CHAPTER I

INTRODUCTION

1.1 Background

The objective of state defense is to guard and avoid squandering the integrity of the Unitary State of the Republic of Indonesia, as well as the state's sovereignty and security from all forms of threats, whether military or non-military in nature. Misuse of technology and data on the internet is one of the unsoldierly risks that likely undermines the sovereignty and security of the nation-state. Each state and non-state actor initiates the danger of free-roaming cyber-attacks. The actors might also be a single person, a group of people, a faction, a company, or even a country[1]. As a result, the government must foresee cyber dangers by developing cyber security methods and determining complete tactics to protect against cyber-attacks; their variations, and therefore the scope of counter-measures, as well as laying the groundwork for law.

The importance of cybersecurity has become even more essential as a result of the internet's darker side. It has been widely proposed to provide nearly complete access to pornography. According to a recent widely publicized poll, more than eighty percent of the photos on the internet are pornographic. While the poll result was revealed to be utterly wrong, the remark that the internet may and does include unlawful, unpleasant, or simply illegitimate information is perfectly fair. It also aids

[1] Rizal, Muhamad, and Yanyan Yani. "Cybersecurity Policy and Its Implementation in Indonesia". JAS (Journal of ASEAN Studies) 4, no. 1 (2016): 61. doi:10.21512/jas.v4i1.967

dishonest traders, terrorist data exchanges, sexual predators, software package pirates, computer hackers, and other criminals.[2]

Cyber Security is a new thing in Indonesia that maybe only a few people knows about its existence, therefore the government has to educate a lot about the cyber security itself to the people and educate more about how to avoid the cybercrimes or cyber-attacks. Cyber security is an advancement and development of technology and security systems, which can be said that its development is important in this era of globalization and technological development. The use of cyber security itself is useful for preventing cybercrime that specifically targets information sources. In general, cyber security is better known as an effort to protect information from cyber-attacks. Cyber-attack itself is an action that is deliberately carried out by one or a group of people to disturb confidentiality, integrity, and data availability. [3]

The tremendous advancement of information technology has transformed the face of the globe and shifted our understanding of what it means to be a nation's power, as well as demonstrating a dispersion of that understanding. A nation's power is measured not only by the size of its economy or the might of its military, but also by the values it provides the world, one of which is its mastery of technology. Almost all actions in the 21st century, from personal to government, rely on the usage of information technology. The use of information technology for harmful objectives endangers a country's national defence. Threats can be both

[2] Barrett, Neil. *Digital Crime: Policing The Cybernation*. London: Kogan Page, 1998.

[3] Boisot, Max. *Knowledge Assets: Securing Competitive Advantage in The Information Economy.* Oxford: Oxford University Press, 1998.

military and non-military in nature. Military risks to national defence are dangers to defence and security, whereas non-military threats to national defence are threats to a country's ideological, political, economic, social, and cultural resilience. The advancement of technology will, sooner or later, impact our cultural conventions, socio-cultural institutions, and (from a socio-political standpoint) our government's decision-making patterns.[4]

It is also critical for national security that information and data be protected, dominated, and managed at the national level through cyber security. Cyber security is strongly linked to data operation, which encompasses a wide range of parties including armed forces, government agencies, state-owned companies, academic institutions, the private sector, individuals, and the global community. Physical security, which encompasses all or any physical components such as data center buildings, disaster recovery systems, and transmission media, is just as important as cyber security when it comes to ensuring the continuation of data operations.

Because of an inaccurate technology development strategy that ignores scientific and technical evaluations, the Republic of Indonesia may be a little behind in keeping up with the rise of information technology. As a consequence, Indonesia has become a non-technologically based nation as a result of technology transfers from industrialized industrial countries. It is possible that a lack of cyber defense might lead to international tensions as well as a deterioration in security and connection between countries. The phrases "cyber" and "security" form the core of

[4] Sudarsono, Juwono. *Ilmu, Teknologi, Dan Etika Berprofesi: Pandangan Sosial Politik. Jakarta: Masyarakat Jurnal Sosiologi*, FISIP UI-Gramedia, 1992.

the phrase "cyber security." Talking about cyber requires discussing information, connections (telecommunication services, networking), gateways (computer systems, gadgets and users), rooms, or locations, as well as the internet. Security, on the other hand, is often associated with the protection of one's assets. Protecting information and systems from major cyber threats is a primary goal of security. This includes the preservation of quality and the protection of computers, networks, programs and knowledge from unexpected or illegal access.[5]

In Indonesia, a cyber-security system and policy have been established, which are controlled by government agencies and the official community. The Ministry of Communication and Science (MCS) is responsible for coordinating cyber security policies (MCI). The Information Security Coordination Team, the Board of Information Security, and the Indonesian Internet Infrastructure Security Incident Response Team are all government institutions that deal with cyber security in Indonesia (ID-SIRTII). The information security coordination Team was formed in April 2010 to monitor cyber security, which is concerned with the acquisition and application of knowledge and monitoring in the sphere of information and technology.

In terms of information security governance, the board of information security is in charge of formulating and implementing policies, as well as monitoring, analysing, and reporting on such policies. In addition, the Minister of Communication and Informatics established ID-SIRTII as a government-supported rule that was implemented in 2012. A second segment of Indonesian citizens is

[5] Ibid p. 28

worried about cyber security. Supporting business ID-CERT works with the Indonesian government in special cases to help ensure that cyber security in Indonesia is properly implemented. The ID-SIRTII, for example, relies on ID-CERT as a support institution. An additional community organization for Indonesian universities who want to concentrate on security improvement is the Indonesia Academic Computer Security Incident Response Team (ID-ACAD-CSIRT). Currently, ID-CSIRT has 40 academic CSIRT members from various universities.[6]

1.2 Research Questions

1. What is the challenges of cyber security in Indonesia?
2. How does Indonesia Government respond to the cybercrime challenges and obstacles in comparison with Georgia Government?

1.3 Research Objective

The objective of this thesis is to find out and analyze the function and the existence of cyber security impacts towards Indonesia national security and also the implementation of cyber security in Indonesia. The outcome of this thesis will produce a perspective that cyber security does not only work in one area but can be useful for many fields, especially in the Indonesia national security system.

[6] Setiadi, Farisya, Yudho Giri Sucahyo, and Zainal A. Hasibuan. "An Overview of the Development Indonesia National Cyber Security.". *International Journal of Technology & Computer Science (IJTCS)* 6, no. (2012): 111.

1.4 Research Significance

The author hope with the result of this thesis will educate the uneducated people about the impacts of cyber security in order to point out that cyber security is very important in this era of globalization and technological advancement. The author hope this thesis would be beneficial for the readers to add insight into the importance of cyber security in the cyber world, as well as the positive impact it has on Indonesia national security. The author hope that this thesis could raise the awareness of the government, so the government can improve the development of cyber security technology in the midst of this globalization era because cyber security is an important thing in this era and in the future, in maintaining cyber security world and in maintaining Indonesia's national security itself.

1.5 Structure of Thesis

The systematics of writing in this study is divided into five parts, consisting of:

CHAPTER 1: The discussion in this chapter is the author explains the background of the chosen topic, determines the questions from the problem formulation, and explains the objectives and benefits of implementing this research.

CHAPTER 2: In this second part, the author develops a framework of thought that will be used in the research. This chapter is divided into two parts, the first contains a literature review, in this section the author describes a study of previous research that the author will use, then the second is a review of theories and concepts that will help the author answer the formulation of the problem in this research.

CHAPTER 3: In this chapter, the author describes the method that will be used in completing this research. From the approach used, namely qualitative, descriptive research methods, data collection techniques and data analysis techniques.

CHAPTER 4: This section is the main point or the highlight of the research and thesis. The most important finding or the most notable aspect of the study and thesis. The author will show all of the data that has been gathered in a systematic way and in line with the theories and ideas that have been developed to answer and address the research issue that is the subject of this dissertation.

CHAPTER 5: In the last part, namely the conclusion, the author will explain the interpretation of the results of the research that has been done. The author will also provide opinions and suggestions regarding the relationship.