CHAPTER 2

LITERATURE REVIEW

2.1. Theoretical Framework

2.1.1. National Security

According to Major General Budi Pramono (Pramono, 2021) based on the TNI Law and TNI revisions since 1998, two notions are constantly compared: (1) defense (defense/defense) and (2) security (security). The term "defense" refers to an endeavor or activity, whereas "security" refers to a state or condition and is a result or consequence (of a process). The phrase "defense" is typically connected with politics and government (the state), whereas the term "security" encompasses a broader topic, namely national security and security of life inside the state, both general (public) and individual. Defense activities will determine national security conditions, but security is determined by numerous elements, not just defense efforts. Defense (when translated into measurable objects) is not the only aspect that explains security when defined theoretically.

National security is not the same as public security. National security is concerned with the existence, integrity, and sovereignty of the state. But public security is concerned with the existence/groups of people who normally reside in the state. The first domain are bound by political bonds, while the second domain are bound by social bonds. A threat/disruption to state security is not always a threat/disruption to an individual/group/community.

Based on the threat escalation perspective, the disturbances of security are perceived as growing from the lightest or individual forms to the most severe or gigantic. Security situations are classified as safe, vulnerable, critical, or crisis. Security can also be viewed through other lenses, such as common security, cooperative security, and comprehensive security. Common security thinks that hostile actor relations can be altered

by enacting security measures that are mutually transparent and non-aggressive. The basic purpose is to eliminate mutual suspicion of the other party's intentions in order to avoid armed conflict (security dilemma). Cooperative security strives to improve understanding of security as the definition of security evolves, including environmental, economic, and social dimensions. The primary focus is on averting conflicts between countries as well as maintaining the status quo within the country itself. The cooperative pattern is utilized to ensure the safety of individuals and groups inside the state.

Furthermore, non-state actors are active in cooperative security to develop the habit of conversation and collaboration among countries. In contrast, comprehensive security refers to anything that is directly or indirectly related to human welfare. The state must prepare multiple security actors to manage this idea. In this setting, security is no longer limited to military challenges, but also includes ideologies, politics, and economics at the domestic, bilateral, regional, and global levels.

Cyber threats are one type of non-military threat that has the ability to damage national security. As we all know, Russia's military campaign against Ukraine was preceded by a huge cyber offensive against Ukraine. Cyber threats can be classified as proxy conflicts or, more accurately, war by proxy. According to Gatot Nurmantyo, the Fourth Generation War carried out by deterioration from inside, notably without resorting to violence, not employing hard power, but rather soft power. This should surely be a worry for Indonesia in order to boost its cyber security.

Based on the explanation above, cyber security as a non-military threat has developed into a threat that can endanger national security. Cyber security can be used as an element of proxy warfare or it can even develop into a hybrid threat as happened in Ukraine. For this reason, capabilities in the defense sector are also needed in order to overcome these cyber threats.

2.1.2. Cyber Security

According to (Ardiyanti, 2014) cyber security is a set of tools, which can be utilized to safeguard the cyber environment as well as organizational and user assets. In cyber security, organizational and user assets transferred and/or stored in a virtual environment. Cyber-security is an endeavor to ensure the acquisition and preservation of characteristics. Defending institutional security and user data Global cyber-security is based on five areas of expertise:

a. Legal certainty (cyber crime law);
b. technical and procedural (end users and business (direct approach and service providers and companies software);
c. organizational structure (highly developed organizational structure, avoid duplication);
d. capacity building and education Users (public advocacy and communications accessible to the latest cyber crime threats);
e. International cooperation (includes mutual cooperation in attempts to combat cyber threats) (rules governing cybercrime);

According to The European Union Agency for Cyber security (ENISA) (Joint Research Centre, 2020) cyber security has evolved into a linear multidomain discipline that encompasses numerous fields and approaches. Indeed, because of the connections between the various aspects of our digital and physical lives, the concept of cyber security incorporates knowledge from a wide range of scientific disciplines, some of which are quite distant. According to the most official standard ISO/IEC 27032:2012:

'Cyber security is described as the 'protection of information confidentiality, integrity, and availability in cyberspace.'

The key principles of cyber security are frequently described as confidentiality, integrity, and availability. (Joint Research Centre, 2020)

a. Confidentiality would be the concealing of information or resources, according to a broad definition.
b. Integrity refers to such dependability of data or resources (and is meant as a collection of safeguards against unauthorized or incorrect alterations).
c. Availability refers to the capacity to legitimately use the necessary information or resources (services).

Understanding how Cyber security is interrelated to other specialisations and the technological areas that are its main drivers, on the other hand, is a very important topic that touches on several elements of cyber security policymaking, such as: (Joint Research Centre, 2020)

a. The capabilities of a Cyber security expert to be considered in generating and fostering coherent syllabuses in education;
b. The science based domains to be boosted to enhance the advancement of Cyber security as a discipline;
c. The market areas to be stimulated in order to establish a more robust Cyber security industry.

Based on these considerations, the European Commission issued an overall Cyber security taxonomy in 2018, which was evaluated by leading Cyber security organizations and a poll including over 700 European research centers. This taxonomy provides a clear and precise indication of fundamental research fields and corresponding sectorial domains. A three dimensional depiction of the Cyber security world can be generated by merging two aspects with existing applications and technology in the digital society, as shown in Figure 6.

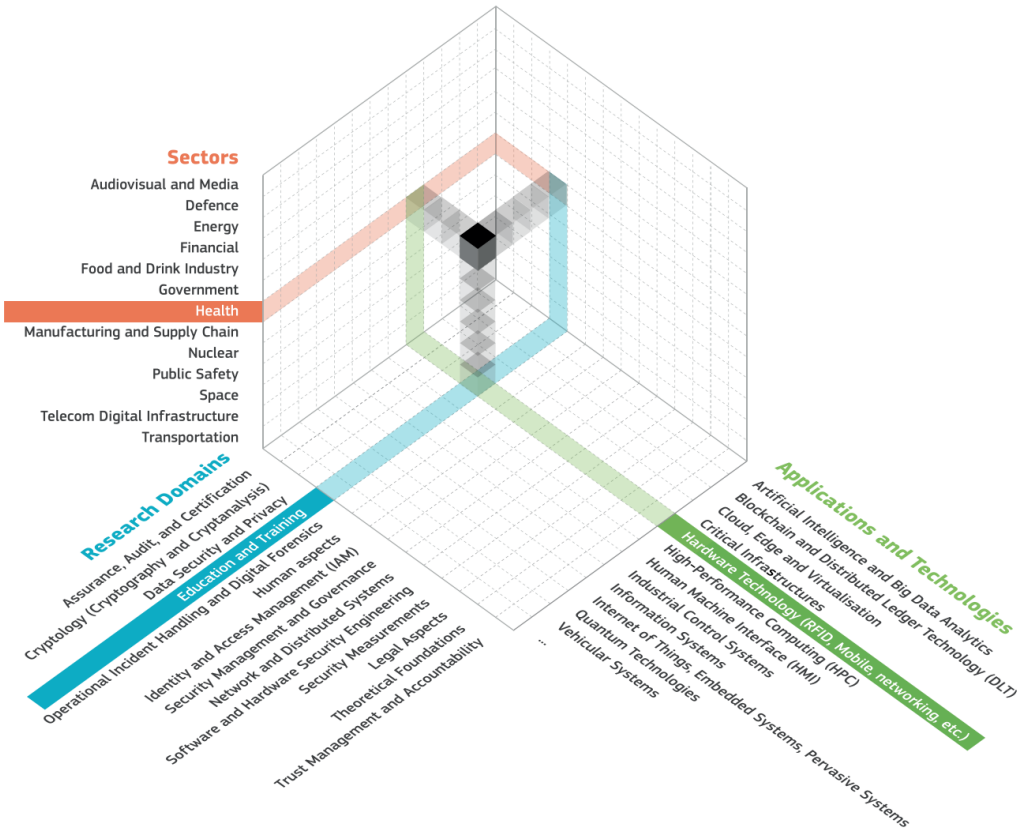

Figure 2.1 Three Dimensions of Cyber Security

Source : Cyber security, our digital anchor, Joint Research Centre. (2020).

Cyber security is portrayed as a broad, complex discipline rather than as a subfield of computer science. While it is present everywhere, each component of this cube necessitates unique theoretical approaches as well as technical execution and expertise.

Cyber security is a complex field in which all sectors, industries, and stakeholders are involved, either vertically and horizontally. Political, economic, and social factors must work together to improve the development of the national capacities. Enforcement, legal authorities, academic institutions, ministry, private sector operators, technology developers, public-private partnerships, and intra-state engagement can all help with this. The ITU model for international multi-stakeholder cyber security cooperation strives to create synergies between existing and future

projects and focuses on the five pillars listed below, which shape the basic building blocks of a cyber security culture. (ITU Cyber security team, 2021)

Figure 2.2. Cyber Security Agenda (5 pillars)

Source : www.unodc.org

a. Legal Measures

Measures based on the presence of legal frameworks addressing cyber security and cybercrime. Legal measures (covering legislation, regulation, and spam laws containment) allow a state to establish basic reaction mechanisms such as crime investigation and prosecution, as well as the enforcement of sanctions for noncompliance or breach of law. A legislative framework establishes the minimal level of behavior upon which additional cyber security capacities can be built. Fundamentally, the goal is to have enough legislation

in place to standardize practices at the regional/international level and ease international cybercrime combat.(ITU Cyber security team, 2021)

b. Technical Measures

Measures due to existence of technological institutions and frameworks dealing with cyber security. Effective ICT development and use can only thrive in an environment of trust and security. Countries must therefore develop and implement approved basic requirements and accreditation processes for software systems and applications. These efforts must be supplemented by the establishment of a national organization handling with cyber security incidents, an authorized government agency, and a national framework to monitor, alert, and respond to incidents.(ITU Cyber security team, 2021)

c. Organizational Measures

Measures based on the presence of synchronization institutions, policies, and plans for national cyber security development. Organizational measures include defining cyber security strategic priorities plans, as well as formalizing organisational roles, responsibilities, and accountability to assure their implementation. These safeguards are required to support the development and implementation of effective cyber security posture. The state must establish broad strategic aims and objectives, as well as an all-inclusive strategy for implementation, delivery, and monitoring. National agencies should be involved to execute the plan and assess its effectiveness. Without a national plan, governance model, and regulatory authority, activities in many sectors become contentious, impeding efforts to achieve successful cyber

security development harmonization.(ITU Cyber security team, 2021)

d. Capacity Building Measures

Measures based on the presence of research and development, training and education programs, qualified professionals, and public sector organizations that promote capacity building. Capacity building comprises public awareness campaigns, a framework for cyber security professional certification and accreditation, professional cyber security training courses, educational programs or academic curriculum, and so on. This pillar is inextricably linked to the first three (legal, technical and organizational). Despite the fact that there are significant socioeconomic and political repercussions, cyber security is frequently approached from a technological standpoint. Building institutional and human capacity is critical for raising awareness, knowledge, and know-how across sectors, implementing rational and effective solutions, and promoting the growth of skilled professionals.(ITU Cyber security team, 2021)

e. Cooperative Measures

Measures due to the presence of collaborative frameworks, partnerships, and information exchange networks. Cyber security is a collective responsibility as well as a transnational challenge as a result of unprecedented levels of interconnection between states. Greater collaboration can lead to the establishment of considerably stronger cyber security capabilities, reducing cyber threats and allowing for improved investigation, apprehending, and conviction of malicious agents.(ITU Cyber security team, 2021)

In terms of cyber cooperation between Indonesia and Australia in relation to the concepts and theories mentioned above, this is, of course, consistent with what was issued by the International Telecommunication Union (ITU), which established 5 (five) pillars for measuring cyber capabilities, namely Legal, Technical, Organizational, Capacity Building, and Cooperation. Meanwhile, researchers will concentrate on two (two) pillars as analytical methods in this study, namely Capacity Building and Cooperation.

2.1.3. Foreign Policy

Foreign policy formulation in the external context is currently undergoing considerable changes. States has to be adaptable in the strategic environment as a result of the use of information technology into foreign policy formulations. James Rosenau mentioned his concept of foreign policy that there are four adaptation patterns:

a. preservative adaptation (adaptable behavior to changes and demands in the internal and external environment);
b. acquiescent adaptation (being concerned regarding internal and external changes);
c. intransigent adaptation (responsive approach to the internal factors); and
d. promotive adaptation (being indifferent to the internal and external environment).

As a result of this adaption, the government must innovate. It has been stated that in the age of globalization, all political decisions constitute foreign policy in some sense. Furthermore, they stated that foreign policy decisions required a strong commitment in the manner of ongoing actions and reactions involving various actors.

Foreign policy is the process of examining, identifying, and solving problems in order to attain national objectives (Hill & Brighi, 2012). Hudson and Day emphasize that foreign policy academics will encounter a

complicated situation ranging from micro to macro analyses. Analysts will work with interdisciplinary fields like as psychology, sociology, organizational culture, anthropology, and others. Foreign policy analysis is an analyst's effort to explain how and why a policy was implemented. Culture, identity, experience, cognitive, and other factors all contribute to the complexity.

According to the mandate of the Law Number 37/1999, the formulation of Indonesian foreign policy actively tries not to interfere in the affairs of other states. But, still creates cooperative relationships based on the principles of togetherness and mutual benefit. As an independent and sovereign country, Indonesia strives to contribute to global peace and social fairness. This is accomplished through foreign relations, which are pursued in collaboration with both the state and international organizations. This strategy is believed to be linked to Indonesia's foreign policy, which is based on the premise of independent and active pursuit of national interests.

Diplomacy, not merely a formal meeting, is used to accomplish Indonesian foreign policy through innovative, active, flexible, and anticipatory concepts. The formulation of Indonesia's foreign policy is carried out through 4 + 1 diplomacy (Augesti, 2019). This diplomacy is concerned with:

a. Increasing Economic Diplomacy
b. Indonesian diplomacy aims to defend Indonesian residents living overseas;
c. Sovereignty and Nationality Diplomacy
d. Increasing Indonesia's Contribution and Leadership in the Region and Around the World, in conjunction with (+1), specifically developing diplomats who are transformative, transparent, and capable of innovating with digital technologies (Fitriani & Vido, 2018).

Departing from the above understanding, Indonesia's foreign policy has adapted to the current strategic environmental conditions, especially in

facing the digital era by continuing to develop its diplomatic capacity regarding the use of digital technology.

2.1.4. Defense Policy

Indonesia has a regulation that serves as a framework for the management of the national defense system. This is stated in Presidential Regulation Number 8 of 2021 on the 2020-2024 General Policy of National Defense. The Regulation also seeks to put into effect the provisions of Article 13 paragraph (2) of Law No. 3 of 2002 on National Defense. According to Article 1 paragraph (1) of the Regulation, the 2020-2024 General Defense Policy serves as a framework for the management of the national defense system. The General National Defense Policy 2020-2024 serves as a guide for planning, implementing, and supervising the national defense system. According to Article 2 of the Regulation, the General Policy is aimed at improving national defense capabilities through the following measures:

a. By building reserve and supporting components, the state defense system for land, sea, and air forces is being implemented.
b. Development and implementation of a large-island defensive strategy.
c. Accountability, transparency, and anti-corruption measures in defense budget administration.
d. Development of the Indonesian National Defense Forces (TNI), capable of strategic deterrence and high mobility, to be deployed both within and outside the jurisdiction of the Unitary State of the Republic of Indonesia in the context of defending sovereignty and protecting national interests.
e. Military sector revitalization as a producer of innovative, strong, independent, and competitive defense and security equipment to meet national defense needs.

f. Expanding international defense cooperation and participation in world peacekeeping missions under the United Nations (UN) and other international institutions in order to contribute to the maintenance of world order and peace
g. Improving non-military defensive capability executed by government ministries, institutions, and regional governments by optimizing the use of national resources for national defense.

Based on these concepts and theories, cyber security is a component of national defense that must be strengthened in terms of non-military defense. This is in accordance with point 7 of Article 2 of the Regulation, which addresses improving non-military defensive capability carried out by government ministries, institutions, and regional governments by optimizing the use of national resources for national defense.

2.1.5. Defense Diplomacy

According to the "Strategic Defence Review" (SPO) concept announced by Britain's Defense Ministry in 1998, defense diplomacy is defined as the peaceful use of defenses in order to produce positive results in the development of bilateral and multilateral ties with a particular country / countries (Dodd and Oakes 1998, p. 22). Defence diplomacy, in their opinion, does not include military operations, but rather encourages forms of cooperation such as:

a. personnel exchange,
b. ship and aircraft exchange,
c. high-level visits and senior commanders,
d. bilateral meetings and dialogue,
e. training and exercises,
f. regional defense forums,
g. military assistance,
h. confidence-building measures, and

i. non-proliferation.

Its primary goal is to foster trust and aid in the establishment of democratic armed forces. It makes a significant contribution to conflict prevention and resolution (Ministry of Defence, London 2011, p. 7).

In 2004, Irish and British researchers A. Cottey and A. Forster offered an expanded definition of defense diplomacy as "peaceful (non-confrontational) employment of armed forces and supporting infrastructure (mainly defense ministries) as a foreign policy and security weapon" (Cottey and Forster 2004, p. 6). This approach broadens the scope of the issue by including both the peaceful use of armed forces, the role of the Ministry of Defence, and the use of defense attachés to prevent wars.

One of the most recent proposals for the definition of defense diplomacy can be found in documents from the Spanish Ministry of Defence. Defense diplomacy defines as "a diverse international activity based on dialogue and cooperation, implemented bilaterally by the defense ministry with allies, partners, and other friendly countries to support the achievement of defense policy and Spanish foreign policy goals" (Ministerio de Defensa, Madrid 2012, p. 18). However, this understanding of the nature and function of defense diplomacy ignores the necessity of multilateral ties or collaborative task implementation inside international organizations. It eliminates an important area of international collaboration by restricting itself to the efforts of its own defense department.

The term "defence diplomacy," coined after the Cold War's end, was prompted by the political need to identify the expanding activities of entities under the jurisdiction of national defense ministries. Its ancestors are from the world of politics, not science. However, there have been attempts to scientifically validate this terminology suggestion, which did not result in a universally recognized definition of defense diplomacy, despite the fact that the notion is widely used in the "scientific circuit" and diplomatic practice.

Researchers from the United Kingdom, Spain, France, Indonesia, South Africa, and other countries are attempting to define defense

diplomacy in light of their own countries' specific situations or security situation. Such definitions, which directly reflect national needs, do not encompass all sectors of defense diplomacy, or even exist at all. As a result, excessive utilitarianism and the emergence of new areas of cooperation are just a few of the issues that complicate the development and reconciliation of the general definition of defense diplomacy.

There is likewise no attempt in the literature to agree on such a definition. On the other hand, there is a widespread belief that defense diplomacy directly leads to increased trust and understanding in international relations. However, there is broad agreement on the general goal of defense diplomacy as a tool to promote the achievement of national objectives and foreign and security policy. It is widely acknowledged that defense diplomacy:

a. It is concerned with reducing hostility and increasing trust among states (in this sense, it is "anchored" in the general tasks of diplomacy);
b. It is to develop stable and long-lasting collaboration and promote transparency in the field of defense in the context of states' regional and global involvement, with the support of "peaceful employment of military troops to prevent conflicts."
c. It may help to achieve common supranational aims;
d. It is intended to influence the modification of partners' positions;
e. It should advocate for the introduction of broad security regulations;
f. It maintains interaction with partners, which may be the purpose of state actions as well as a tool for implementing its special goals

Defence diplomacy has a permanent presence in the system of cooperation between countries and international organizations. Its functional scope is not restricted to "niche" areas of diplomacy or the narrow

"industrial" specialization of persons doing associated activities. It can be used in crisis situations as well as in peaceful cooperation with other governments to define and implement state policy. It is the field of diplomacy that includes support for other countries' armed forces through consultancy, training, or transfer of military equipment and weapons, technical cooperation and defense industries, conducting defense and strategic dialogue, cooperation within military education, exercises involving military resources, and peace and humanitarian missions and operations. It is difficult to disagree with the Australian, Nicholas Floyd, who believes that "defence diplomacy should be closely linked with the design and implementation of international policy" (Floyd 2010, p. 7).

Defense diplomacy is undoubtedly the driving force behind cyber cooperation in the defense sector. Defense diplomacy is a type of diplomacy that strives to collaborate, with the most essential goal of developing capability between countries, often known as capacity building. This is undoubtedly one of the most essential aspects for the defense sector in order to strengthening cyber cooperation with Australia and improve cyber defense capacity building.

2.1.6. Cyber Capacity Building

Capacity building in cyber security architecture issued by the International Telecommunication Union (ITU) is measured based on the existence of research and development, education and training programs, certified professionals, and public sector institutions. (ITU Cyber security team, 2021) Capacity building is integral to the first three pillars (legal, technical and organizational). Despite the fact that there are numerous socioeconomic and political implications, cyber security is frequently approached from a technological standpoint. Building human and institutional capacity is critical for raising awareness, knowledge, and know-how across sectors, implementing systematic and appropriate solutions, and promoting the development of qualified professionals. The number of

research and development, education and training programs, certified professionals, and public sector agencies is used to assess capacity building. (ITU Cyber security team, 2021)

a. Public Cyber Security Awareness Campaigns

   Public awareness efforts include promoting campaigns to reach as many citizens as possible, as well as utilizing NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community centers, community colleges and adult education programs, schools, and parent-teacher organizations to spread the word about safe cyber-behavior online. This includes activities such as creating awareness portals and websites, disseminating support materials, and other relevant activities. (ITU Cyber security team, 2021)

b. Training for Cyber security Professionals

   Existence of sector-specific professional training programs for raising public awareness (e.g., national Cyber security awareness day, week, or month), promoting cyber-security education for workers of various profiles (technical, social sciences, etc.), and promoting professional certification in either the public or private sector. It also includes Cyber security training for law enforcement officers, judges, solicitors, barristers, attorneys, lawyers, paralegals, and other legal actors. This indicator also includes the presence of a government-approved (or endorsed) framework (or frameworks) for professional certification and accreditation in accordance with internationally recognized Cyber security standards. These certifications, accreditations, and standards include, but are not limited to, Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cyber security Forensic Analyst (ISC2), and others. (ITU Cyber security team, 2021)

c. Develop and Support Educational Programmes or Academic Curricula in Cyber Security

Existence and promotion of national education courses and programs in schools, colleges, universities, and other learning institutions to train the next generation in Cyber security-related skills and professions. Cryptoanalysts, digital forensics experts, incident responders, security architects, and penetration testers are examples of Cyber security-related jobs. (ITU Cyber security team, 2021)

d. Cyber security Research and Development Programmes

This indicator tracks investment in national cyber security research and development programs at private, public, academic, non-governmental, and international institutions. It also takes into account the presence of a nationally recognized institutional body supervising the program. Malware analysis, cryptography research, and research into system vulnerabilities, as well as security models and concepts, are all part of cyber security research programs. Cyber security development programs include the creation of hardware or software solutions such as firewalls, intrusion prevention systems, honey pots, and hardware security modules. The presence of an overarching national body is required to improve coordination among the various institutions and resource sharing. (ITU Cyber security team, 2021)

The researcher attempts to expound on the ideas and theories of cyber security, cyber defense, and cyber capacity building in order to build national cyber defense. Which, of course, cannot be separated from how a country increases its cyber capacity building. One of the government's initiatives has been to create cyber cooperation with Australia. It began in 2018 and continues to this day in terms of expanding cyber defense

capacity building. Several frameworks based on the concepts and theories mentioned above, namely: cyber security awareness, cyber security education framework, and cyber security professional training.

2.1.7. Cyber Defense Capacity Building

The current state of Indonesia's national cyber security and defense policy approach may be compared to a complex ecosystem made up of numerous "twisted threads" that are interconnected. The complexities of these conditions can be understood or felt via different events that have happened since Indonesia's inception till the present. This is supported by the contemporary phenomena in which the pendulum of state threats shifts from military to non-military strikes, with information technology serving as the primary key in carrying out cyber operations. (Indrajit et al., 2021)

The events that have occurred in a number of nations in the past demonstrate how this phenomena will continue to be a trend in international relations, particularly those that have been in disagreement for a long time. Every day, cyberwarfare occurs unnoticed and unavoidably. The number and frequency of cyberattacks inside and against Indonesia are steadily growing. If this threat materializes, it will endanger the nation's unity and integrity. As a result, the possibility of such assaults poses a major danger to the Unitary State of the Republic of Indonesia's sovereignty and integrity. (Indrajit et al., 2021)

According to Pros. Eko Indrajit et al, Cyber Defense is an endeavor to deal with cyber threats that undermine national defense implementation. As a result, cyber defense may be described as an endeavor to overcome cyber attacks that create disruption to the implementation of all measures to preserve state sovereignty, territorial integrity of a country, and the safety of the entire nation from threats. (Indrajit et al., 2021)

Cyber threats are one of the non-military threats that countries face in this century of technology advancement. Cyber threats are defined as any intentional or unintentional action by any party, against vital as well as non-

vital objects in the military and non-military domains, which threaten state sovereignty, territorial integrity, and national security. (Indrajit et al., 2021)

We may deduce from these thoughts and beliefs that cyber defense is very closely related to today's modern challenges and threats. This will greatly affect the defense sector of a country. Regarding the protection of national vital information infrastructure, the Ministry of Defense is the leading sector in the defense sector. This obviously increases the Ministry of Defense's ability to strengthen cyber defense capacity building. From the explanation above, we can define that cyber defense capacity building is a cyber capacity building in the defense sector through three measurement indicators in the form of awareness raising, cyber education and cyber training.

2.1.8. Cyber Cooperation

Cyber capacity building also strengthens collective capabilities while facilitating international cooperation and partnerships to respond effectively to cyber-related digital security challenges. Cyber security risks are becoming increasingly transnational, and collaboration remains an essential tool for addressing cyber security challenges. Because of the increasing interconnection and correlated infrastructures, cyber security remains a transnational issue. The global cyber ecosystem's security cannot be guaranteed or managed by a single stakeholder, and it requires national, regional, and international collaboration to expand reach and impact. In this pillar of cooperation, the questionnaire gathered countries with bilateral and multilateral agreements, as well as those involved in interagency and public-private partnerships. Common goals of cyber cooperation include harmonization of minimum security measures, sharing of information and best practices, and codification of behavioral norms. (ITU Cyber security team, 2021)

a. Bilateral agreements on cyber cooperation with other countries

Bilateral agreements (one-to-one agreements) are any officially recognized national or sector-specific partnerships for the government to share cyber security information or assets across borders with another foreign government or regional entity (i.e., the cooperation or exchange of information, expertise, technology and other resources). The indicator also assesses whether threat intelligence is shared. Capacity building includes sharing professional tools, advanced envelopment of experts, and other activities. (ITU Cyber security team, 2021)

b. Government participation in international mechanisms related to cyber security activities

Ratification of international cyber security treaties such as the African Union Convention on Cyber Security and Personal Data Protection, the Budapest Convention on Cybercrime, and others may also be included. (ITU Cyber security team, 2021)

c. Cyber multilateral agreements

Any officially recognized national or sector-specific program for sharing cyber security information or assets across borders by the government with multiple foreign governments or international organizations is referred to as a multilateral agreement (one to multiparty agreement) (i.e. the cooperation or exchange of information, expertise, technology and other resources). (ITU Cyber security team, 2021)

d. Partnerships with the private sector (PPPs)

PPPs (public-private partnerships) are joint ventures between the public and private sectors. This performance indicator counts the number of officially recognized national or sector-specific PPPs between the public and private sectors for sharing cyber security information and assets (people,

processes, tools) (i.e. official partnerships for the cooperation or exchange of information, expertise, technology, and/or resources), whether national or international. (ITU Cyber security team, 2021)

e. Inter-agency partnerships

This performance indicator refers to any official collaborations between the nation's various government agencies (does not refer to international partnerships). This can refer to collaborations between ministries, departments, programs, and other public-sector organizations to share information or assets. (ITU Cyber security team, 2021)

Researchers expect to be able to analyze how the cyber cooperation policies in the defense sector between Indonesia and Australia are associated with several approaches to cooperation that can be carried out by a country in order to increase its cyber defense capacity building through cooperation, including those used in research, using the theories and concepts mentioned above. Specifically, bilateral agreements, government participation in international forums, and inter-agency partnership.

2.2. Previous Research

A number of previous studies have been attached to this section which are relevant to the debate and will help enrich the writing of this research. Although the phenomenon raised in this study is relatively new, especially in terms of the perspective of cyber security as one of the dimensions of threats that can disrupt national security, the following research can be used as a reference in this study. The following are some previous studies related to the thesis research theme:

Table 2.1. Comparison of Past Research

Research Title	Researcher	Methodology	Similarity	Dissimilarity
Complex Interdependence Between Indonesia-Australia Through Cyber security Cooperation Post-Indonesia-Australia Cyberwar in 2013 • Year : 2021 • Type : National Journal	Elva Azzahra Puji Lestari	Qualitative	This study aims to analyze the causes of Indonesia and Australia's choice to continue their cyber security cooperation after the Indonesia-Australia cyberwar in 2013	This study focuses on how the political approach of the two countries to continue bilateral cooperation in the field of cyber security, but does not discuss further its impact on Indonesia's national security.
Analisis Kerjasama Cyber Security Antara Indonesia - Australia Dalam Menghadapi Ancaman Cyber Terrorism • Year : 2019	Nabila Nur Aziza	Qualitative	This study discusses the cooperation between Indonesia and Australia in the field of cyber security	This research only focuses on cyber security cooperation in the field of cyber terrorism

• Type : Thesis				
Kerjasama Indonesia-Australia di Bidang Keamanan dalam Mengatasi Cyber Crime di Indonesia melalui Program Cyber Policy Dialogue • Year : 2019 • Type : Thesis	Hegar Krisnaduta	Qualitative	This study explores the implementation of cooperation between Indonesia and Australia in the field of cyber security	This research only focuses on cooperation on cybercrime
Unraveling the Complexity of Developing a National Cyber Defense Sovereignty Policy: A Case Study of Indonesia • Year : 2021 • Type : International Journal	Richardus Eko Indrajit, Marsetio, Rudy AG Gultom, Pujo Widodo, Resmanto W. Putro, Pantja Djati, Siswo Hadi, Budi Pramono, Luhut Simbolon	Qualitative	The purpose of this study is to describe and at the same time unravel the complexities of managing cyber ecosystems of Cyber Defense in Indonesia.	This study examines the cyber ecosystem in the defense sector in general, but not explicitly capacity building and cooperation.

The Taxonomy of Cyber Threats to National Defense and Security • Year : 2021 • Type : International Journal	Richardus Eko Indrajit, Marsetio, Rudy AG Gultom, Pujo Widodo, Resmanto W. Putro, Pantja Djati, Siswo Hadi, Budi Pramono, Luhut Simbolon	Qualitative	This research focuses on studying various cross-border cyber-attacks that have occurred with the aim of categorizing them based on their common characteristics	This study examines the category of cyber attacks that might disrupt national security, but it does not go into detail about how to build cyber capacity building or patterns of cooperation in the field of cyber security.
Risk Mapping against Cyber Attack Trend in the Perspective of National Defence and Military Sector in Indonesia • Year : 2021 • Type : International Journal	Richardus Eko Indrajit, Marsetio, Rudy AG Gultom, Pujo Widodo, Resmanto W. Putro, Pantja Djati, Siswo Hadi, Budi Pramono,	Qualitative	The purpose of this study is to try to detect which attacks need attention by the military and state defence sectors in Indonesia	This research seeks to identify the types of cyber attacks that have an impact on national defense and the defense sector, but does not specifically

	Luhut Simbolon			address strengthening cyber defense capacity building.
Cyber security As a Component of The National Security of The State • Year : 2020 • Type : International Journal	Olga Vakulyk, Pavlo Petrenko, Iulia Kuzmenko, Maksym Pochtovyi, Ruslan Orlovskyi	Qualitative	This study explores the importance of cyber security issues as a component of Ukraine's national security by analyzing the gaps that exist in ensuring cyber security due to the globalization of the cyberspace.	This study only focuses on Ukraine's cyber security strategy in dealing with global challenges that can disrupt Ukraine's national security
National Cyber Security as The Cornerstone of National Security • Year : 2018	László KOVÁCS	Qualitative	This study seeks to explore the relationship between cyber security and	This study focuses only on the key issues needed to develop a cyber

• Type : International Journal			national security	security strategy that can be used to strengthen national security

Basically, the first three previous researches have the same focus on discussing cyber cooperation between Indonesia and Australia. The journal reference provide practical information regarding perspective of state's national interests in cyber security. However, what makes it different is that the scope of cyber security that discuss in this research specifically related to cyber defense capacity building. The previous research and writings provided above can enrich and provide support to the analysis process thereafter.

2.3. Thinking Framework

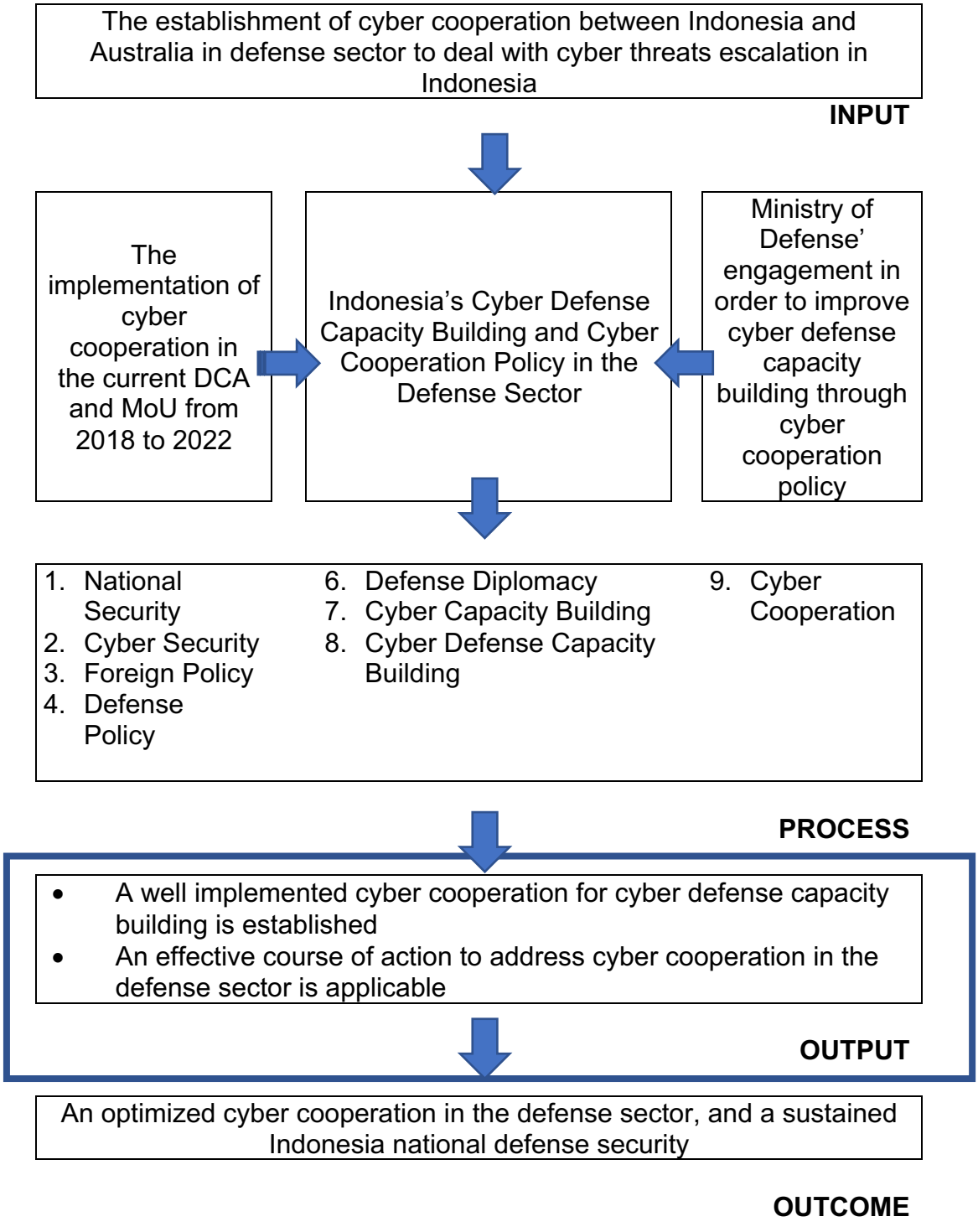

Figure 2.3. Thinking Framework

Source : Processed by Researcher