CHAPTER I
PREFACE

I. Background

In the twenty-first century, information and communication technology started to grow quickly and became a crucial component of the global community. The advancement of information technology, particularly the internet, has become a basic requirement that can influence changes in international community activities. This transformation is being driven by the widespread globalization of technology, which has an impact on the life of the nation-state. Countries are beginning to use digital technology to provide convenience and efficiency in carrying out various activities in international relations.

In the spectrum of statehood, using the internet as media to enhance the relation between parties and make it easier to do diplomacy among the parties, it makes significant corporation rather than conventional style of diplomacy. Public diplomacy is diplomacy through media or internet. Public diplomacy is a crucial part of regional and international communication in international relations. Public diplomacy is widely used by governments everywhere as a potent tool to promote goodwill among the people of neighbouring countries (Mamchii, 2023).

The effects of globalization continue to move endlessly, it does not only provide good effects but also bad effects on human life. The state must begin to be aware of the existence of this new type of threat or crime. The cyber world or better known as cyberspace is a new space in the world that is not limited by space and time. Cyberspace is a worldwide realm inside the technological environment that includes the Internet, telecommunication networks, computer systems, and embedded systems (Fang, 2018). The development of cyberspace has created

various kinds of cyber phenomena. The existence of this cyber phenomenon can bring benefits, but on the other hand, it can also bring harm. The cyber-world is capable of triggering all the things that are integrated into it, such as the social service system, the defense and system of security country, and political system. This situation becomes a vulnerable point and even becomes a threat to the state because it can be misused by parties who take advantage of it. If a country or state lacks the capacity to use technology accurately, appropriately, and correctly, it may be in danger of failing to deal with the cyber era. This supports the need for cyber security and defence in a nation.

Throughout 2022, there were 714,170,967 traffic anomalies or cyberattacks, according to BSSN statistics. Of these, the greatest number of attacks 272,962,734 occurred in January, accounting for more than a third of all attacks during the first half of 2022. Attacks known as "web defacement" or hacking techniques that alter a website's content include modifying its layout, typefaces, advertising, and content in general. This hack has the potential to take more data and other things. This hacking technique mostly targets educational institutions and municipal governments, accounting for about 30% of all attacks. The central government (3.86%), legal institutions (7.23%), and private institutions (16.85%) are additional goals. Specifically, in October 2021, BSSN itself fell prey to a cyberattack that employed the web defacement technique (CNN Indonesia, 2022) .

Indonesia leads the ASEAN region in terms of malware attacks, according to Interpol's ASEAN Cyberthreat 2021 data. First place went to Indonesia with 1.3 million cases. That represents about 50% of the ASEAN countries' overall ransomware danger. According to a recent survey by the National Cyber Security Index (NCSI), Indonesia's cyber security was placed 83th out of 160 countries worldwide and sixth among ASEAN nations (CNN Indonesia, 2022; Timeline et al., n.d.).

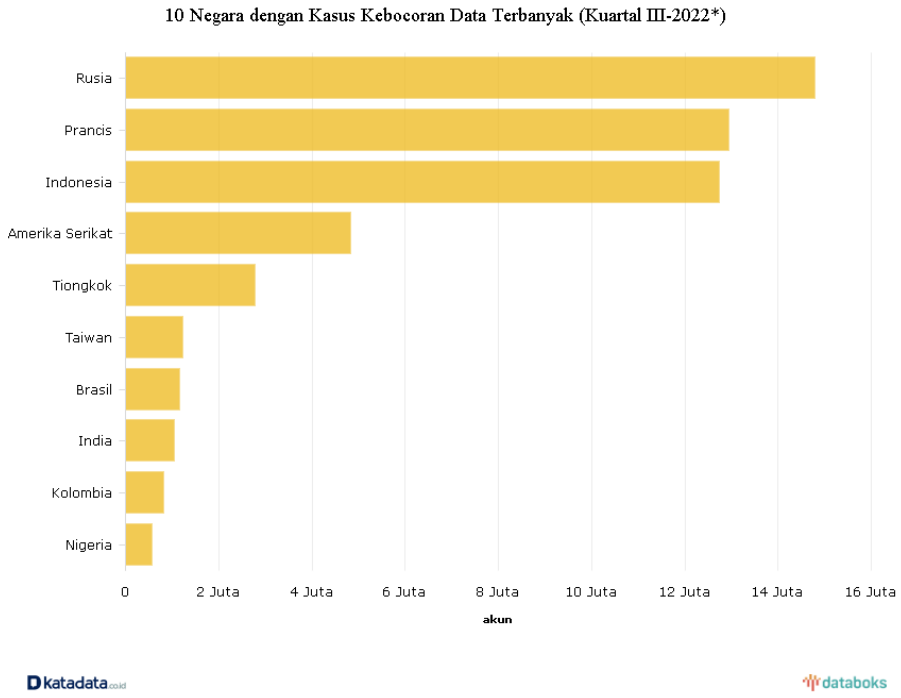

Figure 1.1 The Most Data Leak Countries 2022

Based on information provided by cyber security firm Surfshark, Indonesia is in third place globally for the quantity of data breach cases. According to statistics recorded up until September 13, 2022, 12.74 million accounts nationwide suffered data breaches in the third quarter of 2022 (Cindy Mutia Annur, 2022). The system contained in each platform is the responsibility of the state because licences and internet providers for certain areas are specifically provided by the state. In Indonesia itself, data protection is very crucial because in 2022 Indonesia is the country that being target of the 3rd most cyber-attacks (Cindy Mutia Annur, 2022). Nationals' security has evolved beyond conventional military and geographical limitations. The widespread use of the internet and the expansion of information technology have given rise to a new dimension of warfare, known as cyberwarfare. Cyberwarfare is the act of attacking a nation's systems via the internet with the intention of destroying anything (Cambridge University Press & Assessment, n.d.) . With the traditional boundaries of land, sea, air, and space, cyberspace has emerged as the fifth domain that can be used as a battlefield from a defence perspective. The

increasing prevalence of internet-based platforms, devices, and systems has the potential to become a vulnerability (Kemhan_RI, 2015). As nations continue to rely on digital infrastructure for important purposes like communication, economic activity, and essential infrastructure, they have become increasingly vulnerable to cyber threats. With Indonesia's rapidly expanding digital presence and advanced digital infrastructure, it is essential for the country to have a comprehensive cybersecurity policy in place to counter any foreign attacks. Along with other global cybersecurity cases, Indonesia has also been impacted by hacking into the Border Gateway Protocol, Covidlock malware, Coronavirus ransomware, Remote Code Execution in multiple Windows operating system versions, Arbitrary Code Execution vulnerabilities in all Google Android operating systems, and Solar Winds Orion Platform products (Budi et al., 2021).

The interconnectedness of the global landscape, alongside growing geopolitical tensions, has led to a rise in state-sponsored cyberattacks and cyber espionage. Indonesia, like many other countries, has faced cyber threats from both state and non-state actors. There are several different reasons for these cyberattacks, such as military, political, or economic goals. To protect its economic, political, and social interests, Indonesia must develop a technical security strategy within the framework of international relations. Within scope of state, it’s necessary to have set of policies and realtime active protection as system because a stable regional and international security also depends on the strategy's implementation.

II. Research Problem Formulation

Based on what has explained in background of this research, the research aims to address the following key question:

“What is Indonesia’s Strategy to Response International Cyberthreats?”.

III. Theoretical Framework

As a basis for this research, the author first proposes a theoretical framework based on the issues presented. The theoretical framework serves as the foundation

for thinking in order to investigate and explain. The theory that supports this research can be used to guide research and identify truth. The writer uses one basic theory to stand as the fundamental concept for further study and broad comprehension of the subject. The author use cyber attack theory as a theory to analyse the problem formulation while analysing Indonesia's cyber strategy in response to threats from other nations.

Cyber Attack Theory

Malware refers to any computer code that can be used to steal data, circumvent access controls, and harm or damage the system. In cyber-attacks, there are several types of malware attacks, including spyware, which tracks activity, collects keystrokes, and captures data. Adware was designed to display advertisements but was also discovered to carry spyware. Bots are designed to automatically perform specific actions online. Ransomware encrypts data on a computer using a key unknown to the user. These types of malware are used to alter characteristics in cyberspace. According to the law, the characteristics of cyberspace virtuality allow illegal content such as electronic information and/or documents with content that violates several things, namely decency, gambling, insult or defamation, extortion and/or threatening, spread false and misleading news resulting in consumer losses in electronic transactions, as well as acts of spreading hatred or hostility based on ethnicity, religion, race, and class, and sending threats of violence (2021).

IV. Hypothesis

In response to cyberattacks from international, Indonesia has a weak defensive cyber mechanism.

Literature Review

The goal of previous research is to gather reference and comparison data. Moreover, to anticipate the assumption that this research is identical to others. For

this reason, the researcher has included the following findings from earlier studies in this literature review.

Firstly, the article "Cyber Diplomacy and Protection Measures Against Threats of Information Communication Technology in Indonesia" by Ridha Iswardhana (2021) delves into this critical issue. It exposes the stark reality of Indonesia's cyberspace - a battleground rife with attacks and threats. While domestic measures like the Electronic Information and Transaction Law (ITE Law) offer a first line of defense, their effectiveness is often hampered by the ever-shifting nature of external threats. Recognizing this limitation, the Indonesian government has shifted its focus towards a more holistic approach, embracing cyber diplomacy as a key weapon in its digital ordnance.

This diplomatic action takes on various forms. It involves forging strong partnerships with foreign nations, collaborating on cybercrime prevention and information sharing. It entails engaging in international dialogues, pushing for global norms and regulations that govern the conduct of nations in cyberspace. It even extends to promoting cultural transformation within Indonesia, fostering a digital safety awareness amongst its citizens.

But this cyber diplomacy is not merely a reactive shield. It can also be a proactive spear. By actively participating in international cyber exercises and training programs, Indonesia strengthens its own cyber defenses and contributes to building a more robust global security architecture. Moreover, by investing in domestic technological advancements, it creates a more resilient cyberspace, less susceptible to external manipulation and sabotage.

The results of this multi-pronged approach are encouraging. As Iswardhana highlights, the Indonesian government is no longer relying solely on legal solutions; it is embracing a comprehensive strategy that leverages the power of diplomacy, cultural awareness, and technological innovation. This holistic approach offers a glimmer of hope in the face of a constantly evolving digital threat landscape.

However, the battle for a secure cyberspace is far from over. Indonesia's journey towards digital sovereignty demands constant vigilance, adaptability, and a continued commitment to international collaboration. By proactively engaging in cyber diplomacy, investing in its digital infrastructure, and fostering a culture of digital safety, Indonesia can rise to the challenge and build a cyberspace that is both prosperous and secure, for itself and the world at large (Ridha Iswardhana, 2021).

Secondly, The impact of establishing the National Cyber and Crypto Agency (BSSN) on Indonesia's national cybersecurity posture was examined in a 2018 study by Mulyadi and Dwi Rahayu titled "Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN)". Using a comparative methodology, the study looked at Indonesia's cybersecurity capacities both before and after the establishment of BSSN. Three main BSSN functionalities were the focus of this analysis: Technical capabilities is evaluating the infrastructure and technical know-how of BSSN to address cybersecurity risks. Administrative capabilities are to manage national cybersecurity efforts efficiently, this section assessed BSSN's administrative procedures and structure. Regulatory capabilities: This analysis looked at how BSSN developed and carried out cybersecurity policies and regulations.

Beyond its direct functionalities, the study also highlighted BSSN's strategic role. The agency acts as a central coordinator, facilitating collaboration between various stakeholders involved in local, national, and international cybersecurity. This collaborative approach aims to leverage different expertise and resources to strengthen Indonesia's overall cybersecurity posture.

The research concluded that BSSN's establishment significantly bolstered Indonesia's national cybersecurity capabilities. By addressing technical, administrative, and regulatory aspects alongside fostering collaboration, BSSN is well-positioned to take a leading role in driving further advancements in Indonesian cybersecurity.

Thirdly, Counterattacking Cyber Threats: A Comparative Study of Cybersecurity in ASEAN Countries is a recent study by Safitra, Lubis, and Fakhrurroja 2023 that looked at cybersecurity tactics among ASEAN member countries. The study used a comparative methodology to examine how various nations in the region handle cyberthreats.

The study presented a model highlighting adaptation and learning as critical components of cyber defence. According to this model, by using historical security incidents as teaching moments, contemporary cyber-physical systems can strengthen their defences against attacks. These systems are able to change over time in order to become more resilient to potential threats.

The research findings emphasized the importance of a comprehensive approach to cybersecurity. This includes **prevention** measures to minimize vulnerabilities, **management** strategies to handle incoming attacks, and **response** mechanisms to effectively detect and recover from breaches. The study also highlighted the crucial role of **digital skills** development, **threat analysis**, and **rapid response and recovery** capabilities in building robust cybersecurity postures.

In conclusion, Safitra, Lubis, and Fakhrurroja's study sheds light on the evolving landscape of cybersecurity in ASEAN countries. By emphasizing the significance of learning, adaptation, and a multifaceted approach, the research offers valuable insights for countries within the region, and potentially beyond, as they strive to strengthen their defenses against cyber threats.

Fourth, The state of cybersecurity in Indonesia was examined in a 2021 study by Halimah titled "Cybersecurity Protection in Indonesia". The legal framework and cooperative efforts in place to address cyber threats were the main topics of the research.

According to Halimah, the main legislative framework governing cybersecurity in Indonesia is the **Electronic Information and Transaction Law (ITE Law), ** which was passed in 2008 and updated in 2016. This law lists a number of cybercrimes, such

as unauthorised access to computer systems, data breaches, and the dissemination of illegal material.

The study highlighted the increasing vulnerability of both governmental and private sector entities to cyberattacks. Halimah emphasized the importance of collaboration between these sectors. Private sector expertise can keep the government informed about the latest cybersecurity technologies, enabling a robust knowledge exchange and fostering a more comprehensive approach to combating cyber threats.

In conclusion, Halimah's research underscores the need for a multifaceted approach to cybersecurity in Indonesia. Combining a robust legal framework with effective collaboration between government and private sectors is crucial in protecting the nation from evolving cyber threats.

Fifth, a recent study by Abdurrohim and Rosy (2023)) titled "The Paradox of Indonesia Cyberspace Policy and Cooperation: Neoclassical Realism Perspective" delves into the seemingly contradictory nature of Indonesia's approach to cyberspace. The research employs **neoclassical realism**, a theory emphasizing national security concerns driven by internal political and economic constraints, to analyze Indonesia's digital policy across domestic and international spheres.

The study centers on understanding the **apparent paradox** between Indonesia's domestic cyberspace regulations, governed by the Information and Electronic Transactions (ITE) Law, and its commitment to international cooperation through initiatives like the ASEAN Digital Masterplan. This contradiction arises from the government's dual desire – **controlling cyberspace domestically** for perceived security reasons and **engaging in international collaboration** for broader benefits.

The research highlights several key factors contributing to this apparent paradox:

Domestic Factors:

- **Legacy of Authoritarianism:** Indonesia's historical experience with authoritarian regimes influences the government's perception of cyberspace threats, prioritizing **regime stability** over an open approach. This

perspective informs the creation and implementation of the ITE Law, which some perceive as restrictive.

International Factors:

- **Socialization and Institutionalization:** The study argues that Indonesia's engagement with international organizations and adoption of international norms create a "strategic culture" that limits the government's ability to fully translate domestic policies and ideas into the international arena. This disconnect contributes to the perceived inconsistency between domestic and international approaches.

Abdurrohim and Rosy's study reveals a **complex and multifaceted situation** regarding Indonesia's cyberspace policy. The country navigates the challenge of balancing its domestic security concerns with the benefits of international cooperation in the digital realm. Domestic political considerations and the evolving international landscape play significant roles in shaping this balancing act. Understanding these factors is vital for comprehending the apparent paradox observed in Indonesia's cyberspace strategy.

Research Method

1. Research Approach

The research method that will be used in this study is a descriptive qualitative approach. This approach was chosen to understand and describe in detail Indonesia's cyber strategy and its response to international threats within the framework of international relations.

2. Research Design

The research design involves document and literature analysis with a focus on Indonesia's cyber policy and strategy. The research is descriptive in nature to

describe the cyber strategy that has been adopted by Indonesia and its impact in dealing with international threats.

3. Instruments and Data

The instruments used in this research are related documents and literature. Data will be collected from various sources, including government policies, official reports, academic articles, and other literature sources relevant to Indonesia's cyber strategy. Documents serve as the primary data source for this qualitative study. Documents can be written pieces of art, photographs, or large-scale creations created by someone. written records, such as diaries, life histories, narratives, biographies, rules, and policies. Documents that take the shape of pictures, such as images, live sketches, photos, and more. documents presented as works, such as artwork, which includes photographs, sculptures, videos, and other media (Sugiono, 2016, p. 240). To process the data, the data must be gone through few steps. Firstly, process of gathering data by focussing and selecting based on summary of the data. The presentation of data in the form of research-related explanatory sentences constitutes the second stage. Verification and conclusion-drawing comprise the third stage. At this point, conclusions are made utilising the concepts or theories applied to explain the findings. After that, verification is done to make sure the conclusions are reliable (Sugiono 2016, 246–252).

4. Data Analysis

This study's data analysis will be done using a content approach. To find developments, patterns, and distinctions in Indonesia's cyber strategy and its reaction to global challenges, the gathered data will be qualitatively examined.

According to Holsti (2022), the content analysis approach is a way to make conclusions by systematically, without bias, and broadly recognising different particular aspects of a message. Objective refers to following guidelines or methods that enable other researchers to draw equal results. Systematic refers to the process

of classifying categories or content based on consistently implemented rules. To prevent bias, this also means making sure the data are appropriately chosen. This also includes ensuring that the data is properly selected to avoid bias.

The use of content analysis methods must meet several conditions namely, the first is that the available data consists mostly of documented materials, such as books, newspapers, recordings, manuscripts. The second is that there is a complementary description or certain theoretical framework that explains about and as a method of approach to the data. The third is that the researcher has the technical ability to process the material or data he collects because most Generalist documentation means that the invention must have a theoretical reference (Sitasari, 2022).

5. Research Ethics

This research will pay attention to ethical aspects by prioritizing accuracy and honesty in data interpretation. Data sources used will be accurately cited to respect copyright and research integrity.

6. The Benefits of Research

This research has various benefits, both practical and theoretical, namely:

1. Practical Benefits

Contribute suggestions to raise awareness of cyber threats among stakeholders, Indonesia's cybersecurity team, and the general public.

2. Theoretical Benefits

In addition to the practical benefits mentioned above, this research includes theoretical benefits, such as providing a framework for other researchers to conduct similar studies in order to increase knowledge and deeper analysis of future research.

V. Research Purposes

1. To understand more about Indonesia's cyber strategy as an international actor.
2. To know deeply the Indonesian cyber strategy for preventing and resolving cases of attacks in the cyber world.
3. To fulfill the requirement for achieving the bachelor degree of International Relations in Universitas Muhammadiyah Yogyakarta.

VI. Scope Of the Study

The author chose to restrict the research to Indonesia's cyber strategy in response to threats from other nations from an international relations perspective to perform efficient research and prevent distorting information from the study. Nevertheless, the writer will furthermore gather information that is closely linked to the subject matter.

In this thesis, Indonesia's cybersecurity strategies and policies are looked at, with a particular focus on how Indonesia address threats coming from other countries. It will take a comprehensive approach, covering Indonesia's cyber strategy's technological, constitutional, and political facets. The investigation will acknowledge the interconnectedness of cyberattacks, but its primary focus will be sponsored by the government cyber threats.

VII. Systematically Writing

CHAPTER I is an introductory chapter that contains the background of the problem, problem formulation, theoretical framework, research methods, hypotheses, research objectives, research scope, and research systematics.

CHAPTER II will explain the condition of Indonesia's cyberspace and analyze the strategies carried out by Indonesia in dealing with threats from other countries using the theory of realism.