global Kontemporer*. 2014. Page 11.
21. Mas'ood, Mochtar. *Studi Hubungan Internasional, Tingkat Analisis dan Teorisi*. 1989. Page 90
22. Mas'ood, Mochtar. *Studi Hubungan Internasional, Tingkat Analisis dan Teorisi*. 1989. Page 90-91
23. Buzan, Barry. *Security: A Framework for Analysis*. Boulder: Lynne Reinner Publishers. 1998.
24. Hansen, Lene. *Digital Disaster, Cyber Security, and the Copenhagen School*. International Studies Association. 2009.
25. Bloomberg BNA. *U.S. Has second strongest Cybersecurity in the World, UN Reports*. July 14, 2017. <https://www.bna.com/us-second-strongest-b73014461766/>
26. Pew Research Center. *Cyber Attacks Likely to Increase*. October 29, 2014. <http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/>
27. DSB Task Force on "Resilient Military Systems and the Advanced Cyber Threat;" January 2013. <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>
28. Techopedia. *Threat*. <https://www.techopedia.com/definition/25263/threat>
29. Defense Science Board Task Force on Cyber Supply Chain. November 2016.
30. DCAF, Diplomacy.edu. *Cybersecurity: issues, actors, and challenges*. Page 1. https://www.diplomacy.edu/sites/default/files/Cybersecurity_briefing_note_final.pdf
31. DCAF, Diplomacy.edu. *Cybersecurity: issues, actors, and challenges*. Page 1. https://www.diplomacy.edu/sites/default/files/Cybersecurity_briefing_note_final.pdf
32. DCAF, Diplomacy.edu. *Cybersecurity: issues, actors, and challenges*. Page 2. https://www.diplomacy.edu/sites/default/files/Cybersecurity_briefing_note_final.pdf
33. Department of Defense. *Cybersecurity and the Risk Management Framework*. Slide 2. <https://www.slideserve.com/yerial/cybersecurity-and-the-risk-management-framework>
34. Webology. *International Actions against Cybercrime: Networking Legal Systems in the Networked Crime scene*. September 2007. <http://www.webology.org/2007/v4n3/a45.html>
35. Artur Appazov. *Legal aspects of Cybersecurity*. 2014. http://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Leqal_Aspects_of_Cybersecurity.pdf
36. DCAF, Diplomacy.edu. *Cybersecurity: issues, actors, and challenges*. Page 1. https://www.diplomacy.edu/sites/default/files/Cybersecurity_briefing_note_final.pdf
37. DCAF, Diplomacy.edu. *Cybersecurity: issues, actors, and challenges*. Page 1. https://www.diplomacy.edu/sites/default/files/Cybersecurity_briefing_note_final.pdf
38. Tech Target. *Definition of Hacker*. <https://searchsecurity.techtarget.com/definition/hacker>

39. John H. Dexter. *The Cyber Security Management System: A Conceptual Mapping*. <https://www.sans.org/reading-room/whitepapers/basics/cyber-security-management-system-conceptual-mapping-591>
40. Cosmic. *Signals and Space Monthly Cyber Security Briefing*. April 2017. <http://cosmicaes.com/newsletter-2/newsletter2/>
41. Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidang*. 2012. Jakarta: PT. Tatanusa.
42. Cristin Flynn Goodwin & J. Paul Nicholas (Microsoft). *Developing a National Strategy for Cybersecurity, Foundation for Security, Growth, and Innovation*. October 2013. Page 3
43. Ghernaouti, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. 2013. Page 329. Lausanne: EPFL Press.
44. Ghernaouti, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. 2013. Page 330. Lausanne: EPFL Press.
45. Ghernaouti, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. 2013. Page 330. Lausanne: EPFL Press.
46. Internet Society. *Brief History of the Internet*. 1997. <https://www.internetsociety.org/internet/history-internet/brief-history-internet/>
47. Britannica. *ARPANET; United States Defense Program*. <https://www.britannica.com/topic/ARPANET>
48. Ghernaouti, Solange. 2013. *Cyber Power : Ghernaouti, Solange. Cyber Power :Crime, Conflict and Security in Cyberspace. Lausanne: EPFL Press*. 2013. Page 126.
49. Martin, Jeremy. *The beginner's Guide to The Internet Underground*. Information Warfare Center. 2013.
50. Bitcoin. <https://bitcoin.org/en/>
51. Darkwebnews. *Deep Web: What is it and how to access it?* <https://darkwebnews.com/deep-web/>
52. UNODC. *Cybercrime as a Transnational Crime*. <https://www.unodc.org/unodc/en/cybercrime/index.html>
53. Military Factory. *Secret Internet Protocol Router Network Definition (US DoD)*. https://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=4771
54. CHIPS. *CIWT Assumes Cyber Mission Force Training Role*. <https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=10830>
55. Department of Defense, *Department of Defense Cyber Strategy Summary 2018*. Page 1
56. According to the results of the interview with Dr. Yono Reksoprodjo, this context has caused the cyber domain to fall into the "asymmetrical" category.
57. The RAND. *Cyber-security threat characterization*. 2013. https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR235/RAND_RR_235.pdf
58. Erica Borghard. *Protecting Financial Institutions Against Cyber Threats: A National Security Issue*. September 2018. <https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324>
59. Cristin Flynn Goodwin & J. Paul Nicholas. *Developing a National Strategy for Cybersecurity, Foundation for Security, Growth, and Innovation*. October 2013. Page 4.
60. Patrick. *US, China Among 15 Countries agreeing UN Charter Applies in Cyberspace*. 2013. <http://cnsnews.com/news/article/us-china-among-15-countries-agreeing-un-charter-appliescyberspace#sthash.v9G5beB4.dpuf>
61. Wilshusen, Gegory C. *Cybersecurity Threat Impacting the Nation*. GAO Report of US-CERT. 2014.
62. Council on Foreign Relations. *Confronting the Cyber Threat*. 2011. <https://www.cfr.org/backgrounder/confronting-cyber-threat>

63. United States of America. *Cyberspace Policy Review*. 2009. Washington: The White House
64. Max Smith. *An Outcome-Based analysis of U.S. Cyber Strategy of Persistence and Defend Forward*. <https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward>
- ¹White House. *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. <https://www.whitehouse.gov/articles/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure/>
65. The White House. *International Strategy for Cyberspace*. May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
66. US Department of State. *Pillars of the International Strategy for Cyberspace*. 2014. <https://2009-2017.state.gov/s/cyberissues/strategy/index.htm>
67. The White House. *Launching the US International Strategy for Cyberspace*. May 2011. <https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace>
68. US Department of Defense. *Strategic Plan for the next generation of training for the Department of Defense*. http://prhome.defense.gov/Portals/52/Documents/RFM/Readiness/docs/FINAL_NextGenStrategicPlan_23Sep.pdf
69. Department of Defense United States of America. *Strategy for Operating Cyberspace*. 2011.
70. GAO. *Defense Department Cyber Effort: DOD Faces Challenges In Its Cyber Activity*. Washington: US Government Accountability Office. 2011.
71. PWK International. *Heavy Metals Underpin Asian Arms Buildup*. <https://pwkinternational.com/page/3/?app-download=blackberry>
72. Bulletin of the Atomic Scientists. *Artificial Intelligence and national security*. <https://thebulletin.org/2018/02/artificial-intelligence-and-national-security/>
73. Glenn Greenwald. *Xkeyscore: The NSA files. NSA tool collects 'nearly everything a user does on the internet'*. 2013. <https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>
74. Assante, Michael. *America's Critical Infrastructure Is Vulnerable to Cyber Attack*. Forbes. November 11, 2014.. <http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/>.
75. Rainie, Lee, Janna Anderson, and Jennifer Connolly. "Pew Research Internet Project." Pew Research. October 29, 2014. <http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/>
76. White House. *Fact Sheet: Cybersecurity National Action Plan*. February 9, 2016. <https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.
77. Lyne, James. *We Must Resist over-hyping security thread*. 2012. <http://www.bbc.com/news/technology-16320582>
78. White House. *Executive Order – Improving Critical Infrastructure Cybersecurity*. 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>
79. White House. *Presidential Proclamation – National Cybersecurity Awareness Month, 2014*. <https://obamawhitehouse.archives.gov/the-press-office/2014/09/30/presidential-proclamation-national-cybersecurity-awareness-month-2014>
80. Paletta, Damien. *NSA Chief Says Cyberattack at Pentagon Was Sophisticated, Persistent*. The Wall Street Journal. September 8, 2015. <http://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-was-sophisticated-persistent-1441761541>

81. The Cyber Research Databank. *Top 10 Countries Best Prepared Against Cyber Attacks*. <https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/>

Appendix: