Journal of Human Security | 2024 | Volume 20 | Issue 1 | Pages 109-117
DOI: https://doi.org/10.12924/johs2024.20116
ISSN: 1835–3800

Journal of Human Security

Research Article

State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia

Agus Bhakti[1]* Arfin Sudirman[2], R. Widya Setiabudi Sumadinata[3], Arry Bainus[4]

[1]Department of International Relations, Universitas Padjadjaran, Indonesia. Email: agus22005@mail.unpad.ac.id
[2]Department of International Relations, Universitas Padjadjaran, Indonesia. Email: arfin.sudirman@unpad.ac.id
[3]Department of International Relations, Universitas Padjadjaran, Indonesia. Email: w.setiabudi@unpad.ac.id
[4]Department of International Relations, Universitas Padjadjaran, Indonesia. Email: arrybainus@unpad.ac.id

***Correspondence:** agus22005@mail.unpad.ac.id

Submitted: 19 January 2024 | Revised: 17 April 2024 | Accepted: 01 May 2024 | Published: 02 July 2024

Abstract: This study investigates Indonesia's cyber defence capabilities and strategies in addressing the growing complexity of cyber warfare threats. It also proposes a policy framework for the development of a future cyber division within the Indonesian Armed Forces (TNI). The research adopts a qualitative explanatory methodology with a case study approach, integrating primary data from interviews and observations with secondary data derived from policy documents, scholarly publications, and official reports. The analysis is conducted through triangulation of these diverse sources, contextualising the findings within the Network Centric Operations Centre (NCOC) concept. This concept highlights the importance of synergy between legal frameworks, institutions, infrastructure, human resources, and international collaboration. The study's findings reveal that Indonesia's current cyber defence policies are not fully integrated. Several cybersecurity regulations, including the Electronic Information and Transactions Law, policies from the National Cyber and Crypto Agency (BSSN), and directives from the Minister of Defence, fail to distinguish between cybersecurity (as law enforcement) and cyber defence (as a means of sovereignty protection). National infrastructure, such as the National Data Centre and satellites, remains vulnerable to attacks. Additionally, there is a significant shortage of personnel with specialised cyber expertise, and the country's incident response strategies are primarily reactive. On the international front, while Indonesia has participated in ASEAN forums and various global initiatives, there remains limited progress in technology transfer and capacity building. The originality of this research lies in its thorough mapping of the challenges and opportunities in establishing a TNI cyber division, alongside a proposed design for a national cyber command structure. The study concludes that Indonesia's cyber defence requires regulatory revisions to clarify the military's authority, the development of layered infrastructure (such as SOC, military satellites, and distributed servers), the preparation of highly qualified human resources, and the enhancement of strategic international cooperation. With these measures, Indonesia could strengthen its deterrence capabilities and be better prepared for future cyber warfare.

Keywords: Cyber Defence Policy, Digital Infrastructure, State Sovereignty, Cyber Division, International Cooperation

1. Introduction

The rapid advancement of information and communication technology has significantly reshaped various facets of life, from social interactions to governmental systems [1]. With the onset of the Fourth Industrial Revolution and the emergence of Society 5.0, technologies such as the internet, artificial intelligence, and robotics have become foundational to human activities. While these developments offer substantial benefits in terms of efficiency and convenience, they have also introduced the darker side of increasing cyber threats. Critical infrastructure—spanning finance, transportation, energy, and telecommunications—has become interconnected within a digital ecosystem, rendering it vulnerable to exploitation by hackers. This vulnerability poses the risk of considerable financial losses or even threats to national security [2].

Recognising these risks, several nations have taken strategic measures to enhance their digital defence capabilities. The United States, for instance, was the first to designate cyberspace as the fifth domain of warfare in 2004. This shift in perspective was further solidified in 2009 with the establishment of US Cybercom under the Department of Defence, which coordinates cyber units across all military branches. The integration of cyberspace into defence doctrine has been reinforced over time, particularly during the administration of President Donald Trump, who placed a strong emphasis on offensive cyber capabilities. This approach positioned cyberattacks on equal footing with conventional military operations, confirming that cyberspace is not merely an auxiliary domain but a central component of national defence strategy.

In Southeast Asia, Singapore offers an alternative model. In 2015, the country founded the Cyber Security Agency (CSA), a centralised body under the Ministry of Communications and Information responsible for addressing digital threats in the civilian sector. In the defence domain, Singapore's Ministry of Defence established the Digital and Intelligence Service (DIS) in 2022 as the fourth branch of the Singapore Armed Forces (SAF). The DIS integrates aspects of Command, Control, Communications, Computers, and Intelligence (C4I) to provide a cohesive response to cyber threats. This dual approach—encompassing both civilian and military sectors—has proven successful, with Singapore emerging as one of the world's leaders in cybersecurity and a key regional player in Southeast Asia.

From a military history perspective, the evolution of warfare has progressed through several generations: first-generation warfare centred on massed troops, second and third generations introduced machine guns and artillery, while the fourth generation was characterised by asymmetry, nuclear threats, and guerrilla tactics. Fifth-generation warfare now integrates cyber operations and physical attacks, allowing critical infrastructure to be disrupted without large troop deployments. A notable example is the 2007 DDoS attack in Estonia, allegedly by Russian hackers, which paralysed financial systems and public services. Similarly, Georgia faced cyberattacks ahead of the 2008 South Ossetia War, with government websites and financial services disrupted. The 2007 Stuxnet attack on Iran's uranium enrichment facilities further demonstrated how malware could cause significant physical damage without direct military engagement.

Indonesia faces comparable challenges. The 2013 interception of the President's mobile phone by Australian intelligence raised concerns about the security of national communication systems. Large-scale hacking incidents have followed, including the 2020 Tokopedia breach and the 2022 Conti ransomware attacks on Bank Indonesia and the Directorate General of Taxes. Ironically, the BSSN, established to protect national cybersecurity, was itself hacked in 2021. The peak of the threat occurred in May 2023, when Bank Syariah Indonesia was crippled by the LockBit 3.0 ransomware attack, which threatened the exposure of significant customer data. These incidents underscore the urgent need for enhanced national cybersecurity governance.

The legal framework, such as Ministry of Defence Regulation Number 82 of 2014 on Cyber Defence, already exists, highlighting the importance of securing critical infrastructure. Initial efforts include the establishment of the BSSN and the Cyber Defence Centre within the Ministry of Defence. However, inter-agency coordination remains problematic, leading to overlapping responsibilities and inefficiencies. Additionally, the shortage of skilled cybersecurity professionals presents a significant challenge. There is a pressing need for recruitment, training, and the development of expertise to address increasingly sophisticated digital threats. Drawing inspiration from the United States and Singapore, Indonesia could consider establishing a Cyber Command within a centralized command structure. This would enable coordinated defensive and offensive cyber operations, enhancing integration, maximizing capabilities, and facilitating international collaboration. By consolidating doctrines and incorporating cyber units within the military framework, this approach aligns with the Revolution in Military Affairs (RMA), which highlights the impact of technological evolution on warfare, requiring strategic and structural adaptations.

Moreover, close collaboration between the government and the private sector is vital, as entities such as banking, telecommunications, e-commerce, and internet service providers hold data that are primary targets for cyberattacks. Establishing minimum security standards, mechanisms for threat information sharing, and conducting joint incident-handling exercises should be prioritised. Public participation is equally important, as individual negligence—such as weak passwords or neglecting software updates—often exposes vulnerabilities. National digital literacy campaigns and efforts to foster a cybersecurity culture should become key priorities, ensuring that all citizens actively contribute to safeguarding the digital ecosystem.

When cyberattacks occur, the effectiveness of mitigation and recovery measures largely determines the extent of the resulting damage. Preparedness, including data backups, specialised emergency response teams (CERT/CSIRT), and transparent crisis communication, plays a critical role in reducing public panic. Leading nations in this domain routinely conduct large-scale attack simulations to test response mechanisms and refine their procedures [3]. Indonesia should adopt similar practices by conducting regular drills, identifying vulnerabilities, and continuously improving its incident response systems. This study aims to assess Indonesia's cyber defence capabilities following a government institution hacking incident and to develop policy strategies for addressing future cyber warfare threats. By evaluating the country's preparedness and responsiveness in safeguarding its digital infrastructure, the research aims to provide policy recommendations that can strengthen cybersecurity frameworks. The findings are expected to offer valuable insights to the government, supporting efforts to enhance cybersecurity systems and prevent the recurrence of similar incidents. This study makes a significant contribution to the broader objective of safeguarding national sovereignty in the cyber domain.

2. Literature Review

Numerous studies have explored the field of cybersecurity, highlighting various critical aspects of national and organisational capabilities. One essential factor in strengthening cybersecurity is a country's ability to develop human resources [4]. Additionally, the organisation of effective cybersecurity governance is crucial [5]. The state of cybersecurity capabilities and policies varies significantly across countries and regional organisations [6; 7; 8]. Specific studies have also examined maritime cybersecurity and the role of international organisations [9], as well as the impact of politics, ethics, and norms on cybersecurity practices [10]. Furthermore, cybersecurity is increasingly recognised as a local or sub-national issue [11], and international cooperation remains a fundamental element in strengthening cybersecurity [12]. Cyber diplomacy is also an emerging concept crucial for achieving resilient cybersecurity [13]. The issue of Indonesia's cybersecurity capacity in the face of cyber terrorism has also been explored in recent discussions.

The concept of hybrid warfare is a developing research area, with a particular focus on asymmetric warfare employing irregular forces [14]. Initial research into hybrid warfare emerged from the analysis of Russia's actions in Ukraine, particularly its annexation of Crimea. Hybrid warfare is defined as a combination of conventional, irregular, and asymmetric warfare, integrating both kinetic and non-kinetic methods and involving multiple state and non-state actors. This form of warfare is characterised by ambiguity, as both the attackers and defenders often remain unclear about the nature of the assault and the identities of the involved parties.

Several studies have also examined the importance of cyber defence. Cyber defence has become a priority for many nations, and it is understood to require both passive and active strategies. Advanced countries often view cyber defence not just as a protective measure but also as an offensive capability [15]. Research has explored the evolution of Indonesia's cybersecurity in the context of technological and informational advancements. However, existing studies have primarily provided descriptions or explanations of Indonesia's current cybersecurity status and have not fully integrated global lessons from the broader field of cybersecurity and defence.

Previous research on cyber defence has not specifically focused on Indonesia's capabilities, particularly following the hacking incidents involving BSSN and BSI. Additionally, few studies have highlighted the importance of drawing on cyber defence strategies from successful models in other countries, such as Singapore. This study aims to fill this gap by analysing the cyber defence strategies of nations like the United States and Singapore, offering valuable lessons for Indonesia in strengthening its own cyber defence systems. The Indonesian Defence White Paper, issued by the Ministry of Defence in 2015, highlighted that "several countries in the region have utilized technology to modernize weapon systems such as cyber defence systems." This underscores the growing significance of cyber warfare as a strategic tool capable of inflicting substantial national damage. As a target of numerous cyberattacks, Indonesia has recognised the urgent need to develop a robust cyber defence strategy to address the evolving nature of warfare, now heavily reliant on cyberspace. Singapore, a neighbouring country in the region, offers a valuable example. The country has integrated cyber defence into its national defence strategy, alongside traditional domains such as maritime, air, and land, demonstrating its commitment to adapting to the changing landscape of warfare. Indonesia can draw on Singapore's approach as a model for developing a cyber defence strategy that aligns with contemporary military needs.

The Ministry of Defence Regulation Number 82 of 2014, concerning Cyber Defence Guidelines, emphasizes the critical importance of cyber defence to anticipate emerging threats and assess current defence capabilities. This regulation stresses the need for preparedness, responsiveness, and the capacity to recover from cyberattacks [16]. The United States and Singapore have effectively integrated cyber technology into their defence strategies, adapting to the evolving landscape of cyber threats. By examining the developments in these countries, Indonesia can enhance its own cyber defence capabilities, ensuring a robust and respected future in cyber security. This research aims to analyse Indonesia's cyber defence, particularly in the aftermath of cyberattacks on the BSSN, and to propose future strategies by drawing on the cyber defence models of nations with established cyber capabilities, such as the United States and Singapore.

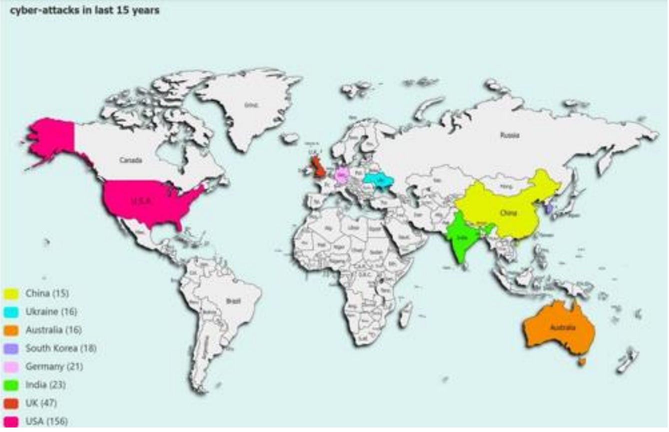

Figure 1: Cyber Attacks in the Last 15 Years

3. Methods

This research adopts a qualitative-explanatory approach with a case study methodology to examine cyber defence within its social, political, and institutional contexts. The qualitative design facilitates an exploration of the meanings, processes, and social issues surrounding Indonesia's cyber defence capabilities, particularly in the aftermath of hacking incidents targeting government institutions. According to Creswell, this approach prioritises narratives over quantitative data, allowing for a nuanced explanation of the complexities and contexts involving various actors and institutions. The case study methodology was selected due to the unique nature of this phenomenon, which unfolds within a specific time and space, incorporating multiple policy networks, actors, and cyber defence systems. The researcher gathered both primary and secondary data to construct a comprehensive understanding. Primary data included interviews and observations with stakeholders from government agencies, the military, practitioners, academics, and cybersecurity experts. Secondary data was sourced from scientific journals, reputable news outlets, institutional reports, and relevant books. These data were then categorised into thematic datasets, encompassing legal frameworks, institutional structures, national and international cooperation, infrastructure, human resources, and operational capabilities. Once collected, the data were condensed and triangulated from diverse sources to ensure validity. Triangulation enhances the accuracy of information by cross-referencing consistent responses from multiple sources, thus ensuring the reliability of the findings. If new indicators arise, the researcher will adjust the conceptual framework to further contribute to the body of knowledge in cyber defence (Figure 2).

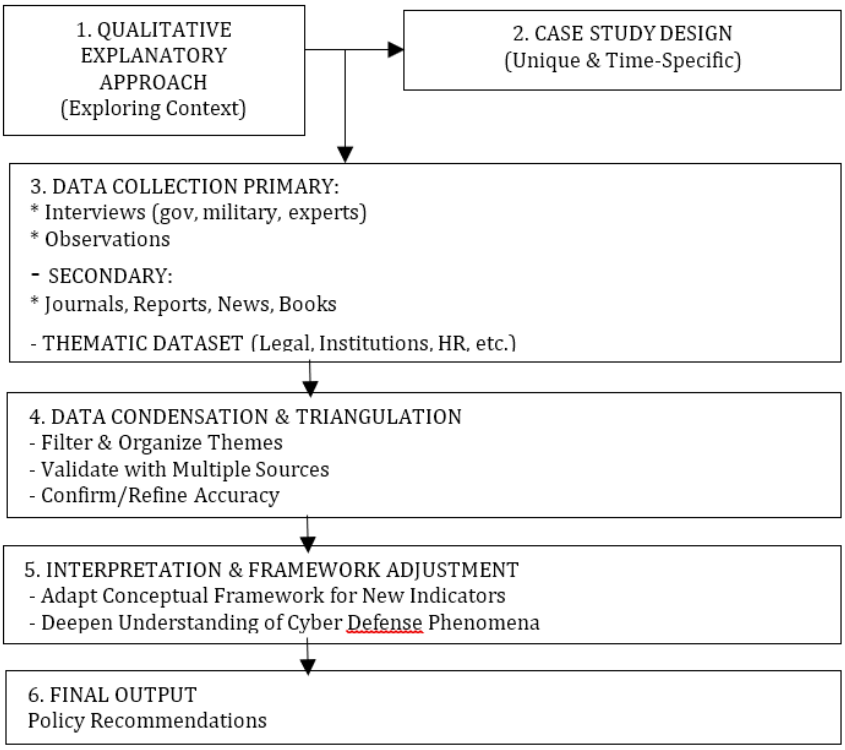
1. QUALITATIVE EXPLANATORY APPROACH
(Exploring Context)
2. CASE STUDY DESIGN
(Unique & Time-Specific)
3. DATA COLLECTION PRIMARY:
* Interviews (gov, military, experts)
* Observations
- SECONDARY:
* Journals, Reports, News, Books
- THEMATIC DATASET (Legal, Institutions, HR, etc.)
4. DATA CONDENSATION & TRIANGULATION
- Filter & Organize Themes
- Validate with Multiple Sources
- Confirm/Refine Accuracy
5. INTERPRETATION & FRAMEWORK ADJUSTMENT
- Adapt Conceptual Framework for New Indicators
- Deepen Understanding of Cyber Defense Phenomena
6. FINAL OUTPUT
Policy Recommendations

Figure 2: Research Flow

4. Result and Analysis

4.1. Global Cyber Threat Trends

Cyber threat trends have escalated annually, driven by the increasing global connectivity facilitated by IT infrastructure. In response, countries are strengthening their cyber forces and weapons to anticipate worst-case scenarios, such as hacking critical infrastructure like power plants. According to Forbes, 2,365 cyberattacks were reported in 2023, affecting 343 million victims and resulting in losses of USD 4.4 million. The USA suffered the most severe attacks, followed by the UK, India, and Germany, with significant impacts also observed in South Korea, Australia, Ukraine, and China. The growing Internet of Things (IoT) increases vulnerabilities in key sectors, including defence, electricity, transportation, and banking. Cyber espionage is becoming more advanced, with examples like Russia's "Snake" malware, the US-Israel Stuxnet worm, and China's Titan Rain. NATO has recognised cyberspace as a critical domain in modern international conflict. An example of the potential risks is illustrated in Figure 3, showing how a cyberattack on a power plant could pose significant threats to national security.

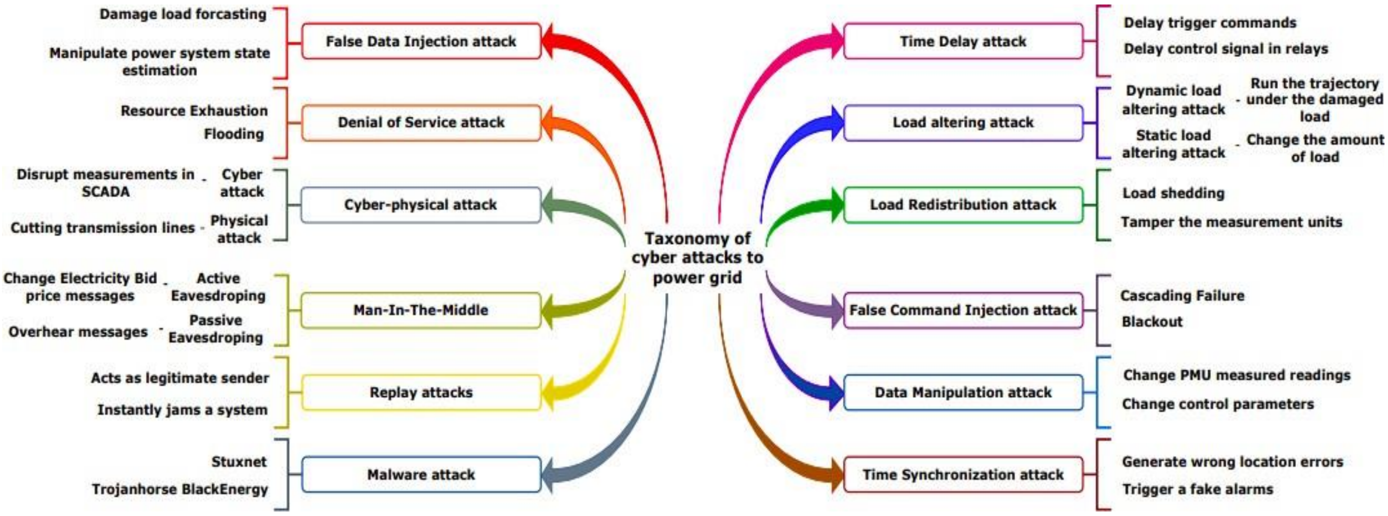
Taxonomy of cyber attacks to power grid
False Data Injection attack
Damage load forcasting
Manipulate power system state estimation
Denial of Service attack
Resource Exhaustion
Flooding
Cyber-physical attack
Cyber attack
Disrupt measurements in SCADA
Physical attack
Cutting transmission lines
Man-In-The-Middle
Active Eavesdroping
Change Electricity Bid price messages
Passive Eavesdroping
Overhear messages
Replay attacks
Acts as legitimate sender
Instantly jams a system
Malware attack
Stuxnet
Trojanhorse BlackEnergy
Time Delay attack
Delay trigger commands
Delay control signal in relays
Load altering attack
Dynamic load altering attack
Run the trajectory under the damaged load
Static load altering attack
Change the amount of load
Load Redistribution attack
Load shedding
Tamper the measurement units
False Command Injection attack
Cascading Failure
Blackout
Data Manipulation attack
Change PMU measured readings
Change control parameters
Time Synchronization attack
Generate wrong location errors
Trigger a fake alarms

Figure 3: Cyber Attacks on Power Plants
Source:Tatipatri and Arun [17]

Cyber threat trends have been steadily increasing each year due to the expanding connectivity of the global society, driven by advancements in IT infrastructure. In response to these growing threats, countries are actively preparing cyber forces and weapons to counter worst-case scenarios, such as the hacking of critical infrastructure like power plants. Data from Forbes reveals that, in 2023, there were 2,365 cyberattacks, affecting 343 million individuals and resulting in losses amounting to USD 4.4 million. The United States experienced the most severe attacks, followed by the United Kingdom, India, and Germany, with countries such as South Korea, Australia, Ukraine, and China also suffering significant impacts. The Internet of Things (IoT) has further heightened vulnerabilities, particularly in sectors like defence, electricity, transportation, and banking. Cyber espionage has also evolved, with sophisticated attacks such as Russia's "Snake" malware, the US-Israel Stuxnet worm, and China's Titan Rain. NATO recognises cyberspace as a critical threat in modern international conflicts. An example of the grave risks posed by cyberattacks is illustrated by a potential attack on a power plant, which could severely compromise national security (Figure 3).

As the nation most frequently targeted by cyberattacks, the United States has expressed particular concern about threats from China and Russia. The US has detected malicious activities originating from China, where state-sponsored cyber actors are embedding malicious code into devices or networks targeting critical infrastructure in the United States. The NSA, in collaboration with international partners, is also engaged in efforts to track and neutralise the Russian "Snake" malware, which has been identified in over 50 countries globally. This malware highlights the evolving nature of espionage, which, traditionally carried out through human infiltration, now extends to cyber networks and individual devices [18]. In March 2024, both the US and the UK accused China of engaging in widespread espionage, which affected millions of individuals, including companies and defence contractors. The United States specifically accused China of targeting government employees, US senators, UK parliament members, and individuals critical of the Beijing regime. The providers of 5G networks, phones, gadgets, and wireless technologies have also been implicated in activities that jeopardise national security. These cyberattacks appear aimed at suppressing dissent against the Chinese government and undermining democratic processes, such as elections.

The 21st century has seen numerous countries worldwide suffer the consequences of cyberattacks, which disrupt defence security, the economy, and ideological structures, often leading to social and political instability [18]. The first significant instance of state-sponsored cyberattacks occurred in 2003, when hackers from Guangdong, China, targeted computer systems in the United States. This attack, known as Titan Rain, focused on extracting sensitive information from NASA and various defence contractors, including Lockheed Martin and Redstone Arsenal. Foreign Policy magazine estimated that China's hacker army comprises between 50,000 and 100,000 individuals. In 2006, during the July war, Hezbollah hacked IP addresses, disabling several Israeli servers and websites. Both Hezbollah and Israel launched "cyber psychological operations" aimed at influencing public and military perceptions [19]. This conflict highlighted the growing intersection of cyber warfare and information operations globally [20].

In 2007, Russian hackers targeted Estonian government systems in retaliation for the relocation of the Tallin soldiers' monument. The cyberattacks impacted parliamentary systems, banking, and media. Estonia sought assistance from Germany, Finland, and Slovenia to combat these attacks. Also in 2007, US and Israeli cyber forces created the Stuxnet worm to sabotage Iran's Natanz nuclear facility. The worm caused errors in uranium enrichment by manipulating centrifuge valves, representing a response to failed diplomatic efforts [18; 20]. In 2008, Russia launched cyberattacks on Georgia, targeting its financial systems and infrastructure ahead of the South Ossetia War. These cyberattacks played a role in hybrid warfare, where cyber operations supported conventional military action [21].

In 2009, the Chinese government conducted extensive surveillance on Tibet's government systems, gathering intelligence for future negotiations [22]. Global cyber threats increasingly target critical infrastructure. NATO acknowledged cyber threats in the 2010 Lisbon Declaration, recognizing cyberspace as a modern conflict domain and incorporating it into military doctrines. NATO is committed to defending its members' critical infrastructure, particularly defence systems, from cyberattacks [23]. The assassination of influential military figures has evolved from conventional methods to technologically advanced approaches, such as drones. A prominent example is the January 3, 2020, assassination of Iranian General Qasem Soleimani, demonstrating the precision of drone warfare [24]. Such attacks, leveraging information-based technologies, raise concerns about the future of military and political stability [25].

Southeast Asia is one of the regions witnessing the fastest growth in the internet market, with the IT-based market value of Southeast Asian countries expected to reach USD 1 trillion by 2030. However, this significant economic potential is not supported by adequate cybersecurity preparedness. In 2023, cybercrime in the region increased by 82%, with Singapore alone seeing a 174% rise in cybercrime attempts through phishing between 2022 and 2023. Of the 86 global cyberattacks documented, Southeast Asia accounted for 68 incidents involving Advanced Persistent Threats (APTs). These cyber threats primarily target governments and businesses, often involving ransom demands for hostage data [26]. According to Interpol data, the primary categories of cyber threats in Southeast Asia include business email compromises, phishing, ransomware, e-commerce data interception, crimeware-as-a-service, cyber scams, and crypto-jacking. Cyberattacks often target critical infrastructure, with data breaches being among the most frequent types of cyberattacks in the region (Figure 4).

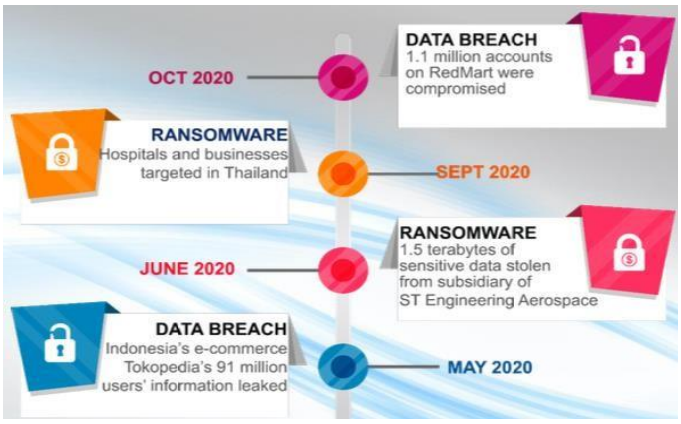
OCT 2020
DATA BREACH
1.1 million accounts on RedMart were compromised
RANSOMWARE
Hospitals and businesses targeted in Thailand
SEPT 2020
RANSOMWARE
1.5 terabytes of sensitive data stolen from subsidiary of ST Engineering Aerospace
JUNE 2020
DATA BREACH
Indonesia's e-commerce Tokopedia's 91 million users' information leaked
MAY 2020

Figure 4: Various Cyber Attacks in Southeast Asia

Ransomware threats have seen significant growth in recent years. According to Interpol data, 2.7 million ransomware attacks were detected globally in 2020. Among the ASEAN countries, Indonesia recorded the highest number of ransomware attacks (Figure 5). Chinese espionage poses a significant cyber threat to Southeast Asia. According to Symantec, over the past decade, Southeast Asian nations have become frequent targets of China's Advanced Persistent Threats (APTs), affecting critical sectors such as energy, telecommunications, finance, transportation, defence/security, and government. China conducts cyber espionage through SCADA systems, gaining control over key infrastructure, including water companies, power plants, telecommunications firms, and defence organisations. This strategic activity aligns with China's ambitions to assert itself as a regional superpower and reflects the broader geopolitical tensions stemming from the South China Sea disputes [27]. China's interests in the region are characterised by both conflict and cooperation. As countries in Southeast Asia work to avoid open conflict, deepening cooperation—particularly in trade—creates dependencies that enhance China's influence, which is further supported by military power. Consequently, Chinese espionage has become an increasingly prominent and real cyber threat to nations across Southeast Asia.

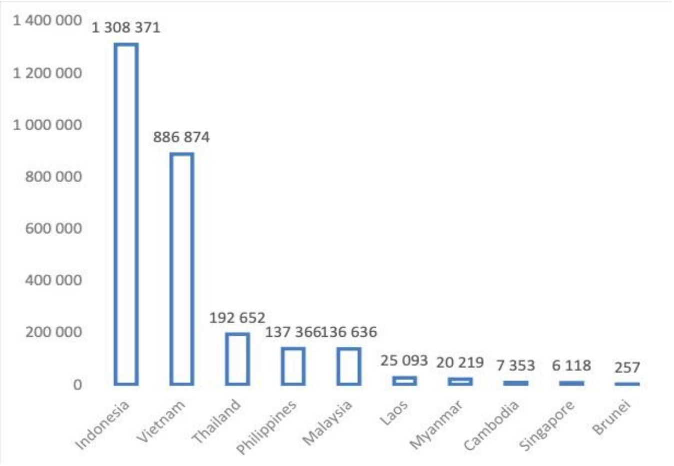

Figure 5: Number of Cyber Attacks in Southeast Asia

4.2. Cyber Threats in Indonesia's National Security

Cyber threats in Indonesia have surged, driven by its growing internet use and population. Data breaches have affected millions, including 15 million Tokopedia users in 2020, 13 million Bukalapak users in 2021, and millions of others across various platforms, including KPU voters and BSI customers [21]. In 2024, the Brain Chiper ransomware group breached the Temporary National Data Centre, demanding a ransom of USD 8 million. As of 2023, anomaly traffic reached over 403 million, with the largest threats being trojans, APT activities, and ransomware. Most cyber threats originate domestically, with 347 cyber incidents reported, primarily impacting government administration and financial sectors. Figure 6 illustrates the most affected sectors. Darknet exposure refers to the leakage of sensitive data or information from agencies and organisations, which can occur on darknet platforms such as trading forums, hacker discussion forums, or instant messaging services. By 2023, 1,647,185 data exposures affected 429 agencies, with government administrations being the most impacted at 39.78%, followed by the finance sector at 9.8% and defence at 0.2%.

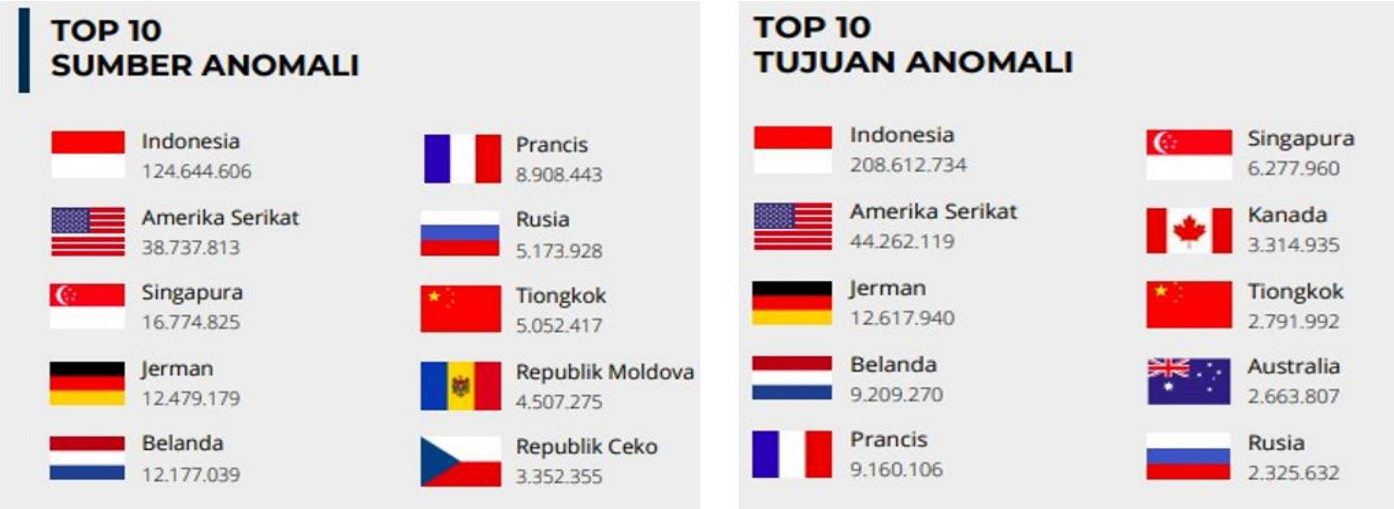

Figure 6: Source and Destination of Anomalies
Source (BSSN 2023 Report)

Numerous threats and incidents have the potential to compromise national security, fostering negative perceptions of the TNI. Cyber incidents directly impact the authority and territorial integrity of the government, with examples including the Papua Merdeka propaganda and online media provocations. These represent psychological cyberattacks that spread biased facts, framing, and manipulated information. Other cyber incidents lead to vulnerabilities in information systems, including the shutdown of the Disinfolahta information system, cryptographic attacks, application weaknesses, hacker control over systems, radar jamming, and malware infections. Recently, the threat posed by drones equipped with precision-guided munitions, as observed in other nations, has emerged as a serious concern for Indonesia's security [28].

These statistics highlight Indonesia's inadequate cybersecurity infrastructure, with current data protection efforts being insufficient. The risk of infrastructure and critical state assets becoming targets of cyberattacks is growing, underscoring the urgency of developing a robust cyber defence strategy to ensure the protection of the nation and its citizens. Information warfare is another significant cyber threat. According to Moustafa ,Bello [29], information warfare is a form of conflict in which information is used as a weapon in both military and non-military contexts. It includes propaganda, media manipulation, cyberattacks, and other information campaigns designed to influence public opinion and damage the reputation of adversaries. In Indonesia, the Free Papua Movement (OPM) has often employed such tactics, using social media platforms like Facebook and Twitter/X to spread negative narratives about the government, as well as organising demonstrations and raising the 'Bintang Kejora' flag, among other methods.

4.3. Cyber Attacks in Indonesia

ASEAN established CERT (Computer Emergency Response Team) cooperation in 2005 to facilitate the sharing of IT expertise and information on cyber vulnerabilities. Over the years, ASEAN member countries have improved their cybersecurity capabilities through CERT collaboration. The ASEAN ICT plan of 2011 led to the creation of ANSAC (ASEAN Network Security Action Council), and the ASEAN Digital Masterplan 2025 expanded CERT's role in protecting critical infrastructure and cross-border domains like maritime and aviation. Interpol also plays a role in addressing cybercrime through initiatives like ASEAN Cybercrime Operations Desks [30].

In 2017, Indonesia enacted Presidential Regulation Number 53, forming BSSN (National Cyber and Crypto Agency), which merged the National Cryptography Agency, the Information Security Directorate, and the Ministry of Information's Application Directorate General. BSSN is tasked with coordinating cyber security efforts, including detection, monitoring, mitigation, and recovery from cyber incidents. In 2022, Presidential Regulation 82 was introduced to enhance cyber security protection for vital information infrastructure in Indonesia, further empowering BSSN in this domain [31]. In 2017, Indonesia's Ministry of Defence established a cyber organisation at the echelon two level, alongside a cyber unit at the TNI headquarters, with a focus on defensive capabilities, including containment and enforcement. Within the TNI Army, the creation of a cyber unit was incorporated in the Kartika Eka Paksi doctrine, which recognised the need for a specialised military technical function with capabilities to respond to telematics security issues and conduct offensive cyber operations. To further bolster Indonesia's cyber defence, Pussansiad, the TNI AD's Cryptography and Cyber Centre, was formed in 2019 [32].

However, the management, containment, and response to cyber threats in Indonesia remain fragmented across various agencies. There are two predominant approaches to cybersecurity, with one focusing on cybercrime within business contexts and the other on national defence. These differing perspectives indicate a lack of unified authority across agencies responsible for handling cybersecurity matters. Indonesia has long been a target of cyberattacks, which are often politically or economically motivated. One early example is the 1997–1999 hacking incident related to the East Timor independence movement, where a Portuguese hacker group targeted the Indonesian government.

More recent examples include online propaganda by the OPM (Free Papua Movement), carding and bank hacking by domestic hacker groups, and cyber-terrorism activities involving figures such as Imam Samudra in 2006. These incidents underscore the use of cyberspace for political propaganda, terrorist recruitment, and illegal funding. Technological advances have introduced new threats, such as the Stuxnet worm, which affected Indonesia as the third most impacted country in 2010. Other espionage activities, like Australia's interception of Indonesian officials' phone communications, have further exacerbated cybersecurity risks and led to strained diplomatic relations. Cybercriminals have become increasingly sophisticated, targeting critical physical infrastructure. Notable examples include the theft of undersea FO cables and the destruction of BTS in Papua, which severely impacted connectivity and communication capabilities.

From 2016 to 2024, data leaks have significantly increased, with the government sector being the primary target. In 2024, the hacking of the Temporary National Data Centre caused extensive disruptions, affecting education, immigration, and agency communications. BSSN, Indonesia's cyber security agency, also faced vulnerabilities, with its Pusmanas site permanently shut down in 2021 due to limited human resources and technology. The Lockbit ransomware attack on Bank Syariah Indonesia in May 2023 highlights the severe economic consequences of cyberattacks, with customer data leaked on the darknet after failed ransom negotiations. Law enforcement struggled to prosecute cross-border cybercriminals, underscoring the challenges of tackling international cybercrime. These incidents highlight the urgent need for robust cybersecurity to protect national defence and security systems, especially with the rise of quantum computing. Cyber threats pose risks to government authority, territorial integrity, and the reputation of TNI. Cyberspace enables negative propaganda, data theft, system sabotage, and even drone attacks. Therefore, combining advanced technology with skilled and ethical human resources is crucial to mitigating future cyber threats. The data on cyber-attacks targeting infrastructure and TNI sites is illustrated in Figure 7.

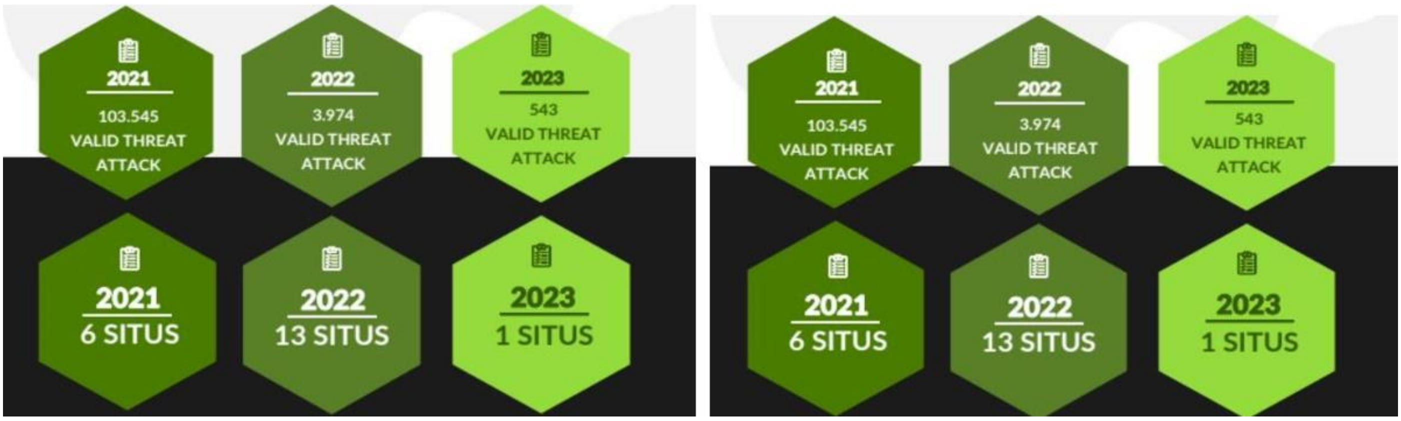

Figure 7: Attacks on Infrastructure and Website Defacement of the Indonesian Army (TNI AD)

Infrastructure and TNI AD sites have also been targeted by cyber-attacks, with recorded incidents of 103,545 attacks in 2021, 3,974 in 2022, and 543 in 2023. These attacks can be classified by their location (internal in the digital space, external in the physical realm) or by their type (technical, physical, social). Technical attacks include data breaches, website defacement, malware, brute force, and DDoS attacks; physical attacks target cyberinfrastructure, while social attacks exploit propaganda, hate speech, and disinformation in virtual spaces [33]. BSSN data indicates hundreds of millions of traffic anomalies each year, highlighting Indonesia as a prime target for both domestic and foreign hackers.

In 2018, Indonesia saw 232,447,974 attacks on its networks, with malware and trojans being the most common threats. Attacks on .co.id, .ac.id, .go.id, .sch.id, and .or.id domains showed the vulnerability of various sector websites. The following year, attacks rose to over 290 million, with the majority originating from the United States. Major incidents in 2019 included power outages in Jakarta, a data breach affecting 13 million Bukalapak users, and cyber-attacks on the Ministry of Home Affairs and the House of Representatives. In 2020, 495 million traffic anomalies were recorded, primarily driven by trojans, with the largest sources being the USA, China, and Indonesia. The year also saw a rise in cybercrimes, including website defacements and data breaches involving Tokopedia, Reddoorz, Kredit Plus, and 2.3 million KPU records. The COVID-19 pandemic and subsequent lockdowns led to a surge in internet usage and cyber-attacks, such as ransomware, Covidlock malware, and corona spyware, disguised as pandemic-related information [33].

In 2021, Indonesia experienced a dramatic rise in traffic anomalies, reaching 1.6 billion incidents, with a significant portion originating locally, indicating an increase in local hacker activity. The three most prevalent types of attacks were SQL injection, XSS. SQL injection, in particular, is capable of manipulating databases, reading sensitive data, and executing malicious commands on operating systems. That year, 83,991 data records from 78 agencies were leaked. However, the threats became more complex, as evidenced by the 4,421,992 APT activities detected throughout the year. APTs are persistent and covert attack methods that allow cybercriminals to infiltrate systems for extended periods to steal data or conduct espionage. Notable APT groups included Winnti (Blackfly/Wicked Panda) and APT40 (Leviathan/Bronze Mohawk), both suspected to originate from China, Lazarus (Hidden Cobra/Labyrinth Chollima) from North Korea, Magecart (FIN 6/Skeleton Spider) targeting the financial sector, and Kimsuky (Thallium, Black Banshee, Velvet Collima) from North Korea. The government administration sector was the most affected, with 885 website defacement incidents, followed by the defence sector, which saw 258 cases. Despite a slight decrease in traffic anomalies, the threats remained significant, particularly with the continued targeting of the government sector through website defacement, 4,001,905 APT activities, and 1,011,209 ransomware attacks. Ransomware attacks, which involve locking or encrypting data and demanding a ransom for its release, were particularly concerning.

These incidents highlight Indonesia's vulnerability to cyber threats, with infrastructure across the TNI, government, and private sectors equally at risk. The diversity of threat actors—whether state-sponsored, non-state groups, or independent hackers—adds to the complexity. The increasing sophistication of attacks requires a comprehensive approach to cybersecurity, focusing on protecting technology, enforcing regulations, and enhancing human resource capacity. Failure to optimise these aspects will result in continued cyber-attacks, which can disrupt national security, erode public trust, and hinder economic growth [34]. In August 2024, Indonesia experienced 14,918,178 traffic anomalies. Malware led with 7.9 million traffic incidents, followed by trojan activities with 3.9 million anomalies. The affected sectors included government administration (47 cases), health (1 case), finance (5 cases), ICT (2 cases), transportation (3 cases), and others (35 cases). Website hacking incidents in August 2024 totalled 11 cases, all within the government sector. This data underscores the government sector's consistent vulnerability to cyber-attacks, highlighting the need for stronger cyber defence and security in the future.

4.4. Indonesia's Cyber Defence Policy

Indonesia's cyber defence policy takes a comprehensive approach, grounded in Article 30 of the 1945 Constitution, which obligates all citizens to contribute to the nation's defence, with the TNI and the National Police (Polri) as the principal entities. The concept of total defence involves the entire population, resources, and territory. Law No. 3/2002 on National Defence highlights the multidimensional nature of modern threats, including cyber espionage, such as the 2009 phone tapping of President Susilo Bambang Yudhoyono by Australia, which falls under TNI's jurisdiction. Telecommunications and cyber regulations have evolved, starting with Minister of Communication and Information Regulation No. 26/2007, which established Id-SIRTII/CC as the incident response team. Law No. 11/2008 on Electronic Information and Transactions (ITE), amended by Law No. 19/2016, addresses cyber threats and illegal content online. Efforts against cyber terrorism were formalized by the National Counterterrorism Agency (BNPT) through Presidential Regulations No. 14/2010 and No. 12/2012, coordinating with relevant ministries and agencies. The 2008 Indonesian Defence White Paper emphasized military and non-military threats but did not focus on cyber threats. However, the 2015 Defence White Paper recognized cyberspace as the fifth domain of warfare, alongside land, sea, air, and space. This marked the integration of cyber threats into Indonesia's defence strategy, which was further bolstered by the TNI forming a cyber defence team in 2012 to develop a roadmap for cyber defence within national security structures.

In 2014, the Indonesian government took concrete steps to strengthen its cyber defence through three key Minister of Defence Regulations: No. 25/2014 on National Defence Doctrine, No. 57/2014 on Strategic Guidelines for Non-Military Defence, and No. 82/2014 on Cyber Defence Guidelines. Minister of Defence Regulation No. 82/2014 outlined the TNI's role in safeguarding internal electronic systems and coordinating cyber security across sectors when needed. Cyber defence was defined as efforts to prevent disruptions to national defence, with threats potentially originating from state or non-state actors with various interests. The regulation identified common threats such as APT attacks, DDoS, defacement, phishing, malware, and infiltration. The regulations aimed to mitigate cyber-attacks through defence, law enforcement, and counterattacks, focusing on deterrence. The targets of cyber-attacks included individuals, critical infrastructure, and symbols of national sovereignty. The need for cross-sector collaboration was highlighted, as cyber systems span government, private sectors, and civil society. While legal and institutional frameworks were in place, challenges remained in inter-agency coordination, capacity building, and system integration. To bolster Indonesia's digital sovereignty and stability, the ongoing development of infrastructure, clear authority divisions, and enhanced cyber law enforcement were deemed crucial.

Indonesia's cyber defence strategy includes prevention, monitoring, analysis, defence, and potential counter-attacks. The Ministry of Defence's role is central in securing the networks of ministries and agencies, with the formation of the Cyber Defence Centre under the Ministry of Defence's Strategic Intelligence underscoring the importance of the TNI's involvement. Presidential Regulation No. 97/2015 further integrated cyber defence into national defence planning, with Minister of Defence Regulation No. 19/2015 focusing on strengthening satellite-based intelligence and preventing sabotage, hacking, and espionage. In 2017, the establishment of the National Cyber and Crypto Agency through Presidential Regulation No. 53/2017, reinforced by Presidential Regulation No. 28/2021, marked a significant step in strengthening Indonesia's cyber defence. Despite these efforts, the agency faced a surge in hacking incidents and data breaches. In the aviation sector, Minister of Transportation Regulation No. 80/2017, later amended by No. 51/2020, mandated the protection of IT systems essential for flight safety. Additionally, Presidential Regulation No. 18/2020 (National Medium-Term Development Plan 2020-2024) prioritised the creation of Cyber Security Incident Response Teams (CSIRTs) in more than 100 agencies. Law No. 27/2022 on Personal Data Protection regulates data subject rights and obligations, with exemptions for national defence and security purposes.

Recent advancements include Presidential Regulation No. 84/2023, which supports the strengthening of the National Security Operation Centre-Security Operation Centre (NSOC-SOC) project and the formation of 12 new CSIRTs. Furthermore, Presidential Regulation No. 82/2022 highlights the protection of vital information infrastructure in critical sectors such as government administration, energy, transportation, finance, health, information technology, food, and defence. On the military front, the TNI AD has developed the Army Cryptography and Cyber Centre (TNI Defence Command No. 6/2021), the Navy is preparing the Naval-CSIRT (Chief of Staff Decision No. Kep/2604/VII/2022), and the Air Force has established a cyber unit within the Security and Cryptography Service. Additionally, the Police formed the Cyber Crime Directorate within the Criminal Investigation Agency. However, overlapping authorities among the Ministry of Communication and Information, BSSN, Ministry of Defence, State Intelligence Agency, National Counterterrorism Agency, the Police, and the three branches of the TNI remain a significant challenge. Cyber threats affect not only the public sector but also the private sector and defence infrastructure. A comprehensive national strategy is essential to clarify the division of responsibilities, build a clearer legal framework, and develop competent human resources. By fostering cross-sector synergy and a well-defined division of authority, Indonesia can better prepare for cyber threats, ranging from attacks and espionage to sabotage, ensuring the security and defence of the nation in the digital era [35].

4.5. Indonesia's Cyber Defence Capabilities

Cyber defence capabilities can be classified based on key elements such as infrastructure, budget, institutional structures, and human resources, as well as by phases/stages such as containment (preventive and mitigation), handling, and recovery. Indonesia's extensive telecommunications infrastructure provides both advantages and vulnerabilities. With 556,006 BTS towers, 479,125 km of fibre optic cables, 860 internet service providers, 216 million internet users, and 370 million mobile devices, the country also operates 17 satellites—the highest in Southeast Asia. However, this infrastructure introduces potential risks, such as the Russian-owned COSMOS 2576 satellite, which could target other satellites, and the possibility of Starlink creating vulnerabilities if not managed by a domestic NOC, as noted in the BPIP-CSIRT report (2024). The BSSN has developed a cybersecurity roadmap for 2019–2045, which focuses on strengthening technological foundations from 2019–2025, integrating intelligence and cyber warfare from 2026–2035, and achieving ICT independence by 2036–2045. BSSN also advocates for cyber resilience, which includes strengthening cyber defence, cyber warfare, and cooperation with non-state actors [23]. To improve Indonesia's position in the Global Cybersecurity Index (GCI), government agencies have established CSIRTs in critical sectors such as public safety, transportation, finance, and aerospace. Aviation is regulated by Minister of Transportation Regulation No. 80/2017, amended by No. 51/2020, with ISO 27001, DO-326A (RTCA), and ED-202A (EUROCAE) security standards.

However, a robust infrastructure alone is insufficient. Institutional synergy, clear authority, and skilled human resources are pivotal to achieving digital sovereignty [23]. The establishment of a cyber branch within the Indonesian National Armed Forces (TNI) is considered strategic, combining both defensive and offensive capabilities, following the example of several other nations that maintain specialized cyber forces. A strong legal framework is also necessary, particularly by separating the roles of cybersecurity (handled by BSSN and Polri) and cyber defence (managed by TNI). Cybersecurity primarily addresses law enforcement issues on a smaller scale, while cyber defence focuses on threats to national sovereignty, including sabotage, espionage, and information warfare. Revisions to the National Defence Law, TNI Law, and various presidential and ministerial decrees are required to clarify institutional roles and responsibilities. The Temporary National Data Centre (PDN) should be designated as a national vital object within the TNI's cyber defence domain.

The proposed cyber command structure, as suggested by Safitra ,Lubis [18] includes two models: a complex structure with multiple directorates or a streamlined model with three main components—Special Cyber Operations Command (Koopssibersus), National Cyber Operations Command (Koopssibernas), and Cyber Training Command (Kodiklat). Koopssibersus would handle strategic secret operations, Koopssibernas would manage detection, containment, recovery, and offensive operations, and Kodiklat would focus on developing doctrines, training personnel, and updating curricula to produce skilled human resources proficient in cutting-edge technologies [18]. This approach ensures that internal defense focuses on protecting TNI networks, while external defence targets critical national infrastructure. Achieving a comprehensive and efficient cyber defence strategy will require cross-agency synergy, a solid legal framework, and professional human resource management. By incorporating strategic infrastructure like the PDN under TNI control, enhancing deterrence, and creating a combined cyber command supported by Kodiklat, Indonesia can build a robust defence system capable of tackling future cyber warfare threats.

4.6. Infrastructure and Human Resources

The NCOC concept views cyber defence infrastructure and HR as a unified variable. Adequate infrastructure, encompassing tech, hardware, and software, ensures optimal HR training and education development, as supporting facilities significantly impact personnel effectiveness. According to Morić ,Dakić [13], anticipated cyber threats include APT, foreign state espionage, and disruptions to C4ISR systems. C4ISR combines radar sensors, imaging satellites, computer algorithms, and networks to process enemy data in real-time. Sabotage of C4ISR can degrade combat capabilities. Thus, increased HR capacity must be accompanied by physical infrastructure, network protection, and tech updates.

To improve the GCI, various government agencies have set up CSIRTs. Critical sectors such as public safety, transportation, finance, and aerospace are prioritized, with aviation regulated by Minister of Transportation Regulation No. 80/2017 jo No. 51/2020, following ISO 27001, DO-326A (RTCA), or ED-202A (EUROCAE) security standards. However, massive infrastructure alone is insufficient. Institutional synergy, clear authority, and reliable HR are key for digital sovereignty. Establishing a cyber branch within the TNI is strategic for combining defensive and offensive capabilities, as evidenced by specialized cyber forces in other countries. The legal framework must be reinforced by clearly distinguishing between cyber security (BSSN–Police) and cyber defence (Army). Cyber security addresses law enforcement matters on a smaller scale, while cyber defence handles threats to national sovereignty, including sabotage of critical infrastructure, espionage, and information warfare. Revisions to the National Defence Law, TNI Law, and relevant Presidential and Ministerial Decrees are essential to delineate the roles and responsibilities of each institution. The Temporary National Data Centre should be designated a vital national asset within the TNI's cyber defence domain.

The cyber command structure must be both efficient and adequate. Safitra ,Lubis [18] proposes two models: a complex structure with multiple directorates or a streamlined model consisting of the Special Cyber Operations Command (Koopssibersus), National Cyber Operations Command (Koopssibernas), and Cyber Training Command (Kodiklat). Koopssibersus would handle strategic secret operations, while Koopssibernas would manage detection, containment, recovery, and offensive actions. Kodiklat would focus on developing doctrines, training, and updating curricula to cultivate HR proficient in cutting-edge technologies [18]. Internal defence would focus on safeguarding TNI networks, while external defence would cover vital national infrastructure, transitioning from a reactive to a proactive system capable of detecting and neutralising cyber-attacks swiftly. Cross-agency synergy, a robust legal framework, and professional HR management are crucial to achieving this. Integrating strategic infrastructure, such as the PDN, under TNI control would enhance deterrence capabilities. A unified cyber command, supported by Kodiklat, could further strengthen preparedness. If all elements are managed effectively, Indonesia will have a resilient cyber defence system capable of confronting future cyber warfare threats.

The model in Figure 8 illustrates multimodal synergy in Indonesia’s cyber defence strategy, where satellites play a crucial role in navigating fighter jets, warships, and ground vehicles, subsequently transmitting data to control stations. To enhance the country’s cyber force human resources, regular recruitment processes, traditional military education pathways, and vocational schools specializing in computer engineering should be considered. Partnerships with civilian IT specialists are also essential for capacity building. However, the recruitment and training of skilled IT professionals must emphasize integrity, patriotism, and nationalism, addressing issues such as those observed within the Ministry of Communications and Digital, where employees were found maintaining gambling sites rather than blocking them.

Figure 8: Interconnection of Defence Technology Systems

Singapore's approach to talent development, which integrates mandatory military service with skill development, serves as a model for Indonesia. Though Indonesia does not have mandatory military service, it could develop a similar talent pool system by collaborating with universities, research institutions, and technology industries. Key capabilities to focus on would include detecting and responding to advanced persistent threats (APTs), managing supply chain risks, preventing social engineering attacks, and advancing cyber intelligence technologies. A civil-military collaborative approach is essential for strengthening the cyber defence workforce, ensuring strict security measures to prevent information leaks among civilian personnel. Education initiatives such as scholarships, international certifications (CISSP, CEH), and joint research projects with tech companies can enhance capabilities. Collaboration with cyber communities, such as AFDI, ID-CERT, and APTIKOM, will facilitate the exchange of ideas and improve security standards.

Although institutions like the University of Indonesia and the National Cyber and Cryptography Polytechnic could be pivotal in developing skilled human resources, the current number of cybersecurity or defence programs remains insufficient. Many programs only offer a limited number of related courses, indicating a need for a broader educational ecosystem focused on cyber defence. Establishing digital forensic laboratories and advancing military technology research will also help improve Indonesia's deterrence capacity. To retain highly skilled IT professionals, the government must provide competitive salaries, career development opportunities, and foster a sense of nationalism. International training programs will also expose personnel to the latest innovations and global trends. By aligning talent development, technological advancement, and national defence goals, Indonesia can cultivate a robust cyber force to safeguard its digital sovereignty. The overall cyber defence framework, as depicted in Figure 9, highlights the integration of these elements into a cohesive strategy.

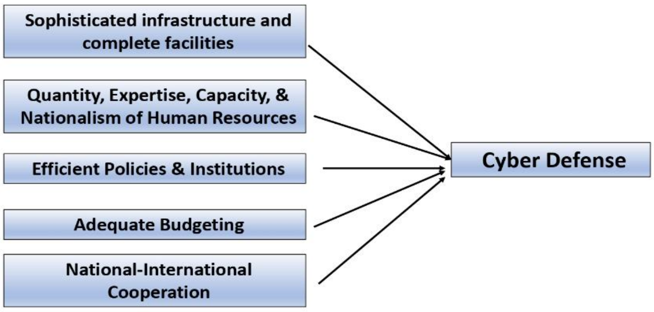
Sophisticated infrastructure and complete facilities
Quantity, Expertise, Capacity, & Nationalism of Human Resources
Efficient Policies & Institutions
Adequate Budgeting
National-International Cooperation
Cyber Defense

Figure 9: Elements of Building a Strong Cyber Defence

4.7. International Cooperation

International cooperation in cyber defence provides access to the latest threat intelligence, technologies, capacity building, and the exchange of best practices. This cooperation does not necessarily require the formation of specific blocs but opens avenues for sharing critical information for intelligence purposes. Regionally, as a founding member of ASEAN, Indonesia has actively participated in cybersecurity initiatives. From 2017–2020, ASEAN developed a cybersecurity strategy focusing on enhancing CERT capacities, coordinated by the ASEAN Digital Senior Officials Meeting. The ASEAN Digital Masterplan 2021 further highlights the importance of the digital space as a key driver of regional growth. ASEAN has also collaborated with Japan through the ASEAN-Japan Cybersecurity Capacity Building Centre to bolster capacities, facilitate information exchange, and share successful practices.

From a defence perspective, the Southeast Asian Defence Ministers (ADMM) established the ASEAN Cybersecurity and Information Centre (ACICE) in June 2021 in Singapore to address cyber threats targeting critical infrastructure. ACICE serves as a platform for information exchange, research, cyber analysis, and sharing best practices within the defence sector. On the international stage, Indonesia is a member of the International Telecommunication Union (ITU), which sets standards for telecommunications and network security. Indonesia is also a member of the International Civil Aviation Organization (ICAO), which oversees civil aviation safety and navigation. Engagement with various forums, such as APCERT (Asia Pacific Computer Emergency Response Team), also fosters knowledge exchange and expertise sharing.

Indonesia's cyber defence capacity will be further strengthened through bilateral cooperation with technologically advanced nations like the United States, France, Japan, and Singapore. Indonesia's cyber forces can benefit from learning from NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), one of Europe's leading cyber defence institutions. Additionally, Russia's robust cyber capabilities in information warfare present an opportunity for Indonesia to study its systems while maintaining a non-aligned stance. Within the TNI, Puskersin (International Cooperation Centre) manages defence relations across countries, including in the cyber domain. This collaboration can be integrated with intelligence agencies to enhance procedures and gain insights into the structure of cyber forces. Through such cooperation, Indonesia will gain technological advancements, expertise, and best practices for developing a strong cyber defence force.

5. Conclusion

Cyber warfare has evolved into a strategic threat, demanding a comprehensive approach that spans policies, technical capabilities, and human resources. The increasing complexity of cyber threats—ranging from the sabotage of critical infrastructure to espionage and hybrid attacks—necessitates the integration of cyber security, which is focused on law enforcement, and cyber defence, aimed at protecting national sovereignty. While Indonesia's legal framework has addressed cyber security through various regulations, the cyber defence landscape remains fragmented across multiple institutions, lacking clear command structures. To address this, the TNI should be positioned as the frontline in cyber defence, while BSSN and Polri focus on non-sovereignty-related cybercrime issues. Cyber defence infrastructure must include centralized SOCs, distributed servers, dedicated military satellites, and digital forensic laboratories, all aligned with international network security standards. Regarding human resources, there is a critical need for high-integrity personnel skilled in cyber technologies, AI, cryptography, and information warfare management. Furthermore, international cooperation remains vital to staying updated on the latest technologies and emerging threat patterns, ensuring that Indonesia's cyber defence capabilities are aligned with global best practices. This multi-faceted approach will enhance Indonesia's preparedness to confront the growing threats of cyber warfare.

Recommendations

a. Regulatory Framework Revision: Reassess and refine the separation of roles between cyber security (BSSN–Polri) and cyber defence (TNI). This should involve revising the National Defence Law, TNI Law, and related regulations to clearly define the TNI's responsibility for handling cyber threats that threaten national sovereignty. The revisions must ensure that TNI's jurisdiction over critical cyber defence operations is well established.

b. Formation of TNI Cyber Branch: Consolidate TNI's existing cyber units into a dedicated cyber branch, or at least establish a centralized cyber command. This command would be tasked with safeguarding strategic national infrastructure such as the PDN, power plants, air transport systems, and VVIP security. It would also possess offensive cyber capabilities to support military operations and national defence strategies.

c. Strengthening Security Infrastructure: Develop a comprehensive national SOC that operates 24/7, ensuring continuous surveillance and rapid response to cyber threats. This should include implementing end-to-end encryption, segmenting critical networks, securing military satellites, and establishing digital forensic laboratories. The infrastructure must also include integrated detection systems with rapid response mechanisms across multiple agencies to handle cyber incidents effectively.

d. Enhancing Human Resource Capacity: Establish special recruitment channels within the TNI to attract tech talent, integrating cyber training with the national defence framework. Universities should offer specialized programs in cyber defence and military technology, encouraging research and innovation. Competitive financial incentives and clear career progression pathways should be provided to retain and motivate high-specialization personnel, ensuring that the workforce is well-equipped to handle emerging cyber threats.

e. Strengthening International Collaboration: Continue and expand Indonesia's participation in ASEAN cyber defence initiatives (e.g., ACICE) and multilateral forums such as ITU, ICAO, and APCERT. Bilateral partnerships with technologically advanced countries in the cyber domain, including the US, France, Japan, and Singapore, should be pursued while adhering to non-alignment principles. These collaborations should focus on technology transfer, intelligence sharing, and joint exercises to enhance Indonesia's cyber defence capabilities.

References

[1] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, & Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics. 2023;12(6):1333. Doi: https://doi.org/10.3390/electronics12061333

[2] Altulaihan E, Almaiah MA, & Aljughaiman A. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. Electronics. 2022;11(20):3330. Doi: https://doi.org/10.3390/electronics11203330

[3] Lallie HS, Thompson A, Titis E, & Stephens P. Analysing Cyber Attacks and Cyber Security Vulnerabilities in the University Sector. Computers. 2025;14(2):49. Doi: https://doi.org/10.3390/computers14020049

[4] Hossain ST, Yigitcanlar T, Nguyen K, & Xu Y. Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. Applied Sciences. 2024;14(13):5501. Doi: https://doi.org/10.3390/app14135501

[5] Riggs H, Tufail S, Parvez I, Tariq M, Khan MA, Amir A, Vuda KV, & Sarwat AI. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. Sensors (Basel). 2023;23(8):4060. Doi: https://doi.org/10.3390/s23084060

[6] AkyeŞİLmen N. Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice. Insight Turkey. 2022:109-134. Doi: https://doi.org/10.25253/99.2022243.8

[7] Backman S. Risk vs. threat-based cybersecurity: the case of the EU. European Security. 2022;32(1):85-103. Doi: https://doi.org/10.1080/09662839.2022.2069464

[8] Mat B, Pero SDM, Zengeni KT, & Fakhrorazi A. Towards an Understanding of Emerging Cybersecurity Challenges of a Small State: A Case Study of Malaysia. Tamkang Journal of International Affairs. 2022;25(3). Doi: https://doi.org/10.6185/TJIA.V.202204_25(3).0002

[9] Cheng ECK, & Wang T. Institutional Strategies for Cybersecurity in Higher Education Institutions. Information. 2022;13(4):192. Doi: https://doi.org/10.3390/info13040192

[10] El Amin H, Samhat AE, Chamoun M, Oueidat L, & Feghali A. An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. Journal of Cybersecurity and Privacy. 2024;4(2):357-381. Doi: https://doi.org/10.3390/jcp4020018

[11] Sailio M, Latvala O-M, & Szanto A. Cyber Threat Actors for the Factory of the Future. Applied Sciences. 2020;10(12):4334. Doi: https://doi.org/10.3390/app10124334

[12] Mushtaq S, & Shah M. Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services: A Rapid Review on Optimising Public Service Management. Information. 2024;15(10):619. Doi: https://doi.org/10.3390/info15100619

[13] Morić Z, Dakić V, & Regvart D. Advancing Cybersecurity with Honeypots and Deception Strategies. Informatics. 2025;12(1):14. Doi: https://doi.org/10.3390/informatics12010014

[14] Hausken K, Welburn JW, & Zhuang J. A Review of Attacker–Defender Games and Cyber Security. Games. 2024;15(4):28. Doi: https://doi.org/10.3390/g15040028

[15] Saeed S, Suayyid SA, Al-Ghamdi MS, Al-Muhaisen H, & Almuhaideb AM. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors (Basel). 2023;23(16):7273. Doi: https://doi.org/10.3390/s23167273

[16] Caramancion KM, Li Y, Dubois E, & Jung ES. The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats. Data. 2022;7(4):49. Doi: https://doi.org/10.3390/data7040049

[17] Tatipatri N, & Arun SL. A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security. IEEE Access. 2024;12:18147-18167. Doi: https://doi.org/10.1109/access.2024.3361039

[18] Safitra MF, Lubis M, & Fakhrurroja H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability. 2023;15(18):13369. Doi: https://doi.org/10.3390/su151813369

[19] Rawindaran N, Nawaf L, Alarifi S, Alghazzawi D, Carroll F, Katib I, & Hewage C. Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom. Digital. 2023;3(3):200-231. Doi: https://doi.org/10.3390/digital3030014

[20] Pengili M, & Raszewski S. Transnational Cyber Governance for Risk Management in the Gas Sector: Exploring the Potential of G7 Cooperation. Gases. 2024;4(4):327-350. Doi: https://doi.org/10.3390/gases4040019

[21] Ulven JB, & Wangen G. A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet. 2021;13(2):39. Doi: https://doi.org/10.3390/fi13020039

[22] Singh TK, & Jha SK. From code to command: Unveiling India's cyberpower strategy. Comparative Strategy. 2024;43(3):223-236. Doi: https://doi.org/10.1080/01495933.2024.2340951

[23] Iftikhar S. Cyberterrorism as a global threat: a review on repercussions and countermeasures. PeerJ Comput Sci. 2024;10:e1772-e1772. Doi: https://doi.org/10.7717/peerj-cs.1772

[24] Alawida M, Omolara AE, Abiodun OI, & Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. J King Saud Univ Comput Inf Sci. 2022;34(10):8176-8206. Doi: https://doi.org/10.1016/j.jksuci.2022.08.003

[25] Maalem Lahcen RA, Caulkins B, Mohapatra R, & Kumar M. Review and insight on the behavioral aspects of cybersecurity. Cybersecurity. 2020;3(1). Doi: https://doi.org/10.1186/s42400-020-00050-w

[26] Poornima B. Cyber Preparedness of the Indian Armed Forces. Journal of Asian Security and International Affairs. 2023;10(3):301-324. Doi: https://doi.org/10.1177/23477970231207250

[27] Hassib B, & Shires J. Manipulating uncertainty: cybersecurity politics in Egypt. Journal of Cybersecurity. 2021;7(1). Doi: https://doi.org/10.1093/cybsec/tyaa026

[28] Guitton MJ, & Fréchette J. Facing cyberthreats in a crisis and post-crisis era: Rethinking security services response strategy. Comput Hum Behav Rep. 2023;10:100282-100282. Doi: https://doi.org/10.1016/j.chbr.2023.100282

[29] Moustafa AA, Bello A, & Maurushat A. The Role of User Behaviour in Improving Cyber Security Management. Front Psychol. 2021;12:561011-561011. Doi: https://doi.org/10.3389/fpsyg.2021.561011

[30] Monteith S, Bauer M, Alda M, Geddes J, Whybrow PC, & Glenn T. Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Curr Psychiatry Rep. 2021;23(4):18-18. Doi: https://doi.org/10.1007/s11920-021-01228-w

[31] Leventopoulos S, Pipyros K, & Gritzalis D. Retaliating against cyber-attacks: a decision-taking framework for policy-makers and enforcers of international and cybersecurity law. International Cybersecurity Law Review. 2024;5(2):237-262. Doi: https://doi.org/10.1365/s43439-024-00113-5

[32] Cremer F, Sheehan B, Fortmann M, Kia AN, Mullins M, Murphy F, & Materne S. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. 2022;47(3):698-736. Doi: https://doi.org/10.1057/s41288-022-00266-6

[33] Efthymiopoulos MP. A cyber-security framework for development, defense and innovation at NATO. Journal of Innovation and Entrepreneurship. 2019;8(1). Doi: https://doi.org/10.1186/s13731-019-0105-z

[34] Borky JM, & Bradley TH. Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering: Springer International Publishing; 2018. p. 345-404. http://dx.doi.org/10.1007/978-3-319-95669-5_10

[35] Fouad NS. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. Journal of Cyber Policy. 2021;6(2):137-154. Doi: https://doi.org/10.1080/23738871.2021.1973526