CHAPTER III

U.S. GOVERNMENT PERSPECTIVE ONCYBERSECURITY ISSUES

Realizing the shifting trends of security issues used to be believed only being dynamic in traditional security context such as war and peace has become quite irrelevant in present time. In fact, the globalization is a widespread phenomenon and technology which becomes one of its aspects also gives much impact in facilitating our life ranging from as a platform in socializing with people around the world to help our government in managing many of critical sectors that are important to our daily life.

However, like two sides of coin, the assistance of globalization and technological advancement do not only bring good impacts, but also challenges towards the security issues including in the matter of cybersecurity issues. Many states had realized the fact about the importance of cybersecurity to serve the state in conducting its statehood businesses. It includes one of world hegemons, United States of America.

Thus, this chapter will specifically focus on providing the analyses within the discussion of how U.S. as one of the states that holds major power in world nowadays is seeing the issue of cybersecurity, especially in term of critical infrastructures which are comprised of many sectors that serve the needs of American citizens. Further, this chapter will also examine the comparison between Obama Administration and his predecessor in Bush Administration. This comparison is necessary to identify the facts such as environmental factors, dilemma or leadership style of both U.S. leaders so that we can know exactly factors that trigger the increase focus of U.S. in increasing cybersecurity over critical infrastructure under Obama Administration.

A. U.S. General Perspective on Cybersecurity over Critical Infrastructure

As one of major powers that has important role in world's order, U.S. is considering the importance of its security stability in many aspects such as politics, economy, social-cultural and averagely anything in general. When security is usually simply perceived in term of physical security guarded by military force of state, U.S. in this case had realized that security issues in fact are not as simple as that. By the emergence of globalization and more interconnectedness between state infrastructures and the cyberspace, U.S. had admitted the fact that cybersecurity is considered as important as conventional security which also need to be assured because both conventional security and cybersecurity are vital to maintain state stability and resilience.

In one hand, many other states perceive cybersecurity either as counterterrorism effort, data protection effort or information security effort and many more which depend upon contextual environment and challenges that they face which must be different between one state and another.

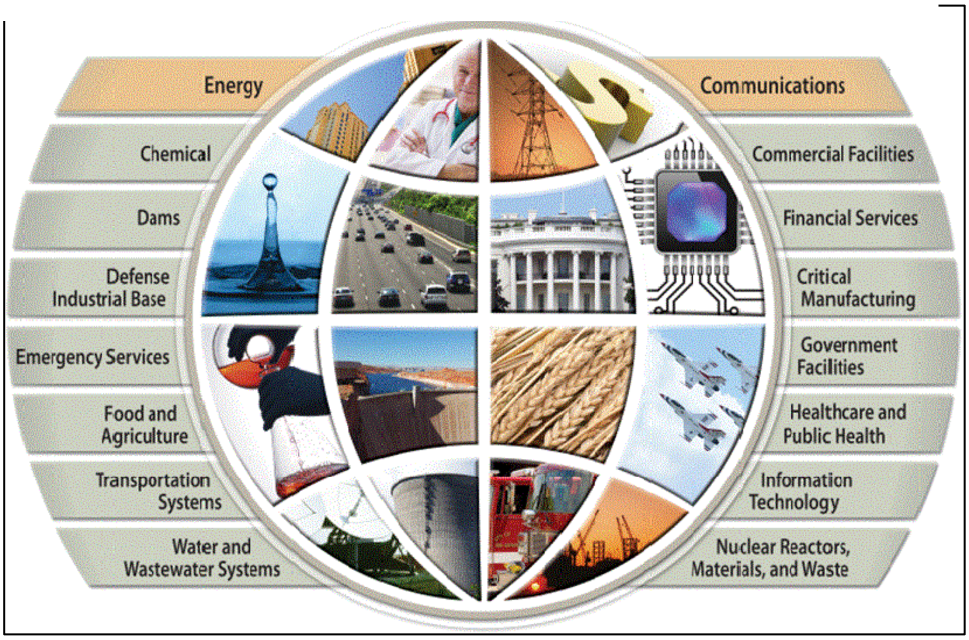
In the other hand, cybersecurity from U.S.' view is specifically recognized as an infrastructure protection effort (Chouri, 2012). Infrastructure in general can be understood as structures, systems and physical components within a country that their existence intended to provide service in the areas it supports (Investopedia, 2016).

Thus, it can be seen how basically U.S. is really prioritizing its infrastructures even when it tries to define cybersecurity in general. Particularly in U.S. context, there exist a term called critical infrastructure which refers to any vital assets either physically or virtually that its breakdown could possibly weakening the daily life service of basic sectors that serve most of American citizens such as public health, economic service and threaten state security in general (Security, 2016).

U.S. critical infrastructures have been becoming one of the most discussed topics by the U.S. state elites, public and private sectors as well as American citizens in common due to the fact of its vital importance as it serves from most basic to the complicated needs of all American society. Thus, in order to understand this fact, the writer of this research will provide the figure of the division of U.S. critical infrastructures that are consisted out of 16 sectors which each of them provide specific service as illustrated below:

Picture 3.2.

U.S. Critical Infrastructure Sectors



Retrieved from (NISAC, 2017)

It can be perceived that the discussion about critical infrastructures is becoming much more relevant in the cyber-related issues due to the fact that many critical infrastructures that belong to the U.S. are managed by using certain system and networks. Thus, this section will examine how critical infrastructures are being interconnected with the system which somehow is quite vulnerable to be disrupted by cyberthreat.

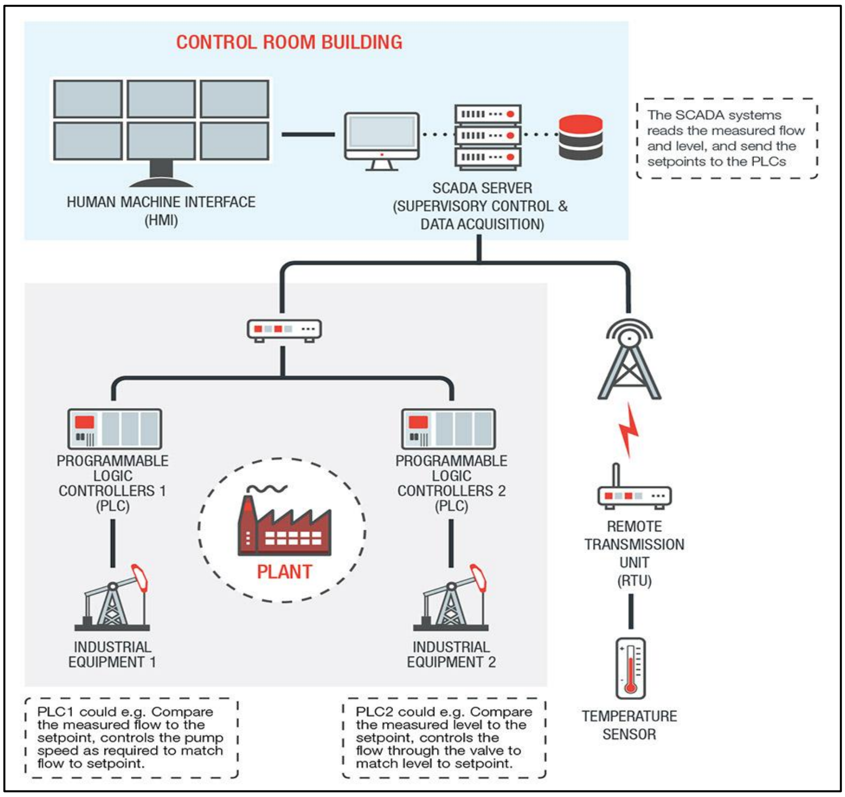
In U.S., many critical infrastructures such as transportation, manufacturing, water and even energy supply are managed by more complex networks and system as the consequences of high advancement of technology in current era. The main reason of the shifting trend of management to be more technological oriented is because of the fact that by doing so, state could provide a service in more effective and efficient way in more preferred controllable environment with less cost compared to few decades ago where state still provided service with more direct men involved.

In U.S. itself, the term to describe the system that is used to manage much of its critical infrastructures is generally known as Industrial Control System which is usually abbreviated as ICS. ICS comprises of types of control system and related instruments such as device and networks which help in controlling industrial process in more electronically efficient way (Micro, 2017).

The most common known type of Industrial Control System is SCADA. SCADA or Supervisory Control and Data Acquisition is a system that focuses on providing control at supervisory level. These SCADA systems are consists of devices distributed in various locations whose function are mainly to acquire and transmit data on the field site connected to Human Machine Interface (HMI) that monitored directly by the responsible operator person in the field (Micro, 2017). Below is the illustration how SCADA system works:

Figure 3.1.

Illustration on the Interconnection of SCADA and Field Sectors


CONTROL ROOM BUILDING
HUMAN MACHINE INTERFACE (HMI)
SCADA SERVER (SUPERVISORY CONTROL & DATA ACQUISITION)
The SCADA systems reads the measured flow and level, and send the setpoints to the PLCs
PROGRAMMABLE LOGIC CONTROLLERS 1 (PLC)
PLANT
PROGRAMMABLE LOGIC CONTROLLERS 2 (PLC)
REMOTE TRANSMISSION UNIT (RTU)
INDUSTRIAL EQUIPMENT 1
INDUSTRIAL EQUIPMENT 2
TEMPERATURE SENSOR
PLC1 could e.g. Compare the measured flow to the setpoint, controls the pump speed as required to match flow to setpoint.
PLC2 could e.g. Compare the measured level to the setpoint, controls the flow through the valve to match level to setpoint.

Retrieved from (Micro, 2017)

The utilization of SCADA enables long distance monitoring and controlling of field site facilitating workers in critical infrastructures sectors. In past, workers had to engage directly to the field site such as electricity plantation or water pipeline in order to perform task or acquire data. With SCADA, these workers can control operations such as opening or closing water pipeline, data acquiring from the sensor system and even monitoring field site and enabling alarm in certain situation from controlling room only (Micro, 2017).

Thus, with such vital importance of Industrial Control System such as SCADA which consists of complicated software and hardware functioned in managing basic critical infrastructures in the state, U.S. also has to face the risk of these new emerging technologies as ICS mismanagement that will give weakening effect for U.S. itself. Human error and irresponsible system operator seeking for personal benefits are among the risks the ICS should face. Furthermore, ICS in fact is often becoming the object of targeted cyberattack as well.

Hence, within the following part of this explanation section, the writer of this research will provide discussion related to several critical infrastructures that are holding the most critical features due to its high interconnectedness with system and networks which make it vulnerable to be disrupted. Further, this section will also discuss the actors who are related agencies in the U.S. departments responsible to manage those critical infrastructures sectors. However, due to the fact that critical infrastructures that belong to the U.S. are pretty much in number. Thus, the writer will give limitation regarding the explanation about this issue as stated in the first chapter of this research. The limitation refers to several sectors that are having the most significant development either in term of cyberthreat that is being experienced by each sector or the priority of security that is attempted by the U.S. government. Those sectors are as listed below:

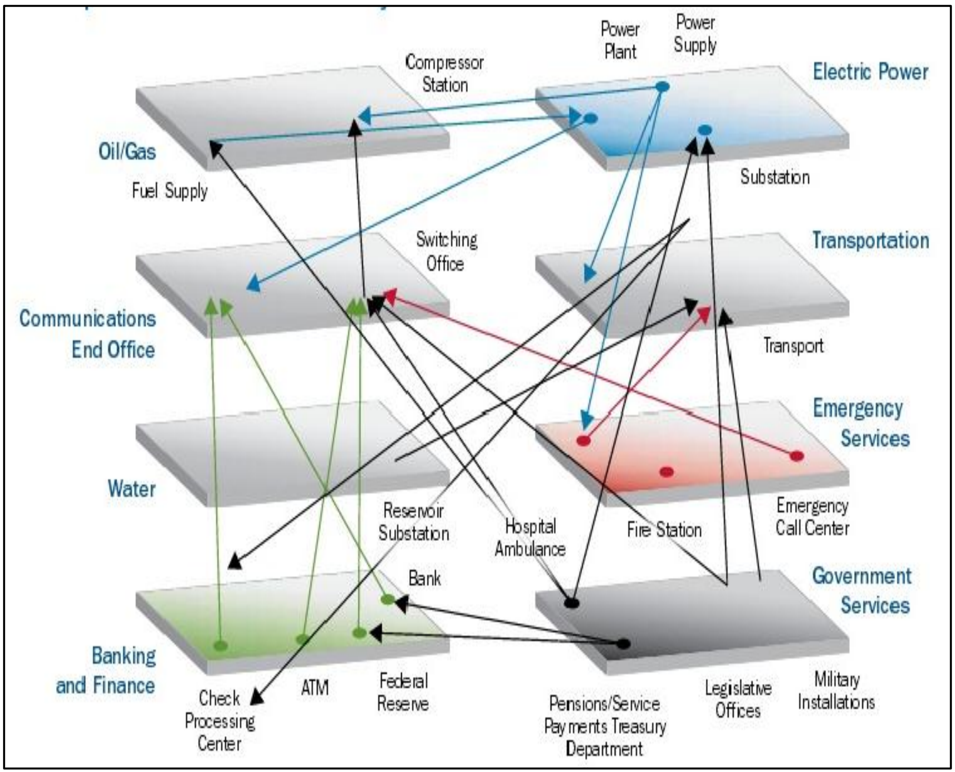
1. Energy Sectors

Energy sector can be said as one of the most prioritized sectors due to its ‘enabling-function’ characteristic. Enabling-function as stated by the Department of Homeland security is described as the ability of energy sector to provide support across all other critical sectors as the fact most of our twenty-first century services ought to be fueled by stable energy supply that if this energy supply cannot be well-assured then it will have weakening effects towards many other critical sectors to perform such as transportation, health and many more (Security, 2016).

In general, U.S. energy sector is segmented into three interrelated elements that include electricity, oil and natural gas. All of those elements are critical since technically and practically almost all industries and economic activity both in micro or macro level are depending upon electricity and fuels which without its support, many economic activities will not be ran well. This then consequently leads to the emergence of consciousness from the energy sectors related to its vulnerabilities which were triggered the U.S. to increase its planning and preparedness towards potential risk that might threaten U.S. energy sector in the future physically and virtually through cyber networks. The illustration of energy sector interdependencies with other sector can be drawn as follows:

Figure 3.2.

Energy Sector (Electricity, Oil and Gas) Interdependency



Retrieved from (Energy, 2007)

From the illustration above, it can be understood the complexity of the support from energy sector towards other critical infrastructures sectors which is no wonder why U.S. has specifically mentioned energy sector as a sector with Enabling-Function that hold major importance of maintaining resilience of other sectors.

Going further, the responsible agency to maintain the sustainability and resilience of the energy sector is recognized to be under the authority of Energy Agency or known to be Department of Energy. This department has vision as constitutes below:

> *"The Energy Sector envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing,*

> *effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government* (Energy, 2007)*."*

Thus, we can see that the vision about how Department of Energy was realizing the importance of energy sector across other sectors as well as vulnerabilities it bears which requires maximum protection and proper responses regarding any threat manmade or any force majeure such as natural disaster.

Specifically, in term of manmade threat, cyberthreat in fact was included in this extent. Vulnerabilities of cyberattack in energy sector lie on the reality that many of energy sectors are managed by using Industrial Control System or ICS as explained before in the previous part of this chapter. In 2015, according to ICS-CERT, an agency that was responsible to protect Industrial Control system of the U.S. reported that energy sector was the second-biggest sector that experienced cyber incidents. In 2015 alone, around 46 incidents of cyberattack was reported (NCCIC/ICS-CERT, 2015).

Thus, the Department of Energy was realizing the importance to collaborate with other agency in order to address proper response towards it. In this case, following the announcement on June 2006 regarding the completion of National Infrastructure Protection Plan (NIPP) from Department of Homeland security that was responsible towards overall critical infrastructures protection, Department of Energy was appointed as sector specific agency that has right and responsibility to support the execution of NIPP including in term of assuring cybersecurity of critical infrastructure in all level of government which have been partnering with other agencies in national and federal state level as well as private industry and other security partners whose main purpose is to ensure the stability and resilience of U.S. energy management (Energy, 2007).

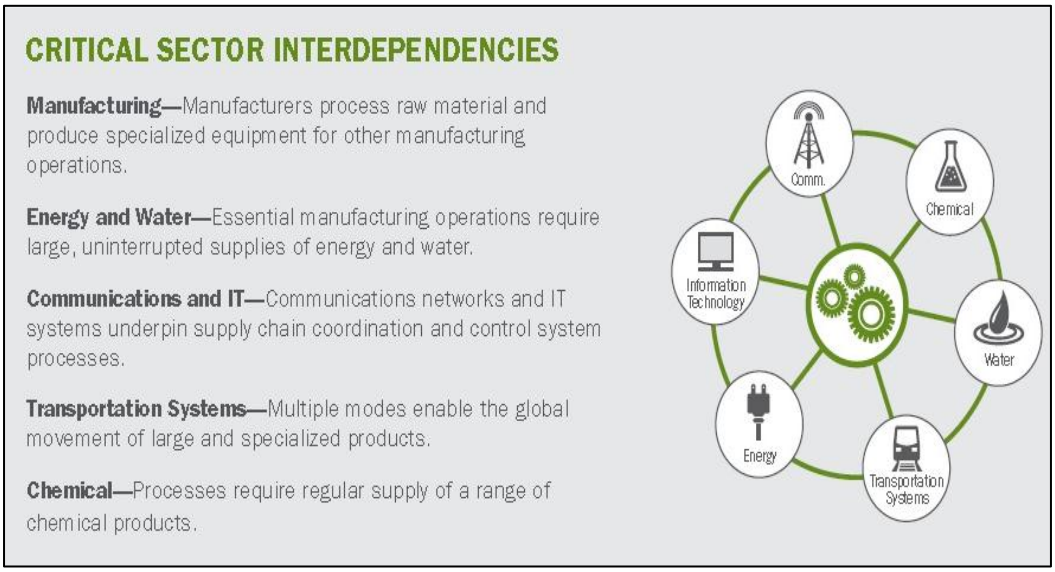
2. Critical Manufacturing Sector

Critical manufacturing was established as a national sector by Department of Homeland Security in 2008 as it was recognized to have significant impact in the national development. Critical manufacturing sector is operated in term of processing raw materials into specific parts or equipments that are vitally used in other U.S. industries.

Thus, similar to energy sector, this critical manufacturing sector is also having interdependency-factors that are contributing the resilience of other sectors. This sector produces parts or equipments that are needed by other sectors such as electricity and mining equipments, commercial vehicles parts and even aerospace equipment products. Similarly in return, critical manufacturing sector is also hugely supported by other sectors. It is known that in the manufacturing and production process, this sector also needs electricity and water supply and even in order to distribute the finished products, this sector needs proper transportations system as well so that the products can be evenly distributed in relatively punctual manner. The interdependencies itself are illustrated as follows:

Figure 3.4.

Critical Manufacturing Interdependencies with other Critical Infrastructures



CRITICAL SECTOR INTERDEPENDENCIES

Manufacturing—Manufacturers process raw material and produce specialized equipment for other manufacturing operations.

Energy and Water—Essential manufacturing operations require large, uninterrupted supplies of energy and water.

Communications and IT—Communications networks and IT systems underpin supply chain coordination and control system processes.

Transportation Systems—Multiple modes enable the global movement of large and specialized products.

Chemical—Processes require regular supply of a range of chemical products.

Retrieved From (Department of Homeland Security, 2015)

Furthermore, besides its important interdependencies with other critical infrastructures sectors, critical manufacturing is also considered as the most prioritized sector similarly like energy sector because critical manufacturing in fact has contributed US$2.08 trillion representing around 12.5% of total U.S. GDP in 2013 (Security, 2015).

Therefore, it is no wonder why with such vitality of critical manufacturing sector, U.S. has been realizing that the state needs to pay huge attention in assuring the resilience of this sector. The most identifiable risks that could possibly threaten this sector are range from natural disaster, the unstable supply chain, context of geopolitical condition of other states towards U.S. related to market target, terrorism and cyberattack.

Specifically in term of cyberattack, in 2015, it was reported that 97 cyber incidents were addressed towards critical manufacturing sectors, while usually in the previous years, energy sectors used to be the most targeted sector by cyberattack. In fact energy sector was in the second most-targeted sector during 2015 experiencing only 46 cyber incidents (ICS-CERT, 2015).

Furthermore, recognizing the fact that most of Critical Manufacturing is also using Industrial Control System or ICS as a platform of common operating system, cyberattacks then become more real challenges towards this sector that could possibly harm U.S. because of stolen information, business reputation, and intellectual property related issues. Thus, in this extent, Department of Homeland Security that focuses on regulating the critical infrastructure protection including the critical manufacturing sector has attempted to work shoulder to shoulder with other related agencies in national and federal state level and even academic and research organization in order to provide comprehensive protection assurance over critical manufacturing sector which is hoped to be fully resilient so that it can support the stability of U.S. economic and American citizens life (DHS, 2015).

3. Transportation Sectors

In our globalized world nowadays, the movement and mobility of people, good and services, money and also capital are considered important as it is become one of the characteristics in globalization. Therefore, realizing this fact, transportation sector is then becoming among top-prioritized critical infrastructures sector which plays role to facilitate the movement of U.S.

citizens inward and outward the country as well as ensuring the flow of goods and services through shipping process.

Therefore, in order to provide comprehensive services towards the citizens, U.S. government has categorized several sub-sectors that become the assets of U.S. transportation sector as a whole. The division is illustrated as follows

Table 3.1.

Assets Importance of Transportation sector in U.S.

Num.	Name of Asset	Importance
1.	**Aviation**	• composed of airports, heliports, seaplanes bases, support services, air traffic control and navigation facilities • approx. 19,700 airports in the U.S., with 500 offering commercial services • approx. 780,000 passenger flights take place across the U.S. monthly
2.	**Maritime**	• geographically complex and diverse system consisting of waterways, ports, and intermodal landside connections • consist of nearly 95,000 miles coastline, 361 ports, more than 25,000 miles of navigable waterways, and more than 29,000 miles of marine highway
3.	**Freight Rail**	• approx. 1,33 million freight cars in service (2013) • consists of 140,000 miles of active rail track • transports more than 70% of all U.S. coal shipments • approx. 73 billion in operating revenue for the 7 class 1 railroads (2013)

4.	**Highway and Motor Carrier**	• composed of bridges, major tunnels, trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, school buses, and key intermodal facilities • includes nearly 4 million miles of roadway, more than 600,000 bridges and 400 tunnels
5.	**Pipeline**	• more than 2.5 million miles f pipelines span the U.S. to transports nearly all of the natural gas an approx. 65% of hazardous liquids, including crude and refined petroleum • above ground assets include compressor stations and pumping stations
6.	**Postal and Shipping**	• includes large integrated carriers, regional and local courier service providers, mail services, mail management firms, and chartered and delivery services • approx. 720 million letters and packages moved each day
7.	**Mass Transit**	• include transit buses. trolleybuses, monorails, heavy rail(subway), light rail, passenger rail, commuter rail and vanpool/rideshare • 10.3 billion passengers trips in 2012

Retrieved From (Security and Transportation, 2015)

Hence, it can be understood the complexity of the transportation sector that its activity is covering transportation in land, air, maritime and even regulating pipeline and portal shipping. Thus, like energy and critical manufacturing sector, this transportation sector is also much depending on other sectors and vice versa. The concrete examples of these interdependencies are for example, transportation sector is depending on the supply of energy sector such as electricity and fuel from oil and gas. In return, energy sector is also depending on the support of transportation sector to distribute the fuel and energy commodities throughout the state, the proper utilization of distributing mechanism is equipped with advanced and secure transportation infrastructure.

In fact, transportation technologies nowadays become more and more cyber-based purposely to increase economic efficiency. There is an increase of dependence in this sector upon the technologies including Industrial Control System, as well as other operational functions such as navigation, positioning, tracking and communication in general (Security and Transportation, 2015).

Such dependence on cyber-based technologies is indeed assisting much of transportation both public and private party in regulating the sector. However the interconnection of those technologies may allow malicious actors to access key vulnerabilities of the system for personal benefit (Security and Transportation, 2015). It is proven by the fact that there are more or less 23 cyber incidents attacking the transportation sector in 2015 which made this sector as among top five most-targeted critical infrastructure sectors by cyberthreat (ICS-CERT, 2015).

Reminiscing this fact, the Department of Transportation in collaboration with Department of Homeland Security started to improve the management of transportation sector both physically and virtually through the enhancement of system and networks. Further, department of transportation supported the execution of National Infrastructure Protection Plan (NIPP) and was appointed as Sector Specific Agency to implement frameworks established by Department of Homeland security in order to create better and secured transportation system of the U.S.

Thus, to sum up the explanation of this section, U.S. as one of major powers in world has identified cybersecurity as critical infrastructure protection effort because of its consciousness over the vital feature of critical infrastructures in serving the needs of all American citizens. Among 16 infrastructures which all of them are important, the writer of this research has provided the comprehensive explanation in three most-prioritized sectors namely Energy, Critical Manufacturing and Transportation. The reason why the writer chose those three sectors is mainly because of its interdependencies characteristic towards other sectors that the support of those three sectors are hugely needed by other critical infrastructures. In addition, the fact that those three sectors are included as the top five most-targeted critical infrastructures by cyberattack has also illustrated the urgency of these sectors to be well-secured physically and virtually through cyber networks.

B. Comparison of Cybersecurity Development in Bush and Obama Era

After understanding the notion about how U.S. define the term cybersecurity from its own perspective revealing how importance critical infrastructures are for U.S.. In this case, the writer of this undergraduate thesis will provide a discussion that will specifically focus on comparing the development of cybersecurity from two periods of U.S. presidential leadership led by Bush and Obama. Such comparison is important to examine cybersecurity policy of each leader as well as in understanding the state political environment and dilemma faced by each leader which might be different from one another.

The reason behind the writer’s attempt to compare the development of cybersecurity issues of U.S. under those two Presidents leaderships is lying upon the notion that one of the variables within this thesis is to prove the existence of increasing over cybersecurity development in critical infrastructure aspects during Obama’s period as president. Thus, to prove such statement, it is considered necessary to provide comprehensive comparison from the previous period which belonged to Bush.

In a nutshell, the concrete way to examine the increase of cybersecurity development in Obama compared to Bush era can be taken from several data such as increasing budget and the forming of new agency that were not existed yet during the Bush period. One concrete data about the increasing in budget that supports the higher protection upon U.S. cybersecurity on critical infrastructure is coming from FISMA, the abbreviation from Federal Information Security Modernization Act. FISMA in this extent is functioned as guidelines for many of U.S. departments and specific agencies on its own responsibilities related to the protection of state assets from any risk of unauthorized access that may disrupt U.S. stability and security. Specifically for FISMA that was regulated for Fiscal year 2016 and 2017 regulated and aided by the role from National Institute of Standards and Technology (NIST) focused on improving the protection of cybersecurity in critical infrastructure (Security, 2016).

Furthermore, tracing back the previous years before 2016, FISMA budgeting including IT spending in fact were increased year by year. The data are illustrated as follows:

Table 3.2.

FISMA Spending Illustrating the Increasing Budget in Obama Era

(In Billions of Dollars, FY2006 to FY2015)

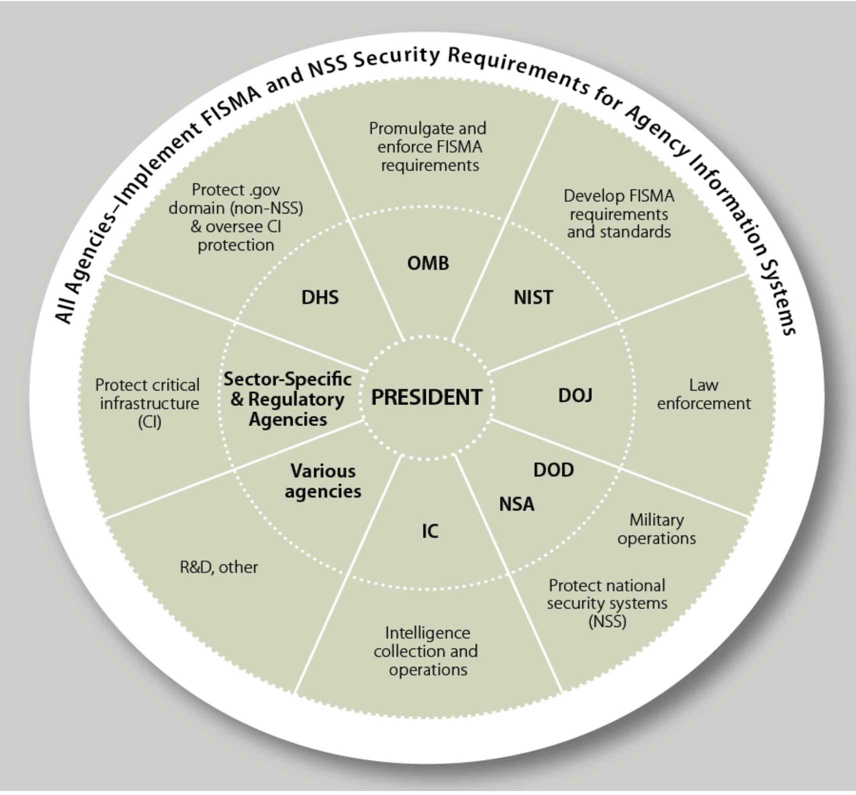
	Bush Period			**Obama Period**						
Fiscal Year	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
FISMA Spending	5.5	5.9	6.2	6.8	12.0	13.3	14.6	10.3	12.7	13.1
Total IT Spending	66.2	68.2	72.8	76.1	80.7	76.0	75.0	73.2	75.6	80.4
FISMA Proportion of Total IT Spending (%)	8.3	8.7	8.5	8.9	14.9	17.5	19.3	14.1	16.8	16.3

Retrieved From (Fischer, 2016)

From the table above, we can see FISMA spending during Obama period started from 2009 and the following year until 2015 were increased much even two times bigger compared to the Bush era from 2006 to 2009.Although there was still fluctuation, compared to Bush period, the budget allocated during Obama’s era was pretty much bigger. Thus, by knowing the increase of FISMA budget spending to support several agencies in protecting its cybersecurity aspects in critical infrastructure, it can be understood that during Obama's era indeed there was shifting focus towards higher priority over the ensuring of critical infrastructure cybersecurity.

Furthermore, referring to the FISMA as one of ultimate framework that gives guidance for many of U.S. agencies especially in term of addressing counteraction towards cyberthreat, below is the data regarding the U.S. department that have the most significant roles in the issue of cybersecurity:

Picture 3.2.
Simplified Schematic Diagram of Federal Agency Cybersecurity Roles


All Agencies–Implement FISMA and NSS Security Requirements for Agency Information Systems
Promulgate and enforce FISMA requirements
OMB
Develop FISMA requirements and standards
NIST
Protect .gov domain (non-NSS) & oversee CI protection
DHS
Protect critical infrastructure (CI)
Sector-Specific & Regulatory Agencies
PRESIDENT
DOJ
Law enforcement
Various agencies
R&D, other
IC
Intelligence collection and operations
DOD
NSA
Military operations
Protect national security systems (NSS)

Retrieved From (Fischer, 2016)

Based on the picture above, it gives the simplified illustration of roles that belong to several U.S. agencies and departments which have the most concern in the issue of cybersecurity. It can be perceived that President holds the supreme power as it is located in the center of the diagram due to the fact how importance is the President's roles in leading the cabinet which consisted of all departments and oversee the development on cybersecurity issues.

Meanwhile, NIST (National Institute of Standards and Technology) as the agency that formulated FISMA hold responsibility to develop standards that later will be applied to all federal civilian and other related agencies. Specifically in term of critical infrastructure as the main topic in this research, Department of Homeland Security (DHS) has the biggest responsibilities in operational practices of protecting federal civilian system as well as assisting private sector in protecting the assets of critical infrastructures.

Furthermore, DHS are cooperating with sector-specific and regulatory agencies in providing strong collaboration to protect the assets critical infrastructures for example DHS is cooperating with Department of Energy (DoE) in protecting the cybersecurity over energy infrastructure and also with Department of Transportation (DoT) in the matter of transportation sector. Thus, this sector-specific cooperation between DHS and other U.S. agencies is built depends on which department that regulating the critical infrastructure sector itself.

Beside quantitative data of FISMA spending, another concrete evidence to prove that there was increase upon cybersecurity development of U.S. critical infrastructure is by reminiscing the existence of Obama's Executive Order (EO) 13636 specifically addressed to improve critical infrastructure cybersecurity. Though, it should be admitted that such improvement is also created by Bush during his period. However in Obama's era, there were more dynamics on the creation of policies and programs in more legislative form such as bills associated with critical infrastructure protection. While in Bush period, though it has less bills proposals in term of critical infrastructure cybersecurity, there were still many frameworks and councils invented in his era. Even when Obama came into the office, Obama still could continue big leap that Bush had created in his period.

Thus, it is clear that different leader has different approach even when within the similar scope of issue. It is due to the fact that each leader faced certain dilemma and environment following the nature of political, economic and social context that happened during his period. Therefore, with such fact, the following section of this sub-chapter will be focusing specifically on discussing the dilemma and environmental features from Bush and Obama. The discussion is presented as follows:

1. Cybersecurity in Bush Era

Bush was one of the most popular Presidents of United States with his own specific policy focus and leadership style. Bush whom many people said as a child born with silver spoon in his mouth, marked as 43rd President following the succession of his father, George Herbert Walker Bush as former President of the U.S.. Bush also known as Bush Junior was inaugurated on January 20, 2001 (Museum, 2017).

As soon as Bush came into the office and held position as the most powerful person of the U.S., he was facing an incredible challenge on so-called September 11th terrorist attacks of World Trade Center and

Pentagon building or popularly known as 9/11 case. It was a day of grief for whole Americans as their lost of fellow citizens lives, material devastation and most of all dignity and pride as a proud nation. It was counted nearly 3000 people died. Thus, this event has marked the trend of Bush policy focus to be more hard-power oriented which was illustrated by his decision in invading Afghanistan with mission to overthrown Taliban regime as it was argued that this regime was responsible for hosting shelter to Osama bin Laden, the leader of Al Qaeda group who was accused by U.S. as the extremist terrorist group that was responsible for the 9/11 case (Staff H. , 2009).

Following the 9/11 which many Americans refer as the darkest day of U.S. history, Bush then declared his War on Terror. A policy that metaphorically illustrated war against terrorism through international military campaign, made him as the president with most approval rating of all time in the U.S. with 90% percentage polls (staff G. , 2001). Thus, it showed such event of terrorism attack really became a turning point for Bush presidency which also became the dilemma for himself as people said that utilization of many hard powers such as military assets by Bush administration have somehow disrupted the image of U.S. as an aggressor country. Meanwhile in one extent, such hard power-oriented approach was a normal thing for Bush who came from Republican Party that holds the importance of military superiority (Cipto, 2003).

With such context, the 9/11 case became the environmental influential factor for Bush era to produce foreign and domestic policy that focused more on terrorism eradication effort through tangible power such as military assets. Thus, in relation to the topic of this research, it can be seen how the major focus of U.S. at the moment was really into the 9/11 responses, though also much of initiative to improve the cybersecurity was also established during Bush era.

In 2003, for example, government released the strategy to secure cyberspace following the spreading of Sapphire internet worm that had influenced internet based application of the state such as airline flights and also influenced speed of the web (Harvey, 2016).

Furthermore, nearly the end of Bush presidency, he released Comprehensive National Cyberspace Initiative (CNCI) in 2008 which marked the focal point of Bush administration focus in improving and proactively giving responses towards future vulnerabilities as the development of telecommunication and information technology are getting more advanced. However, the further details of this initiative were classified by the Bush administration for certain reason mainly to secure the initiative so that it can be well-executed (Rollins and Henning, 2009).

Meanwhile, specifically in term of critical infrastructure, Bush administration was focusing more on protecting the physical form of critical infrastructures and key assets of the U.S. following the 9/11 terrorist attacks proven in targeting the physical disruption of U.S. assets.

This protection attempt was illustrated by the release of national strategy of Physical Protection of Critical Infrastructures and Key Assets in 2003. However, some parts of this national strategy had also started to give focus on cybersecurity as well as it is being mentioned several times within the written document (Security, 2003).

In summing-up statement, Bush era of presidency was pretty much being challenged by terrorism attack of 9/11 case which marked his policy directives of war on terror that successfully arose his overrated image as well as increased his approval polling. However, even though Bush was facing such challenge, much of cybersecurity initiative was started by his administration for example the CNCI which later became future continuous project of upcoming U.S. President as Bush Successor.

2. Cybersecurity in Obama Era

Following the resignation of Bush as U.S. President by the end of 2008, his successor Barack H. Obama, a 1961-born President has taken the office on January 20th, 2000 and made him the 44th and the first African-American President of U.S. in all time (Staff, 2017). Besides his popular image backed with Democratic Party's liberal view, when Obama was coming to the office, the condition of U.S. economy at the moment was not quite good. The mortgage crises became the biggest crises of U.S. economy after the Great Depression 1939 several decades ago that started nearly at the end of Bush administration. However, the effect was pretty much becoming a burden for Obama as these crises were quite devastating U.S. economy at that moment.

In addition to the mortgage economy crises, Obama was also challenged with the argument to rebuild the image of U.S. that was put into risk due to U.S. involvement in war on terror. It was quite aggressive marked by the attempt to kill Osama Bin Laden and invasion to Afghanistan which draw many criticisms from the world view. Thus, following this event, Obama argued that the overreliance of Bush upon hard power has somehow given devastating effect for the U.S. image and he suggested that the U.S. needed to utilize more soft power to rehabilitate this damage by suggesting a proposal during his campaign in 2008 (Lagon, 2011).

In the relation to cybersecurity as the main discussion of this undergraduate thesis, the attempt of Obama administration in framing agenda and initiatives regarding the cybersecurity issues can be considered as U.S. attempt to utilize more soft power. It is mainly because by doing such attempt, U.S. can build a new image of U.S. as a country that does not merely care about hard and military power but also to the new non-traditional security issues such as cybersecurity.

Consequently, the attempt to focus more on cybersecurity was then successfully renewing the image of U.S.. In this extent, it was proven by the establishment of U.S. cooperation even with its non-allied state such as Russia and China in the cybersecurity-related issues whereas U.S. had also suspected them to play major role on breaking the U.S. system (Brown and Yung, 2017).

Furthermore, besides the increase of budget on FISMA, another improvement in cybersecurity issues, specifically on critical infrastructure-related issues were shown by the attempt of Obama administration to declassify the outline of major government effort to protect the U.S. computer networks within the CNCI that was initiated by Bush Administration. However, it was still being categorized as fully classified project during bush era. This was then brought relatively fresh air for the U.S. citizens by knowing that the government has focus more on critical infrastructure protection not only for public sector but also the private sectors protection and cooperation too (Nakashima, 2010).

Thus, we basically can admit how much were the improvements made by the Obama administration in term of cybersecurity and critical infrastructure network protection. Even though, such improvements were also proven to be exist in Bush era, However, Obama has more supporting features to support him to focus more in cybersecurity issues. Among them is to build new image of U.S. as a country that does not merely care about hard power and military efforts just like what happened during Bush era following his counterterrorism effort of 9/11 attacks.

As a concluding statement of this chapter, U.S. as a well-known major power in the world has its own perspective in defining cybersecurity. According to U.S., it is as the critical infrastructure protection effort. With such fact, U.S. holds the argument about how vital 16 critical infrastructures are to serve daily life of U.S. citizens that somehow also have vulnerabilities of network attacks as they have more interconnection to the network and system-based management such as Industrial Control System (ICS). Among the sectors, the energy, critical manufacturing, and also transportation sectors were became top five of the most important targeted cyber incidents sector in 2015.

Furthermore, with such importance of U.S. cybersecurity on critical infrastructure, the role of leader of state in determining the policy directives is also considered as influential factor. Bush and Obama presidential periods are pretty much interesting to be discussed and compared as they have quite different environmental influential factors during their presidency. It can be named that the 9/11 was the vital feature to shape the Bush's policy directive to focus more on the hard power utilization as it was experiencing more physical attacks during the 9/11. However, several initiates or starting points were also created by Bush that became the continuous project for Obama administration. Obama in the other hand can be said to have quite dynamic development on cybersecurity issues because of his policy and budget improvements which were somehow categorized as an attempt for U.S. to rebuild its devastating image due to U.S. focus that became paid more attention on soft hard power during Bush Administration.