CHAPTER 1

INTRODUCTION

1.1. Background

Robert Tappan Morris, a PhD student at Cornell University, created a method to estimate the extent of the internet in 1988. The application would crawl the internet, install itself on other computers, and then count the number of copies it made. When the results are tallied, they will show the number of machines that are connected to the internet. With each installation, the infected PCs deteriorated gradually until they crashed. It was the first Distributed Denial of Service (DDoS) attack, and it was completely unintentional. (Townsend, n.d)

More than three decades after the first cyberattack, cyber threats are increasing in conjunction with human reliance on technology (figure 1). It is unknown when the first cyber attack occurred in Indonesia, but since the government assisted Badan Siber dan Sandi Negara or National Cyber and Crypto Agency (BSSN) in 2017, it has been clear that Indonesia is one of the countries that frequently faces cyber attacks.

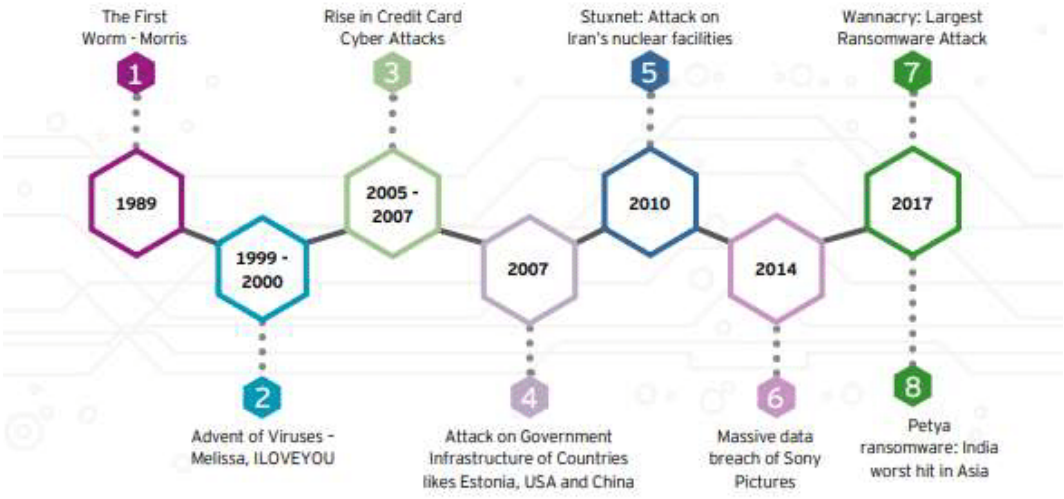

Figure 1.1. Timeline of Cyber Attacks (1989-2017)

Source : Clim, A. (2019).

According to International Telecommunication Union (ITU) Global Cyber Security Index (GCI), Indonesia was placed 24th internationally in the 2020. There was a significant increase when compared to Indonesia's position in 2018 which was ranked 41st. (ITU Cyber security team, 2021)

Asia-Pacific region

Member State	Score	Regional Rank	Global Rank
Singapore	0.898	1	6
Malaysia	0.893	2	8
Australia	0.890	3	10
Japan	0.880	4	14
Republic of Korea	0.873	5	15
China	0.828	6	27
Thailand	0.796	7	35
New Zealand*	0.789	8	36
Indonesia	0.776	9	41
India	0.719	10	47
Viet Nam	0.693	11	50
Philippines	0.643	12	58
Iran	0.641	13	60

Figure 1.2. Global Cyber Security Index 2018
Source : ITU Global Cyber Security Index 2018

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10

Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38

Figure 1.3. Global Cyber Security Index 2020
Source : ITU Global Cyber Security Index 2020

In contrast to Indonesia, Australia is more advanced in terms of cyber security developments. According to the Global Cyber Security Index 2020 statistics, Australia is ranked 12th in the world, much ahead of Indonesia, which is ranked 24th. Despite the fact that Australia is immediately above Indonesia in fifth and sixth place in the Asia-Pacific region. (ITU Cyber security team, 2021)

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14

Country Name	Overall Score	Regional Rank
Korea (Rep. of)	98.52	1
Singapore	98.52	1
Malaysia	98.06	2
Japan	97.82	3
India	97.49	4
Australia	97.47	5
Indonesia	94.88	6
Viet Nam	94.55	7
China	92.53	8
Thailand	86.5	9
New Zealand**	84.04	10

Figure 1.4. Australia's Position in GCI 2020 (Global and Asia Pacific)

Source : ITU Global Cyber Security Index 2020

According to Presidential Regulation of the Republic of Indonesia Number 82 of 2022 concerning Protection of Vital Information Infrastructure. It is stated that one of the scopes of Vital Information Infrastructure is the defense sector. The Ministry of Defense will be the lead of this sector. The Ministry of Defense has previously issued a policy regarding Regulation of the Minister of Defense of the Republic of Indonesia number 82 of 2014 concerning Cyber Defense Guidelines. This rule establishes the embodiment determination, concept, and will to carry out cyber defense on

information systems, control, and communication in the defense sector. This handbook embodies the framework for implementing cyber defense, which must be understood and guided by each individual in accordance with their tasks and functions.

And based on the Minister of Defense Regulation Number 14 of 2019 concerning the Organization and Work Procedure of the Ministry of Defense, the Ministry of Defense established a new organizational structure in which there is Pusat Pertahanan Siber or Pushansiber (Cyber Defense Center) under Badan Instalasi Strategis Pertahanan (Defense Strategic Installation Unit) which has the task of implementing governance, cooperation, operations and cyber defense security assurance.

Based on these circumstances, Indonesia attempts to strengthen its cyber capacity building through cooperation with other parties/countries. This become one of the foundations of Indonesia in cyber security development. One of Indonesia's efforts, especially in the defense sector, is to establish cyber cooperation with Australia. This is realized by cyber cooperation in the Defense Cooperation Arrangement (DCA) between the Indonesian and Australian ministries of defense in 2018. Together with this, a Memorandum of Understanding (MoU) in the field of cybersecurity was signed in the same year between BSSN and Department of Foreign Affairs and Trade (DFAT). The cooperation is as part of the outcomes of the 2+2 dialogue meeting between Indonesia and Australia.

However, the fact is that cyber threats in Indonesia continue to increase. According to data from Pusat Operasi Keamanan Siber Nasional (National Cyber Security Operations Center) BSSN, there has been a two-fold rise in cyber attacks against Indonesia from 2020 to 2021. There have been roughly 490 million cyberattacks during the first year of the Covid-19 pandemic, with a huge spike of nearly one billion cyberattacks in 2021. This record indicates that the trend of cyber-attacks will continue to rise as people shift from physical to online activities. Malware infection is the most frequent attack, accounting for 62% of all attacks, followed by trojan activity (10%)

and target information collection effort (9%). Attacks reached a record high of 1.652.521.839 by end of 2021, and it is expected that number will continue to grow in 2022. According to research by Frost and Sullivan that was started for Microsoft in 2018, cyber security has cost Indonesia a deficit of up to 478.8 trillion IDR, or 34.2 billion USD, and it continues to grow on occasion.

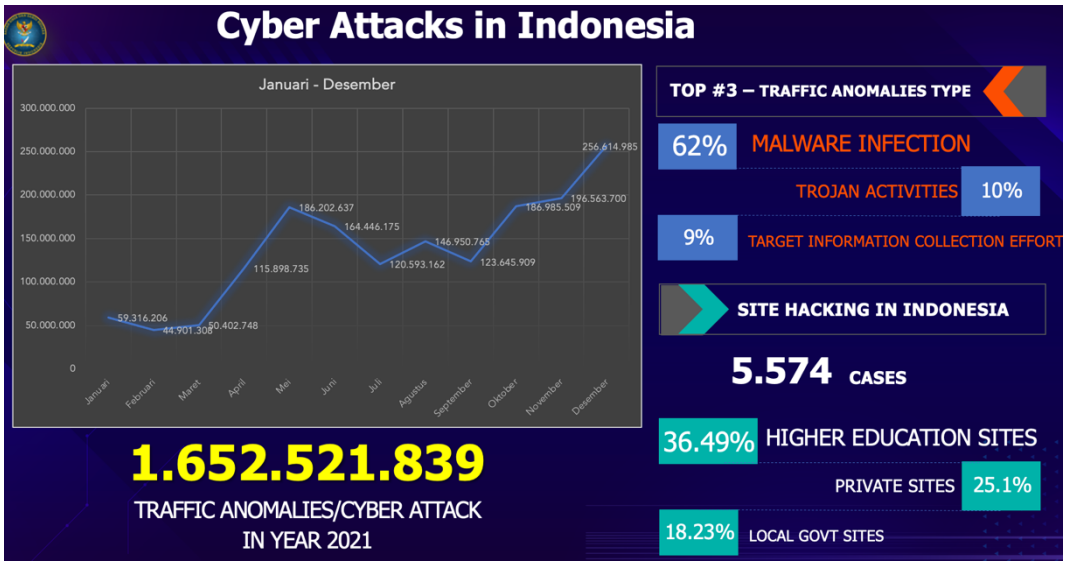

Figure 1.5. Indonesia`s Cyber Attack Report 2021
Source : www.bssn.go.id

Another fact is that Pushansiber, the Ministry of Defense's leading cyber defense sector, remains to perform inadequately. According to Nur Arifina, the most significant impediments in Pushansiber are funding and human resources. The administration has not taken seriously the provision of a cyber budget. To improve and reinforce the cyber defense system, it is important to restructure and develop. Pushansiber's position in the cyber system sector is vulnerable due to several limitations. Based on the principle of system network security, there is still very limited support from the government to carry out the newest security to deal with present cyber threats. (Arifina, N., 2021)

Based on the above conditions, it is necessary to take action from the Ministry of Defense to be able to strengthen its cyber defense.

Strengthening and developing Pushansiber is very important in efforts to build cyber defense in the defense sector.

1.2. Focus and Sub-focus

1.2.1. Focus

Based on the background described above, the research focus is the establishment of cyber cooperation between Indonesia and Australia in the defense sector to deal with cyber threats escalation in Indonesia as a challenge for Indonesia. In this regard, the implementation of cyber cooperation in the current DCA and MoU will be analyzed. This was done in order to provide consideration for Indonesia's defense diplomacy in improving bilateral cyber cooperation with Australia.

1.2.2. Sub Focus

From the focus defined above, the sub focus to study in this research will be as follows:

a. the implementation of cyber cooperation in the current DCA and MoU from 2018 to 2022.
b. the course of action taken by Ministry of Defense in order to improve cyber defense capacity building through cyber cooperation.

Knowing the current conditions of cyber cooperation implementation and course of action taken related to cyber cooperation in the defense sector is expected to provide an analysis to increase cyber defense capacity in the future.

1.3. Problem Formulation

DCA is a defense cooperation between the Indonesian and Australian ministries of defense. Defense cooperation between the two countries has existed for a long time, even before DCA existed. However, regarding cyber cooperation between the two Ministries of Defense, this is

certainly a new scope of cooperation. This is certainly a challenge for the defense sector to be able to increase its cyber defense capacity building through this cooperation.

With these backdrops and explanations which is previously described, the research question to raise are as follows:

a. *How was the implementation of cyber cooperation in DCA and MoU in terms of cyber defense capacity building from 2018 to 2022?*
b. *How was Ministry of Defense's course of action in order to improve cyber defense capacity building through cyber cooperation ?*

Thus, speaking of cyber cooperation for cyber defense capacity building, it will fully consider Indonesia's defense policy and national security.

1.4. Research Objectives

In accordance with the defined research inquiries, the objectives of the research to obtain are as follows:

a. To scrutinize the results of cyber cooperation that has been established in DCA and MoU in terms of increasing cyber defense capacity 2018-2022.
b. To define possible actions related to cyber cooperation in the defense sector in order to strengthened Indonesia's cyber defense capacity building.

1.5. Research Benefits

1.5.1. Theoretical Benefits

The result of this research is expectantly able to provide a horizon regarding the implementation of Indonesian defense diplomacy for cyber defense capacity building. Besides that, the research can also provide insight, information, and depiction for the development of defense diplomacy study.

1.5.2. Practical Benefits

This research can be considered as another reference example related to the implementation of defense diplomacy between the two countries. In addition, it can enrich the literature that studies bilateral relations between Indonesia and Australia in the defense sector in general, and cyber cooperation in particular. Again, it hopefully can be useful for other parties who want to broaden their horizons regarding cyber cooperation. It is also for the Government of Indonesia, in particular the Ministry of Defense, to carry out what is stated in the 2020-2024 general national defense policy. According to Article 2 of the Regulation Number 8 of 2021, the General Policy is aimed at improving national defense capabilities through improving non-military defensive capability executed by government ministries, institutions, and regional governments by optimizing the use of national resources for national defense. Apart from that, it is also to provide a scientific contribution to support the realization of the national cyber security law.