CHAPTER IV

INTERNATIONAL AND DOMESTIC FACTORS THAT WERE INFLUENCING U.S. DECISION TO INCREASE THE DEVELOPMENT OF CYBERSECURITY ON CRITICAL INFRASTRUCTURE UNDER OBAMA ADMISTRATION

With the phenomenon of globalization along with its advancement of technology, the International relations situation nowadays is much or less characterized with the new atmosphere full of opportunities yet challenges especially for the states. As world and many statehood aspects are more interconnected to the networks, state seems to have more concern to protect its critical assets which are considered vital for the daily life of its citizen. This fact is being realized by many states nowadays, so is United States of America.

U.S. as discussed in the previous chapter had realized the importance of critical infrastructure for servicing its citizens making this country even specifically defined the meaning of cybersecurity as effort to protect its critical infrastructures. Many dynamics developments happened during Obama administration which was illustrated by budget improvements on cybersecurity as well as the establishment of frameworks and the strengthening effort of the related agencies. Those kinds of dynamic developments were quite different from the predecessor era which belonged to Bush. This difference relied upon the environmental features that influenced many of Bush policies such as 9/11 terrorist attacks that somehow became the main reason of Bush to produce policies that focused on U.S. involvement in counterterrorism effort with the utilization of more hard power.

Realizing this fact, the writer of this research is aware of the policy in decision-making process, there must be many important factors that influence a state under specific administration to focus more on certain issues as illustrated in the Bush era. Thus, this chapter will specifically provide a comprehensive explanation related to the background that influenced Obama administration in lifting up its cybersecurity over critical infrastructure.

Referring to the decision-making process model by David Easton, the writer generally assumed that there were international factors such as cyberthreats coming from other states that tried to break the cybersecurity of U.S. critical infrastructures in their own personal objectives. There were also domestic factors consisted of demand and support that came from U.S. non-state actors such as interest groups which seeked for U.S. approval upon the notion that cyber networks as a field full of risk needed to be protected holistically. Furthermore, in general, the writer also presumed that U.S. effort in increasing its critical infrastructures cybersecurity was purposely executed in order to achieve stable cybersecurity which become one of its national interests in term of security in general. The further discussions are explained as follows:

A. International Environment Factors

It is understood that the decision-making process model introduced by David Easton was comprised of several elements. Among them is the environmental factor. Easton argued that environment is a crucial element for a political system since it is characterized as an interlinked chain where environment is able to influence the political system both positively and

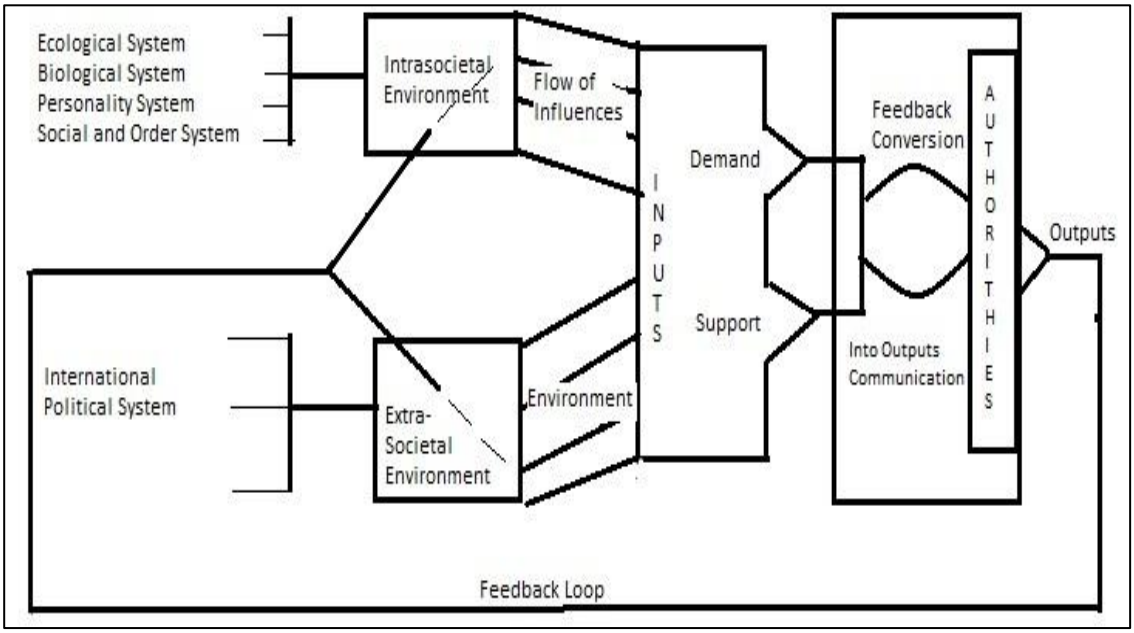
negatively (Nitisha, 2016). That is why political system was perceived by Easton as an open system that should be able to respond toward disturbances as well as adapt itself in particular condition (Saheb, 2016).

Specifically talking about environment aspects on the decision-making process model, Easton has divided political environment into two which are Intrasocietal and Extrasocietal. In one hand, Intrasocietal can be described as apolitical systems existed within the same society which forms the society segmentation and also influences the existence of the political system of that society. The examples of Intrasocietal environment are social structure, economics and cultural condition (Fisher J. , 2010).

In the other hand, Extrasocietal referred to all systems that were existed outside the given society (Fisher J. , 2010). The concrete examples of this environment are international political systems such as alliances, international social systems which comprised economic, demographic, socio-cultural and etc (Pooja, 2016). The below illustrated scheme showed us how Intrasocietal and Extrasocietal as environment influenced overall decision-making process within a political system as proposed by Easton:

Figure 4.1.

Comprehensive Model of Easton's Political System with Intrasocietal and Extrasocietal Environment Factors



Retrieved From (Pooja, 2016)

The existence of Intrasocietal and Extrasocietal as environmental factors within the scheme of Easton's political system informed how those kinds of environment either that was existed within or outside the society were having a significant influences towards demand and support in the decision-making process of the government in a given society. Thus, the section of this chapter will specifically discuss the Extrasocietal factors which comprise the international factors regarding the attempt to prove the first hypothesis of this thesis research related to the existence of external state influence towards the increase of cybersecurity on U.S. critical infrastructures.

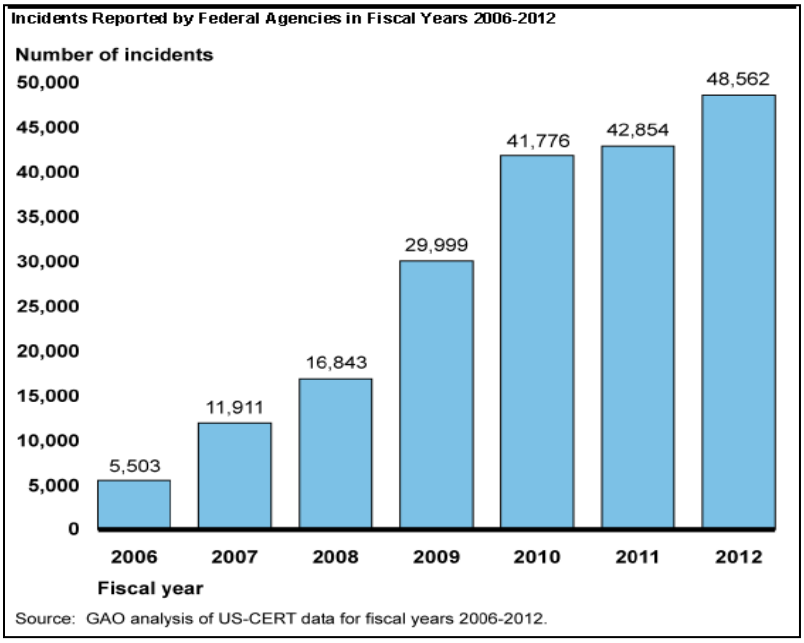
As Easton had argued, any system that lied outside a given society and had significant influence either disturbed or facilitated the system itself were considered as an Extrasocietal environment. Thus, it can be basically perceived

how cyberthreats that were coming from Nation-state outside U.S. and had tried to attack U.S. networks on critical infrastructure during or before Obama administration was somehow became the main factor for U.S. to finally take the decision in increasing the development of cybersecurity on critical infrastructure under Obama administration.

In a nutshell, cyberattack can be defined as an attempt by hackers to damage or destroy a computer network or system (Oxford, 2017). From the investigation of GAO or Government Accountability Office, one of U.S. agencies which provides evaluation and audits process for the U.S. congress has found a fact that year by year there were significant increases of U.S. experience of being attack by cyber networks. It can be illustrated by the diagram below:

Figure 4.2.

Reported Cyber Incidents from 2006-2012 Fiscal Years

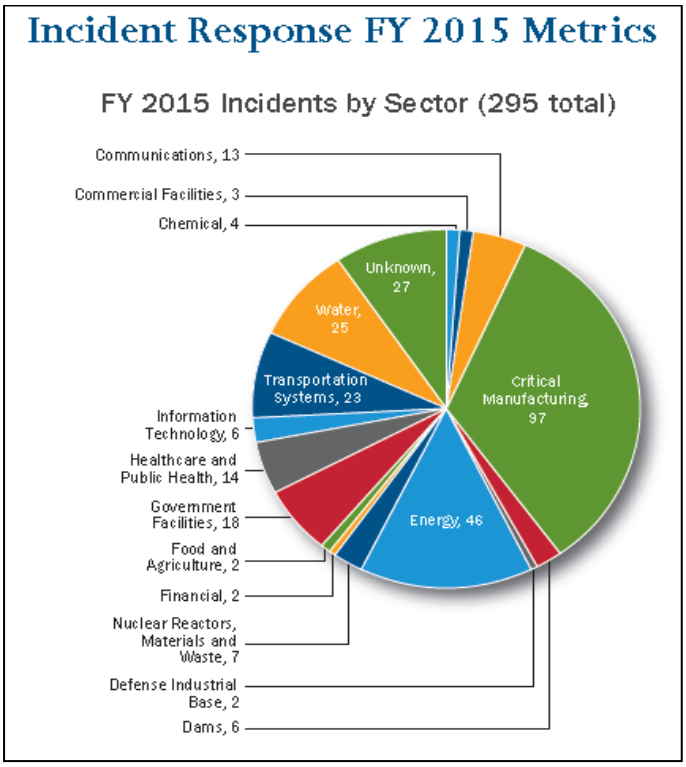


Retrieved From (Office, 2013)

The chart above shows the significant increases of cyber incidents reported by many U.S. federal agencies had been experienced. The increase had approximately been around 782% in 6 years from 2006 to 2012 fiscal year (Office, 2013).

Meanwhile, specifically in term of cyberthreat in critical infrastructure, the annual review from Industrial Control System – Cyber Emergency Response Team (ICS-CERT) in 2015 had revealed that cyberthreats in that fiscal year remained high as numerous cyber incidents had reported to be experienced by related federal agencies that managed the critical infrastructures. The diagram below illustrated the proportions of cyber incidents experienced by 16 U.S. critical sectors

Figure 4.3.
Reported Cyber Incidents on U.S. Critical Infrastructures on Fiscal Year 2015



Retrieved From (NCCIC/ICS-CERT, 2015)

The illustrated chart above shows top five sectors experiencing the biggest number of cyber incidents were the critical manufacturing sector, energy sector, water, transportation and government facilities sectors. Some of these sectors had been explained comprehensively in the previous chapter as well.

Furthermore, the writer was well-aware that there were quite many cyberthreats to mention. Therefore, the writer will only limit the discussion by dividing the section into two. They are U.S.' direct experience of International cyberattack and U.S. lesson learnt from other states' cyberattack experience. Both sections will be explained based on the most focal event of cyberthreat and where those threats originated from. The discussion will be explained further below:

1. U.S.' Direct Experience of Internationally Originated Cyberattack

The shifting world from simply internet of computer to internet of things allowing the management of many daily aspects with internet networks had increasingly formed the premises on how the risks increased along with the benefits (Mattern and Floerkemeier, 2010). Particularly, high interconnection of U.S. critical infrastructures and networks control such as Industrial Control System (ICS) have enabled more efficient and less costly management of infrastructure sectors.

However, as mentioned before in the previous chapter, the utilization of technology like ICS require a well-managed cybersecurity of the state as it needs to protect most critical sectors that serve the daily needs of all American citizens. As the time goes by, many of improvements were made by U.S. government to increase U.S. cybersecurity such as budget improvement and

the establishment of framework to protect related agencies. However, there were numbers of cyberattack that have been experienced by U.S. either in past or under Obama administration which somehow became the triggers for U.S. to make another cybersecurity improvement.

U.S. Department of Defense (DOD) has mentioned several times that the nation-state actors were investigated to have a significant attempt in breaking U.S. networks either to exploit data or disrupt the system such as China, Russia and North Korea (Defense, 2015). According to the writer's analyses those nation-states are included in the Extrasocietal environment as explained by David Easton. It was because the behavior of those nation-states to perform cyberattack towards U.S. were influencing the way U.S. to increase its priority in improving its cybersecurity under Obama administration. Thus, the further part of this section will mainly deliver data related to the critical cyberattack performed by China and also North Korea towards the U.S. government. The reason of the writer to choose those two states was because of the dynamics cases and data availability related to the cyberattack performed by China and North Korea. The discussion well be as follow:

a. China Cyberattack

Talking about China, it has been believed that the possession of this country over great assets of technology consequently increased its cyber capabilities. However, there were so many accusations addressed towards

China about the cyberattack and espionage it has commited, though, Chinese government argued those accusations as baseless (Wortzel, 2013).

From U.S. perspective particularly, U.S. has claimed that China has stolen many of global business Intellectual Property to benefit Chinese company as an attempt to surpass U.S. in economy (Defense, 2015).

Further, the range of Chinese cyber effort addressed towards U.S. were ranged from espionage over military and intellectual data where the victims were claimed not only happened to be U.S. official agencies but also private companies. Thus, it was considered as the threat against U.S. interest especially in term of security stability matter. It is known that, cyber espionage was categorized as one of cybersecurity threats that could possibly weaken state performance that could be dangerous as it allows the cyberthreat performer to gain control over classified data. Gaining control ranged from attaining documents to modifying and discarding it.

Below are the general data of U.S. victim in China cyber espionage both public and private corporate in a five year period prior 2015 as delivered by National Security Agency intelligent:

Picture 4.1.

Illustration of U.S. Victims of Chinese Cyber Espionage Prior to 2015

Retrieved From (Windrem, 2015)

The above figure has shown the successful Chinese cyber espionage that were spread throughout the U.S. region where each red dot represented one cyber incident that was experienced either by public or private corporate. More than 600 corporates became the victims of this cyber espionage where many military classified data such as U.S. critical infrastructure and secret formula of industries were stolen as informed by an NSA intelligent (Windrem, 2015).

Furthermore, one of the most popular cases of Chinese cyber espionage was known as Titan Rain. It was a term used by U.S. to illustrate Chinese attempt in stealing U.S. military sensitive information in 2005. As quoted from Time magazine, the investigation revealed that the hackers were not simply using Chinese systems as launch pad but in fact they were China-based (Thornburgh, 2005).

In the following year, 2007, U.S. press has reported about the cyber intrusions performed by Chinese cyber operators towards Lockheed Martin, a contractor company that handled the project of U.S. F-35 joint strike fighter. Following this intrusion, Chinese launched its J-31 Stealth fighters which some experts claimed that this Chinese J-31 was closely resembled U.S.' F-35 and was developed using the U.S. original design plan (Wortzel, 2013). This is in fact had something to do with U.S.' critical infrastructure cybersecurity especially in term of Defense industrial base sector.

In recent decade, 2012, under Obama Administration, a report addressed to the congress was revealing that U.S. Department of Defense had experienced more than 50,000 attempts of cyber intrusions. Even though the fact that it was not all of those cyberattacks were performed by Chinese government, but majority of them were done by China. Furthermore, on the same year, U.S. National Aeronautics and Space Administration (NASA) reported the existence on intrusion over their Jet propulsion laboratory network. The following investigation revealed that the intrusion was coming from China-based Internet Protocol (IP) addresses which allowed the hackers to have a full functional control over the NASA network ranging from modify to delete the NASA existing data (Wortzel, 2013).

Overall, China according U.S. perspective has been claimed to play major role in breaking U.S. networks and has performed numerous kinds of cyber intrusions purposely to attain and control over military and industrial

data. U.S. considered this as a threat of national interest as the intrusions that were performed by Chinese originated IP addresses were financially worth US$ 338 billion in a year alone (Wortzel, 2013).

b. North Korea Cyberattack

As one of the most isolationist states in the world, North Korea closeness upon its own possession on cyber assets such as technology and cyber capabilities has been becoming a dilemmatic thought for most of other state leaders. No clear data or literature on this matter consequently made uncertain assumptions upon the North Korea cyber capabilities which then led to the increase of awareness from many states including U.S (Jun, LaFoy and Sohn, 2015).

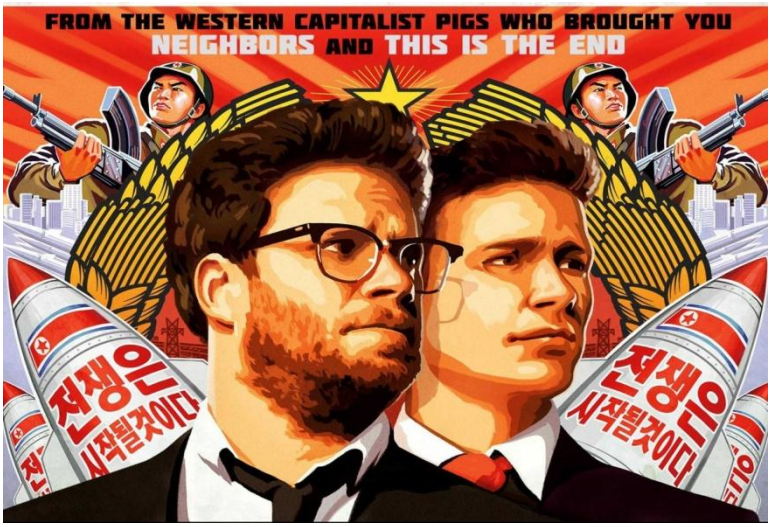
Probably one of the most thrilling cases ever happened related to the North Korea attempt in addressing cyberattack towards U.S. was in the case Sony Pictures Entertainment. Recently in November 2014, U.S. major Entertainment Company, Sony Pictures, had experienced series of intrusions causing company's computer became unable to perform and the leaked of classified business information such as emails and personal data of Sony's movie stars and employee as well as the stealing of unreleased movie projects (Defense, 2015).

This cyberattack performed by a group called Guardian of Peace happened following the upcoming release of a sarcastic comedy movie with satirical contents about North Korea also in 2014 called 'The

Interview' which North Korea claimed this cyberattack was not theirs but complimented it as righteous deed (BBC, 2015).

Picture 4.2.

Poster of 'The Interview' Movie Which Claimed as the Reason Behind North Korea Cyberattack on Sony Pictures



Retrieved From (Smith, 2014)

U.S. government in this extent claimed the North Korea cyberattack as one of the most destructive cyberattacks up to now as it was also accompanied with series of threat of terrorism and intimidation when the hacker group called Guardian of Peace threaten U.S. with 9/11 likely attack on the cinema that tried to show this movie. Following this serious threat in December 17th, Sony Pictures temporary cancelled the release of this movie that was planned to air on December 25th. However, in December 23rd, Sony then decided to have a limited release of this movie (BBC, 2015).

This kind of cyberattack towards Sony Pictures Entertainment Company according to the writer's analyses is a threat towards one of U.S. Critical Infrastructures namely Commercial facilities which one of its subsectors included entertainment and media sector. Even though, only small numbers of cyberattacks threatened this sector for example in 2015 with only 3 cyber intrusions reported, but still once it was attacking this U.S. sector the loss of material could not be compared with U.S. loss of dignity. That is why this then became one of main reasons for U.S. to improve its cybersecurity on critical infrastructure.

2. U.S. Lesson Learnt from Cyberattacks Experienced by other States

Besides having its own series of experience in being threaten by cyberattack, U.S. in fact was quite aware with any cyberattack event that was experienced by many other states as U.S. is also conscious about this contemporary growing threat. As one of the most advanced countries in term of technology and cyber capabilities, U.S. had shared the same view with many other countries around the world about the importance of cybersecurity and related cooperation for the stability of international order.

One of the most concerned cyberattack cases that had seized up U.S.' focus was experienced by Ukraine. This country, in December 23rd, 2015 was facing unplanned power outage as major companies that were handling the electricity distribution experienced series of remote cyber

intrusions. This power outage was affecting approximately 225,000 Ukrainian customers in Ukraine's 131 cities and towns (ICS-CERT, 2016).

Russia in this extent was publicly being blamed by several Ukrainian officials as the actor behind the cyberattack on its power grid. It was mainly because Ukraine investigation following the attack found a malware called BlackEnergy which has been believed as well by Ukraine government was originated from Russian (Perez, 2016). This cyberattack was said by some experts as the following consequences of the high tension between Ukraine and Russia in their geopolitical conflict of the Crimea annexation case (Higgins, 2016).

U.S. was also involved in this case by helping in organizing the interagency team and sending U.S. representatives from related agencies such as U.S. Computer Emergency Readiness Team (US-CERT), Industrial Control System – Cyber Emergency Response Team (ICS-CERT), National Cybersecurity and Communication Integration Center (NCCIC), FBI and many more. These U.S. representatives were hoped to work altogether with the Ukrainian government by investigating the cyberattack incident openly (ICS-CERT, ICS-CERT, 2016). The U.S. assistance in the Ukrainian power outage was believed by the writer as U.S. effort to share the similar view regarding the danger of cyberattack and put the further effort to prevent future attacks.

Furthermore, to sum up this section, the writer also argued that this kind of attack against Ukrainian power grid had somehow inspired U.S. to

notice that the breakdown of such vital critical infrastructure could possibly happen in a real life. Even though in fact, there was no report related to U.S. experience in being attacked by cyberthreat especially in term of its electricity energy sector, but there were scenario existing within a report issued by Cambridge University and Lloyds of London that theorized if the similar cyberattack happened against U.S. electrical grid, it could have been believed that 93 million people from New York to Washington D.C. will experience a moment without power and impact U.S. economy to loss US$243 billion to US$1 trillion with no exception of another collateral damage such as the messed up supply chain and business downturn (Campbell, 2016). Thus, such event had much or less inspired U.S. to address the increase of its cybersecurity especially in critical infrastructure aspect such as energy sector as security stability including in energy aspect is considered as one of U.S. focal national interests.

B. Domestic Factors: Demand and Support from U.S.' Non-State Actors

After understanding the international environmental factor or called by Easton (1953) as Extrasocietal which also has direct interlink with the domestic environment and consequently influences the decision-making process of Obama administration, in this part of discussion, the writer will deliver a comprehensive explanation related to the demand and support that existed within the U.S. domestic statehood especially the one that were coming from the non-state actors.

As mentioned in the previous chapter, demand and support are two most important elements within Easton's decision-making process. Demand in one hand can be described as various interest and need from the society that were collected and aggregated within the political system's decision-making process. Meanwhile, support is the willing participation of the society towards particular decisions or policies that were produced by the government such as obedience towards law and involvement in general election (Ahmad and Eijaz, 2015). In the section, the writer will deliver a discussion related to the demand itself in specific. According to Easton, it was derived from three important elements within a state namely society, political elites, and also international environment.

1. Demand to the U.S. Government Originated from Society, Political Elites and International Environment to Improve its Critical Infrastructure Cybersecurity

First, the demand came from society. Society itself can be described as a group of people that are aggregating in an ordered community (Oxford, 2017). Thus, according to writer's analyses, interest groups that were almost always existed in every society were one of the main sources of demand that were derived from as interest group of persons with likely similar interest which influence the way they act altogether to achieve their common goals (Merriam-Webster, 2017).

In relation to this thesis' topic which discussed the background of U.S. decision under Obama administration to increase its critical infrastructures' cybersecurity development, the writer argued that there was specific interest

group that worked and performed an advocacy towards the U.S. government related to the cybersecurity issue itself which more or less influenced the public policy produced by U.S. government within this issue. One of the most notable interest groups which worked in this field is Information Sharing and Analysis Centers (ISACs).

ISACs and its related sub-councils is a non-profit organization that was established in the 1999 followed the establishment of the 1998 Presidential Decision Directive – 63 (PDD-63) regarding the wish of U.S. federal government to establish the platform for each critical infrastructure sectors to share the information related to threat and vulnerabilities they faced at the moment. The main task of ISACs is to help each critical infrastructure's owner and operator in protecting their facilities, personnels and customers from any cyber and physical threat so that they can respond towards those threats correctly and enhance their resilience (Centers, 2016).

ISACs in relation to this research topic has played quite an active role to perform good bi-directional approaches both to the critical infrastructures sectors and the government where ISACs was also claimed to have excellent track record in sharing actionable information a lot faster than any other government partners (Centers, 2016). Formed as an organization that had focus specifically on critical infrastructure cybersecurity protection, ISACs also had performed several advocacy efforts to the U.S. government as the attempt to enhance its own performance in this field in regard to the enhancement of critical infrastructure cyber and physical protection as a whole.

The concrete example of ISACs' policy advocacy can be looked into its published paper regarding to the Financial Services of ISACs leader testimony namely Denise Anderson who addressed to the U.S. House of Representatives in cybersecurity, infrastructure protection and security technology subcommittee. This testimony specifically asked U.S. government to support the effort of private sectors in establishing its own council in ISACs since not all of the critical infrastructure sectors were all joining the ISACs. Furthermore, ISACs also asked the government support to recognize ISACs as an organization that plays critical role in critical infrastructures' cybersecurity protection (Anderson, 2015).

Going further, any policy advocacy effort was also illustrated to be executed by scholars and academician that with their professional status and knowledge were able to understand the U.S. cybersecurity development as a whole. One of the examples from the advocacy attempted by scholars was in form of policy recommendation towards this issue. Center for Strategic and International Studies (CSIS) scholars also released such policy recommendations towards the Obama administration entitled "Updating U.S. Federal Cybersecurity Policy and Guidance: Spending Scarce Taxpayers Dollars on Security Program that work". This policy recommendation was released in 2012 and mainly contained suggestions towards the U.S. government to update its current guidance in cybersecurity protection as its last update was in November 28th, 2000 and argued such policy update could

secure U.S. cyber assets more without spending more money (Reeder et al, 2012).

Secondly, examining the demand came from the political elites. The political elites can be perceived as notable persons in state politics whose influence was powerful enough to affect the decision-making of the state. Thus, in this case the writer argued that political elite in the issue of critical infrastructure's cybersecurity improvement under Obama administration is Obama himself.

Obama as a state leader who held the legitimate power to handle the state politically had the biggest influence in this case. His background of Democratic Party has shaped his view that the U.S. cyber defense in critical infrastructure is much more important by improving the act of protection and strengthening U.S. cyber assets which somehow had slightly different view from the republican stands on cybersecurity (Secure128, 2016). Republican Party expected the U.S. in cybersecurity effort to be more offensive than defensive like the Democratic Party policy illustrated. It is mainly because the republican believed that world nowadays is a dangerous place and thus it believed that U.S. needed to maximize its military and agency strength in responding towards the threat (Party, 2017). However, overall stand illustrated that both democrat and republican were in favor to improve U.S. cybersecurity as it held as one of U.S. national interests.

Thirdly, discussing the demand came from the international environment. According to the writer's opinion, the international environment

somehow has interrelations with the international factors context discussed in the previous section of this chapter. The writer argued that in the context of cybersecurity improvement made by the Obama administration, the exact demand derived from other states that requested upon the improvement itself was likely to be none as this kind of decision was domestic business of U.S. itself. The extrasocietal environment perceived as international factors in this extent was having direct influence towards the domestic U.S.

However, the international environment as argued in the previous section has become a platform where many of events such as cyberattack happened either it was addressed towards U.S. or experienced by other countries. This is directly or indirectly influenced U.S. decision making as those kinds of cyberattack events alarming U.S. about how vulnerable was the network system while how highly dependent was U.S. towards the management of critical infrastructure using the internet and network system.

Furthermore, even though, there was no direct demand from international environment addressed towards U.S. to specifically improve its critical infrastructure cybersecurity, within this international context, there were many International involvements successfully attracted U.S. to improve its cybersecurity. U.S. involvement in adopting international agreements of cybersecurity was inspired from one that was included in the UN Charter and Geneva conventions and rules of conduct making this country aware upon the international environment of cybersecurity that vulnerable and full of risks (Sofaer, Clark and Diffie, 2009).

As a sum-up statement, Obama decision to improve its critical infrastructure cybersecurity was somehow shaped by the demand from several elements of U.S. statehood which are the society comprised of Interest group and professional scholars, the political elite which is the Obama himself with the influence of his political party background, and the last is the international environment which has direct interlink with the extrasocietal environmental factor as explained in the previous section of this chapter.

2. Support towards U.S. government to Improve its Critical Infrastructure Cybersecurity

Support in the scope of this thesis discussion can be defined as willing participation of society to facilitate or execute any government policies. Those willing participations for example are obedience towards law and regulations, paying taxes as well as participation in general election and giving vote (Ahmad and Eijaz, 2015).

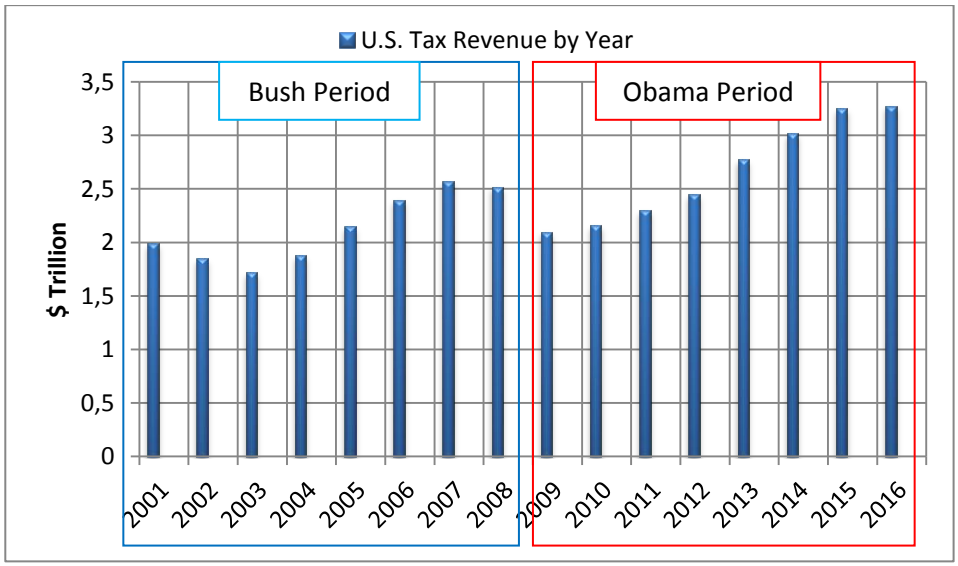
However, before proving that there was a thing such a support alternated by the American citizens, we need to have a concrete overview on how the U.S. native was considering the issue of cybersecurity. One of the proofs was shown by the research polling that was done by Justin McCarthy in a website namely Gallup.com. The research was conducted on February 2016 and addressed to more than a thousand adults living in U.S. 50 federal states including the District of Columbia regarding their opinion towards the critical threats to the vital of U.S. interest.

The result of this research surprisingly revealed that cyberterrorism as one form of cybersecurity related issues became the top three threats towards the U.S. national interest that held approximately 73% of polls following International terrorism in the first category with 79% polls and the development of nuclear weapon by Iran in the second category with 75% polls in total (McCarthy, 2016).

In term of taxation, even though there was no specific kind of taxes that the society could pay to support the cybersecurity. Society taxes payment were based upon their own economic activities. However, year by year, the tax revenue that the government obtained from the society kept getting higher which can be illustrated by the following data:

Figure 4.4.

Chart of U.S. Tax Revenue by Year



Retrieved from: (Amadeon, 2016)

From the illustrated chart above, it can be perceived that during Bush era from 2001-2008, the U.S. tax revenue was in a dynamic development with quite ups and downs movement. The peak was in 2007 when the tax revenue was approximately US$2.57 trillion. However, it was reached its bottom in the following year in number of US$2.1 due to the heavy mortgage crises. Meanwhile, in Obama era, after being left with such heavy homework of mortgage crises, this administration was successfully responded by addressing several policies which caused the increase in economy even until Obama left the office in 2016 without any single downturn.

Thus, in relation to the support of society, even though the taxes payments were not specifically addressed to support Obama in improving the cybersecurity condition of the U.S, the writer argued that the increasing pace in tax revenue illustrated how society was appreciating any Obama policy by giving their material support in form of tax revenue. Because of their consciousness to support will contribute much in every aspect of their life including in term of cybersecurity where such tax revenue was the capital for any budget allocation for each fiscal year. Thus, it somehow has interlink with the increasing budget of critical infrastructure's cybersecurity improvement under Obama administration as discussed as well in the previous chapter.

Besides tax revenue, according to the writer's personal analyses, U.S. is actually have a really big capacity either in term of its possession over advanced technology and successful experience of counteraction over

cyberattack to recover the result of threatened country's assets. This capacity is also become one of supporting factors that shaped public opinion on how capable is the country for not only being defensive from cyberthreat in this anarchic world but also offensive enough to interfere other states if U.S. wants to as hoped by the Republican Party side. Thus, this kind of capacity can be said as indirect factor that shaped U.S. public opinion about how good the U.S. capabilities is in term of cybersecurity and how proud the citizens should be actually, and with such awareness, U.S. citizens can fully support the Obama's policy that improved much of its cybersecurity on critical infrastructure development.

As an overall concluding statement of this chapter, the writer's hypothesis about the existence of international environmental factors comprised of Cyberthreat and Cyberattacks that were experienced by U.S. directly and other state somehow inspiring U.S. to be well-aware with the importance of cybersecurity issues was proven to be true. U.S.' cyberattack experience by China's Titan rain and North Korea's Sony pictures were among the concrete examples of the possibility of cyberthreat itself. Furthermore, Ukrainian's power outage presumably caused by cyber intrusion was also somehow made U.S. realize the vulnerabilities of critical infrastructures over cyberthreat. Thus, all of those international environmental factors were influencing U.S. to realize the urgency of improving overall critical infrastructures cybersecurity.

The second hypothesis which argued the existence of demand and support from the domestic U.S. statehood that influenced U.S. to improve its critical

infrastructure cybersecurity was also proven to be true. In one hand, demands that were coming from the society such as interest group and professional scholars have shaped U.S. view on cybersecurity as those interest groups and scholars provide an advocacy effort to recommend the update of U.S. public policy. Second, political elite that also became the source where the demand originated from happened to be Obama himself as he held the most supreme and legitimate political power of U.S. and backed up by shared-view with his democratic party about the importance of defense act for U.S. cybersecurity. Thirdly, demand from international context was having strong interlinks with the international environmental factor. In this extent, even though there was no state demanded U.S. to improve its cybersecurity, the international environment itself became the platform where many of cyberthreats were from influencing Obama to realize the anarchic situation of world cybersecurity order. Last but not least, the support aspect came from the domestic condition happened to be originated from U.S. citizens that became more aware in cybersecurity issues and thus had direct consequences upon their support towards the government illustrated by society willingness to pay tax as one of government revenues and capitals to improve many of U.S. state aspects including cybersecurity

Overall, this chapter has successfully delivered data and facts related to the existence of International and domestic factors that were shaping U.S. decision to increase the development of cybersecurity on its critical infrastructure under the Obama administration as in fact cybersecurity is one of most prioritized National interest that belongs to the U.S.