# CHAPTER V

# CONCLUSION

The emergence of globalization as a contemporary phenomenon in International relations has been bringing many issues to be examined further. Where the past globalization was merely perceived as the falling trade barriers that facilitated the movement of people, good and services and capital, such definition has been developed wider nowadays, especially with the advancement of technology such as internet which also influenced the way government conducted its statehood live in servicing its citizens.

However, the dilemma then emerged as the utilization of technology did not only give facilitation towards the government in conducting the statehood live but it also was accompanied along with the risks. In the past, there were not many things managed by networks and internet. The threat only happened to be in the form of physical threat such as the damage of computers assets. However, in current era, as many sectors in state known as critical infrastructure which comprised of many important sectors providing basic service for its citizens were managed more by networks in the cyberworld, the risk also increased along with the growing threat. Such concern has been becoming focus for many states around the world including for the U.S.. As a growing major power, the assurance over its security stability including in cybersecurity is a focal concern and has been becoming one of U.S. national interests.

U.S. defined cybersecurity as protection effort towards critical infrastructure sectors, then it was no wonder that critical infrastructure could be

such a main concern for U.S. because of its important features in serving American citizens that its destruction or disturbances could have weakened effect for the state. The examples of most prioritized critical infrastructures for U.S. were energy sectors, critical manufacturing sector and also transportation sector. Those three sectors in fact were very important as they served U.S. citizens for most basic needs such as electricity and mobility needs which each sector also had interdependent feature that supported other sectors. If one could possibly be broken down by cyberthreat then the loss would also be impacting other sectors.

Main disturbances usually threatening U.S. critical infrastructures were argued to be mainly caused by cyberthreat. It was said so due to the fact that almost all of those critical infrastructure sectors were currently managed by network system purposely functioned to provide an effective management in less costly ways. However, such system was vulnerable due to its openness characteristics with high potential to be interfered by cyberthreat. One of the concrete examples of system that was used by U.S. government known as Industrial Control System.

Admitting such crucial characteristic of cybersecurity in critical infrastructure aspects, U.S. government especially under Obama administrationwas trying to improve this cybersecurity issues which were proven by the increasing budget on FISMA and total IT spending implemented by many U.S. federal agencies. Such improvement in cybersecurity under the Obama administration was mainly influenced by different environmental factors that existed within his presidential era which was quite different from his predecessor.

In one hand, Bush administration was much busier in handling the physical counterterrorism effort due to the major terrorism case of 9/11 attack by alternating more hard power. Meanwhile, Obama had much more vision on cybersecurity issue as it can be one of ways for U.S. to renew its devastating image caused by the previous administration as well as to respond towards the growing cyberthreat towards the critical infrastructures.

The increasing cyberthreats that seized U.S. focus to improve its cybersecurity on critical infrastructure were mainly derived from the International environment. China and North Korea were among the states claimed by U.S. to play major role on breaking U.S. networks. There were so many investigations done by U.S. agencies found out China based IP Addresses were among the top list of cyber originated intrusions. North Korea in the other hand was popular with its Sony Pictures cyberattack case which was presumably caused by the Sony's new satirical movie release regarding the North Korean leader and consequently causing the cyberattack that leaked Sony pictures confidential assets and information. Furthermore, not only direct cyberattack experience that inspired U.S. to improve its critical infrastructure cybersecurity but also influence by other state experience such as Ukraine in its power outage case. This Ukrainian case inspired U.S. how such important energy sector could also possibly be interfered by cyberthreat.

Furthermore, the existence of demand and support from the domestic U.S. statehood also became the reason behind the improvement of its critical infrastructure cybersecurity. In one hand, demands coming from the society such

as interest group and professional scholars have shaped U.S. view on cybersecurity as knowledge and understanding owned by those interest groups and scholars had given them overview about the urgency of cybersecurity and then triggered them to provide an advocacy effort to recommend the update of U.S. public policy.

Second, political elite that also became the source of the demand 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 strongly interlinked with the international environmental factor. In this extent, even though there was no state demanded U.S. to improve its cybersecurity but 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 coming from the domestic condition happened to be from U.S. citizens who became more aware in cybersecurity issues. This awareness thus has directed consequences upon their support towards the government as illustrated by society willingness to pay tax as one of government revenues and capitals to improve many U.S. state aspects including cybersecurity.

Overall, U.S. improvement on cybersecurity over critical infrastructures under Obama administration was proven to be caused by International and domestic factors that successfully shaped U.S. view on how urgent the cybersecurity issues were. Such improvement was considered necessary as the

growing cyberthreat could possibly give devastating effect towards U.S. national interest which is security in general and cybersecurity in specific.

Furthermore, in general, this undergraduate thesis research was highly inspired by several studies and subjects whom the writer had taken during her study in this undergraduate degree such as Contemporary Issues in International relations where cyber related issues were considered as a new emerging phenomenon, Sovereignty and Globalization studies which had provided much of information for chapter two as well as United States Foreign Politics where the discussion related to U.S. governance was pretty much inspiring and gave much inputs to the writer in conducting this research.

Also, the writer personally wished that this thesis research can give contribution towards the study of both International relations in general as well as within the study of cybersecurity related issues in specific as in fact even in Universitas Muhammadiyah Yogyakarta's thesis repository, the writer found there were not much students that discussed this issues in their thesis while this topic now can be considered as one of the most contemporary issue where pretty much literatures can be used as a new research topic basis. Thus, the writer also suggested for the further inquiry for any scholars and readers of this undergraduate thesis that were interested in this study to perform another research in related issues of cybersecurity with whole new different scope and research object for example research of cybersecurity in Indonesia scope or perhaps in another regions in order to examine different cases which probably can reveal new interesting facts and information.