CHAPTER I

INTRODUCTION

A. Background

Living in world where globalization has been identified as a common phenomenon consequently leading to the fact that there is an increase of utilization over technology, such as internet and advanced gadgets following the nature of human in a more integrated and interconnected world.

However, it is not only people individually who have been involved in what so called as cyberspace but government as well. Cyberspace in this extent is a term that specifically refers to the notional environment in which communication over computer networks occurs (Oxford, 2016). In this case, government is also depending on the cyberspace since information technologies involved within it enables government to held transnational dialogue and even ensure the facilitation of the global flow of goods and services as well as manage its domestic affairs such as water supply, electricity and even functioned as data storage.

Nevertheless, alongside with the advancement of technology which pushes the relations between nations to be more integrated, like two sides of coin, it is also gives consequences for the states to ensure its cybersecurity to be well-managed since there are so many possibilities coming from other states that want to crack down the system for bad purposes such as espionage and sabotage of national assets which specifically defined with the term cyberthreat. This is then becoming a new trend following the emergence of so-called as non-traditional security issues of

nation-state which has shifted the field of the conventional battle from land, air and sea to the cyberspace (Srikanth, 2014).

Hence, it is no wonder that one of the most hegemonic power which of United States of America is realizing the urgency to embrace the importance of increasing its cybersecurity, reminiscing the experience of the state in being attacked by cyberthreats coming from other countries regardless its mastermind is state or non-state actors, those cyberthreats are jeopardizing the national security of U.S., as dangerous as the conventional threats. Russia, Iran, North Korea and China are among the actors whom U.S. claimed to play major roles on breaking the system of homeland security for their own specific interests (Defense, 2015). Following this fact, consequently U.S. is trying to enhance their capability to manage their cybersecurity in any aspect of statehood lives including critical infrastructure.

Critical infrastructure itself can be defined as assets, systems, and networks whether physical or virtual, considered so vital to the United States that their destructions would have a weakening effect on security, national economic security, national public health or safety, or any combination of it (DHS, 2015). U.S. government, political elites and the President had realized that the nation must be prepared for any attack against its electrical grid or other critical infrastructure assets that the disruption might cost a lot, not only economic material losses but also lives and national dignity.

The history of U.S. in developing its cybersecurity was started in1977 when the general accounting office recommends to limit the number of federal employees

who can use a computer as a way to prevent network security breaches (Post, 2003).As time goes by, following the fact that the activities of the U.S. federals are getting intensely attached to the computer networks and cyber space, in May 2003, the department of homeland security finally decided to create specific office so that the national cybersecurity of the white house can be carried out holistically. Until now, cybersecurity is one of main foci of the U.S. department of homeland security as well as other U.S. departments such as department of defense and many more.

Further in domestic scope, presidential administration in this extent can be considered as one of the most important factors that determines the development of state awareness towards cybersecurity issues. Political situation and circumstances in general also can determine the tendencies of president to focus on particular issues of state security.

The changes of political regime marked by presidential alternation always influence the directives of states in focusing in particular issue because different leader will have different style of leadership and face different challenges from the domestic and international environment which then produce different policy to approach those challenges.

Take a look at Bush administration, he was coming from Republican Party popularly known with its focus on supporting military superiority following the case when U.S. being attacked on 9/11 case. U.S. then was declaring the war on terrorism especially towards the axis of evil which are Iran, Iraq and North Korea (Ribeiro, 2013). In his administration, Bush's image was rather known with the

utilization of hard and tangible power that one of the proofs can be illustrated with his unilateral decision to invade Iraq in 2003.

Meanwhile, Obama administration was still being involved with the utilization of hard power proven with the U.S. involvement ranging from the escalation forces in Afghanistan to the killing of Osama bin Laden in Pakistan which draw many criticism, yet his decision to make U.S. utilize more soft power should be appreciated because Obama had realized that as a President he should rehabilitate the damaged image of U.S. from the previous administration until his era (Lagon, 2011). This then becomes one of the reasons why the U.S. under the Obama administration has added the focus to emphasize more on the development on cybersecurity issues which is categorized as a development more on soft power proven by the behavior of state in framing agendas and initiatives as well as attraction and persuasion activities to the U.S. societies and engaging with other states too in this issue. The exact proof is illustrated in Obama era, when several cybersecurity policies and budget allocation were specifically discussed which then brought a relatively fresh atmosphere to the U.S. because the state leader finally gave attention to the soft power as well and considered it as important as hard power.

The main point which is highlighted about how cybersecurity is significantly improved during Obama administration is proven by the increasing of state funding upon the major agencies that responsible in managing the state cybersecurity which applying so-called as FISMA (Federal Information Security Management Act). In the end of Bush administration in 2007, total FISMA spending was only 5.9 billion

dollars while when Obama came into the office, the total spending of FISMA over the overall IT budget is kept increasing until its peak on 2012 with total amount of 14,6 billion dollars (Fischer, 2016).

Furthermore, even for the fiscal year of 2017, the Obama administration was proposing around 17 billion dollars altogether for the cybersecurity which then illustrated how the world keep on more interconnected through the globalization. The U.S. government under Obama administration realized that there was urgency to keep the national interest of the U.S. especially in the matter of cybersecurity to be well-assured particularly through the increasing of cybersecurity funding as well as the strengthening of state agencies that has direct business to the matter of cybersecurity (Fischer, 2016).

B. Research Question

"Why did U.S. under the Obama administration have the urgency to increase the development of cybersecurity over its critical infrastructure?"

C. Theoretical Framework

In conducting the research, the needs of proper theory is important because theory will provide guidance and perspective in seeing the particular phenomenon that would like to be observed. In this research, the writer will use several concepts and theories as described below:

1. Concept of National Interest from Realism Theory

The concept of national interest is among the most popular concept that was coming from Realism. Referring to the thoughts of Hans J.

Morgenthau, National interest is the key concept in international relations that drives the way state utilizes its powers. In addition, Morgenthau is also arguing on how state politics is a matter of skill in harmonizing endless needs (interests) and scarce resources (power) which become the reason why government decision-makers can respond on behalf of the nation state towards the opportunities and dangers that are brought by the international system.

Morgenthau's way of thinking is based on the premises that the key point of national interest is to ensure the survival of the state. Survival here refers to the capacity of states to protect its physical identity such as territorial integrity as well as political identity for example 1) maintaining the existing regime and 2) cultural identity such as maintaining ethnic norm and preserving linguistic and history especially from the disruption of other states (Mas'oed, 1990).

2. Decision Making Process Model

Decision making process is one of the most crucial parts within the political system that belongs to the state. This process enables the government to create certain policies and output towards either its domestic or foreign relations as the response of problems or necessity that the state has faced at the moment.

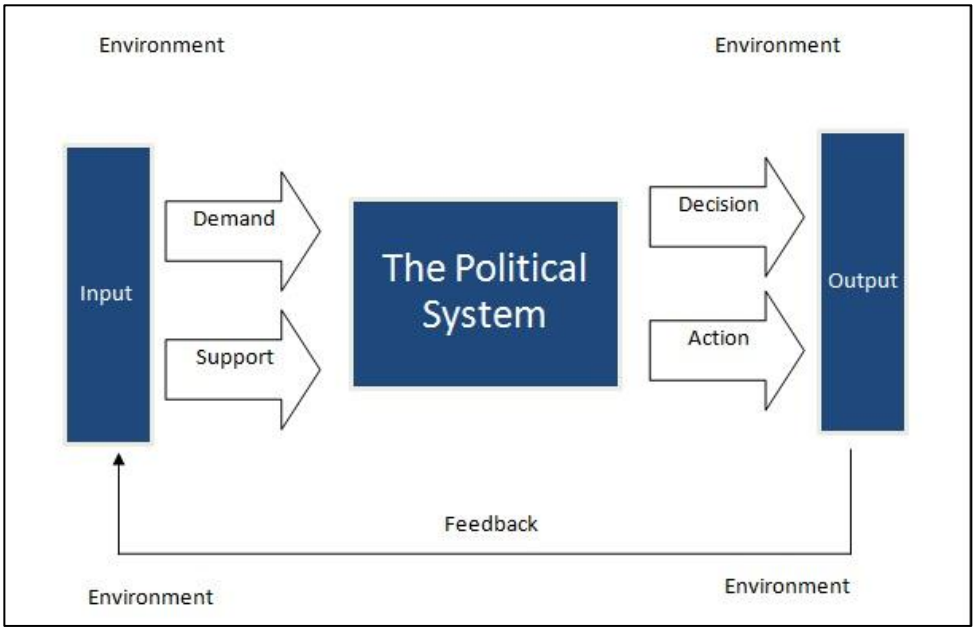
There are actually many decision making process models and approaches proposed by many scholars, but in this research, the writer will use the decision making process model that is introduced by David Easton,

a popular American political scientist whose works have been influencing the international relations world even until today.

The model of decision making process by David Easton is illustrated on the scheme below:

Figure 1.1.

Decision-Making Process Model by David Easton



Retrieved From (Mukti, 2014)

The above illustrated scheme explains how the decision is made within a state. Generally, the process begins when there is input. According to David Easton, it is consisted of two namely Demmand and Support. Demand itself can be defined as aggregated interest that arise from the very nature of human personality and society. In simpler words, demands are aspirations of the people. There are generally three sources of demands according to its originality. The first is society in which the citizens that live within the country. Second, Political elite refers to notable person whose influence is significant on the political system of the

state. The third is the International environment in which considered as important as the domestic factors and circumstances, for example International security context at the moment. Meanwhile, support is the willing participation of society or other actors involved within a state which can be in form of material participation, obedience towards law and regulations, participatory support and many more (Ahmad and Eijaz, 2015).

The next process happens within the political system itself where demands and supports are collected from society, political elites and international environment are selected and discussed critically by the branches of government which are executive, legislative and the judicial body of state in which after certain period of discussion, there will be outcomes produced in the form of decisions and actions that later will be applied to the statehood live.

In contrast to Easton's model that is emphasizing on the importance of overall structure in decision-making process, there exist so-called structural functionalism model suggested by Gabriel Almond tried to give additional aspects towards Easton's model. Almond in this extent tried to emphasize more in the argument that functions as the most significant features in the political system itself which is why then he gave several additional elements to complete the model especially in the stage of input and output.

Almond identified seven functions of political system which among them that are relevant to be used as analytical tools in this research namely Interest aggregation and articulation as well as political communication. Interest aggregation in specific is an activity that illustrates how interests in the society are collected and the differences between those interests are being balanced for example if there are any competing proposals from different interest group in the society (Janda, 2011). Meanwhile, Political articulation happens in a degree where citizens and citizen groups can influence policy through democratic institutions (Chhatre, 2008).But overall, those functions are existed to explain how demand and support as input of political system obtained or selected carefully by the branches of government before they are converted to become a policy (Sikandar, 2015).

Therefore, based on the model and concepts as described above, the writer of this research will use it to analyze the factors behind the decision of United States of America in increasing the development of cybersecurity over its critical infrastructure under the Obama administration.

First, the concept of national interest will explains how U.S. as an independent state is also having national interest especially in term of achieving security and stability. This becomes the reason why U.S. is addressing several policies and initiatives in order to ensure its cybersecurity over critical infrastructure. In addition, not only domestic policy that is launched to strengthen U.S. condition domestically, but U.S. in fact also addresses specific foreign policy

towards other states in order to engage on the issue of cybersecurity more in international level as well. In simpler words, U.S.' attempt in conducting specific domestic and foreign policy according to writer's analyses is merely because of it wants to achieve all of its national interest especially securing its domestic cyber system including critical infrastructure.

In this sense, realism believes that International system which is consisted of many other states with their own conflicting national interest are bringing out challenges towards U.S. security, especially reflecting from several attempts coming from foreign states including China, Iran, Russia and many more that are proven trying to break down U.S. system and networks in order to obtain classified information or disrupt U.S.' critical infrastructure. This is why U.S. is triggered to address proper policy in order to ensure its own security. As delivered by Obama in his speech about cybersecurity in Stanford University, he described that great harm can threaten the U.S. since in Military sector for example is proven being attacked by hackers from Russia and China, which then Obama declared that cyberthreat is a challenge for U.S. National Security (Secretary, 2015).

Second, the decision-making process model by David Easton will help the writer of this research in explaining the factors behind the considerations of U.S. government under Obama administration to increase the development of cybersecurity over its critical infrastructure. The writer will examine deeply what kind of input that the society, political elites and international context have given the force to the U.S. government to create the decisions in form of state policy that

focuses more on the cybersecurity. Furthermore, the writer will use both original David Easton's decision-making process model that is emphasized on structure as well as the revisited model suggested by Gabriel Almond in which the writer thinks it will be quite relevant since Almond also emphasizes on functional aspects of structure within the political system itself.

The concept of national interest and the decision-making process model is believed by the writer to explain the relations between how national security, one of U.S. national interest in this globalized era is put in risk and then consequently will lead to the mechanism of decision-making process as form of U.S. consciousness to create policy that will able to secure its cybersecurity holistically.

D. Hypothesis

The urgency of United States of America to increase the development of cybersecurity over its critical infrastructure under the Obama administration is because of two conditions. Those are:

1. Internationally, there are many potential risks of cyberthreat from foreign countries that can threaten U.S.' cybersecurity
2. Domestically, there are demand and support from the elements of U.S. statehood especially coming from non-state actors such as interest group, scholars and academician as well as political elites.

E. Range of Research

In order to provide a comprehensive explanation, this research will explain the case related to the urgency of United States of America to increase the development of cybersecurity over its critical infrastructure under the Obama administration. Therefore, the time limitation will be specifically confined under Obama administration only. However, other relevant data related to another presidential administration will also be used in order to provide a comprehensive comparison towards the analyses of this research. Furthermore, the fact that critical infrastructures of the U.S. are consisted of 16 sectors, the writer then will only take three most important sectors within the U.S. critical infrastructures itself that are giving most of the information and illustrating the purpose of this research itself, considerably those sectors are energy sector, critical manufacturing sector and transportation sector.

F. Purpose of Research

This research aims at:

1. examining the triggering factors and events that are influencing U.S. in concerning the issue about cybersecurity over its critical infrastructure.
2. examining three critical infrastructures that are holding the most impacted and reasonable motivation for U.S. to be cyber-secured in accordance with cyberthreats that are attempted by many state actors.
3. examining the domestic policy that addressed by U.S. in ensuring its cybersecurity over critical infrastructure and also its foreign policy towards other countries in this issues.

4. developing the knowledge of the writer as well as fulfilling the requirement to be a graduate of International Relations.

G. Research Methodology

During the making-process of this research, the writer will use an explanative research method that involves a deep exploratory research with the process of collecting facts using qualitative data which combined with personal analysis using specific theory and concept as mentioned previously.

The method of collecting data is in the form of secondary data sources. It means that the source of this research will mainly be taken from books, journals, articles and encyclopedia both in copied form and in e-resource taken from the internet. The writer believes that by using such sources will enable the exploration of data towards a comprehensive and reliable data.

H. System of Writing

The system of writing of this research will be arranged as follows:

Chapter I: This chapter is an Introductory part of the research which contains Background, Research question, Theoretical Framework, Hypothesis, Scope of Method, Methodology, Purpose of Research and the System of Writing.

Chapter II: This chapter will provide an explanation related to globalization as an issue that gives influence toward the development of cybersecurity in general.

Chapter III: This chapter will explain the perspective of U.S. government on the issue of cybersecurity and its development throughout history specifically on critical infrastructure aspects as well as comparison between Bush and Obama administration within this issue.

Chapter IV: This chapter will try to prove the hypotheses that there are International and Domestic factors which influence the Obama administration to increase the cybersecurity development using the Decision-Making process model introduced by David Easton

Chapter V: This is the end of the research that will conclude all the findings in form of conclusion.