Journal of Human Security | 2023 | Volume 19 | Issue 2 | Pages 91-106
DOI: 10.12924/johs2023.19020012
ISSN: 1835-3800

Journal of Human Security

Research Article

National Cybersecurity Policy Analysis for Effective Decision-Making in the Age of Artificial Intelligence

Editha Praditya[1], Syamsul Maarif[1], Yusuf Ali[1], Herlina Juni Risma Saragih[1], Rui Duarte[1], Firre An Suprapto[2]*, Riant Nugroho[3]

[1]Republic of Indonesia Defense University.
Email: praditya.editha@gmail.com
[1]Republic of Indonesia Defense University.
Email: maarif.syamsul73@gmail.com
[1]Republic of Indonesia Defense University.
Email: yusufali8788@gmail.com
[1]Republic of Indonesia Defense University.
Email: herlinsara897@gmail.com
[1]Republic of Indonesia Defense University.
Email: ruiduarte73@yahoo.com
[2]State University of Surabaya.
Email: firresuprapto@unesa.ac.id
[3]Jenderal Achmad Yani University.
Email: riant.nugroho@lecture.unjani.ac.id

Submitted: 1 April 2023 |In revised form: 7 December 2023 | Accepted: 12 December 2023 | Published: 24 December 2023

Abstract: The increasing development of Information and Communication Technology has formed cyberspace and has given birth to threats and potential cyber-attacks that impact a nation's national interests. This study aims to address the concern of cybersecurity. It is expected that recommendations will be produced for policy, priority action plans, and thematic maps as part of the National Action Plan (NAP) for Cybersecurity. This study employed qualitative methods and utilised the Rollet model, MICMAC, and MACTOR methods for analysis. The National Cybersecurity Strategy in Indonesia aims to address the increasing incidence of technical and social cyber-attacks, including data leaks, malware, trojans, and social cyber-attacks. It seeks to implement a comprehensive and forward-thinking approach to cybersecurity. This approach highlights the significance of an integrated, collaborative, and flexible National Action Plan (NAP) for cybersecurity. The objective is to protect the country's digital interests from 2024 to 2028. The study emphasises the importance of aligning the National Action Plan (NAP) for Cyber Security with key policy directions, including the RPJMN 2020-2024, RPJPN 2025-2045, and digital transformation. The importance of comprehensive implementation of cybersecurity policies, governance, risk management, and international cooperation as foundational elements for successful transformation is emphasised. Furthermore, it emphasises the significance of continuously adapting to evolving policy directions.

Keywords: Artificial Intelligence, Cybersecurity, Policy, Micmac, Mactor, and NAP for Cybersecurity.

Introduction

The development of Information and Communication Technology (ICT) has led to the formation of cyberspace as a global domain that is becoming more integrated with people's social lives. The activities in the cyberspace domain have resulted in various threats and potential cyberattacks, which have implications for a nation's national interests (Alihosseini et al., 2021).

The digital landscape in Indonesia is currently experiencing rapid growth and is accompanied by significant potential. According to a survey conducted by the Indonesian Internet Service Providers Association (APJII), the number of internet users in Indonesia during the 2022-2023 period was 215.63 million. The number experienced a 2.67% increase compared to the previous period's 210.03 million users. The percentage of internet users in Indonesia is 78.19% of its population, which is 275.77 million. The high level of Internet literacy in Indonesia has potential value for the growth of the digital economy (Mat et al., 2019).

Indonesia's digital economy is projected to reach USD 77 billion in 2022, reflecting a 22% growth compared to 2021. Indonesia's significance in the ASEAN digital economy is notable, with approximately 40% of the total value of ASEAN digital economy transactions originating from Indonesia. Indonesia's digital economy sector experienced growth in investment, with a deal value of USD3 billion in the first quarter of 2022. This represents the second highest value, following

Singapore. The digital economy sector is projected to double its valuation to USD130 billion by 2025 and is expected to reach USD220-USD360 billion by 2030.

However, the expansive potential for the development of Indonesia's digital economy also brings about possible cyber threats and incidents. The National Cybersecurity Operations Centre report up until October 2023 documented 333,182,709 traffic anomalies. The three most prevalent anomalies were malware activity (42.9%), trojan activity (35.6%), and data leaks (9.38%). The number of consecutive data leaks in the form of cyber incidents was 22 cases from 2020 to 2022. The total number of cyber complaints in 2022 reached 1000.

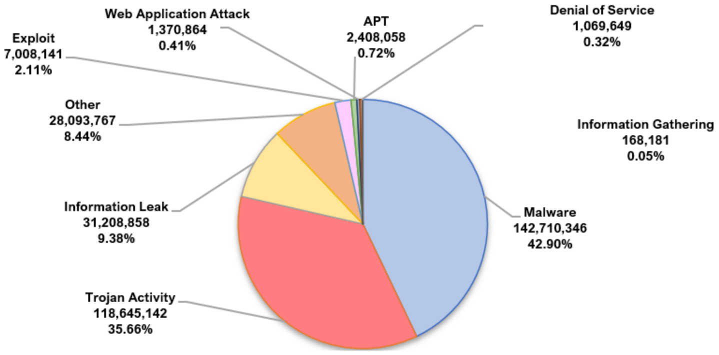

Figure 1: Indonesia Cybersecurity Traffic Anomaly January-October 2023.

The presence of cyber threats and incidents necessitates the protection of cybersecurity. Cyber-attacks on infrastructure are frequently linked to tangible entities in the physical world, resulting in actual damages and casualties (Patel & Chudasama, 2021). Cybersecurity is crucial for maintaining the uninterrupted operation of cyber infrastructure in the face of cyber-attacks. The effectiveness and reliability of information networks, both nationally and globally, require serious attention to cybersecurity to ensure their availability and integrity (Brantly, 2021).

Cybersecurity refers to the management of access to network systems and the information they contain in the cyber domain (Amuda et al., 2022). Effective maintenance of cyber domain security leads to the categorization of the cyber domain as a reliable, dynamic, and trusted digital infrastructure. Conversely, inadequate maintenance of cybersecurity poses a significant risk to the economy and national security, categorising the cyber domain as highly vulnerable within the digital world (Strelicz, 2021).

The International Telecommunications Union (ITU) (2008) defines cybersecurity as a comprehensive set of tools, policies, and technologies aimed at protecting the cyber domain and its assets. The assets in question include internet-connected computer devices, personnel, infrastructure, applications, services, telecommunications systems, and information units transmitted and/or stored in cyberspace. Cybersecurity aims to protect and preserve assets from cyber risks (Weiss & Biermann, 2023).

The ITU's description of cybersecurity indicates that it encompasses all aspects of information security, particularly in the realm of cyberspace. These efforts to secure things on the internet (Internet of Things / IoT) can also be referred to as all forms of security measures (Nayyar, 2019). The security guarantee primarily protects against various cyber-attacks, including cybercrime, malware dissemination, personal data theft, hacking, and cyber espionage.

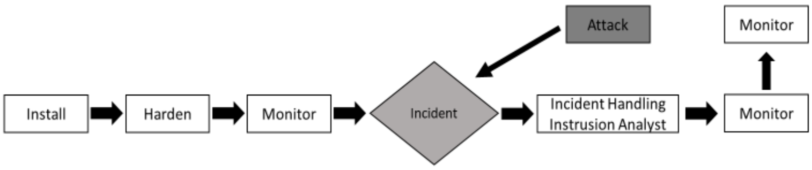

Figure 2: Cybersecurity Scope Chart.

The International Telecommunication Union (ITU) identifies five essential pillars of the national cybersecurity agenda that global cybersecurity institutions should possess (Siboni & Sivan-Sevilla, 2019). The five factors include legal certainty, technical and procedural aspects, organisational structure, capacity building, and international cooperation. The five pillars, also known as the Global Cybersecurity Agenda (GCA), are then explained in relation to the national interests of each jurisdiction as follows:

- Legal certainty refers to the requirement for a country to establish comprehensive national legislation, including cybersecurity policy and strategy documents, as well as regulations that support the implementation of cybersecurity measures.
- Exploring the technical aspects and procedures that delve into standardisation, protocol accreditation, and the identification of software vulnerabilities for cyber security purposes.
- An organizational structure created to create strategies and implementations to prevent, detect and respond to all forms of attacks on critical information infrastructures.
- Capacity building aims to enhance the knowledge and skills of cybersecurity professionals to advance the goals of the national cybersecurity policy agenda.
- International cooperation is crucial for countries to effectively address the ever-evolving challenges of cybersecurity. It is essential for nations to engage in cooperation, dialogue, and coordination to tackle these issues.

When developing a cybersecurity policy, it's important to consider different types of flows and scenarios, as well as understand the workings of a bureaucratic hierarchy. The paradigm of state administration is divided into three forms: the political system, state administration, and public policy (Safitra et al., 2023). These three elements are closely connected and depend on each other. The existence of public administration is contingent upon the seamless functioning of the three systems.

Creating a solid political climate and a strong administration is a challenge for public administration in order to achieve effective and efficient governance (Rimawi, 2022). Strong politics and administration are essential for the success of the reconciliation process. The urgency of achieving effective politics and administration that truly prioritise the welfare of the people is a pressing issue (Nguyen et al., 2020).

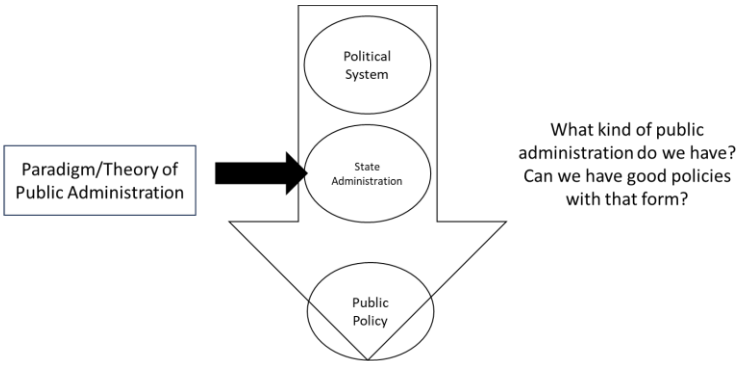
Political System
State Administration
Paradigm/Theory of Public Administration
What kind of public administration do we have? Can we have good policies with that form?
Public Policy

Figure 3: Paradigm/Theory of Public Administration.

However, public administration in Indonesia faces several challenges, including the need to improve the utilisation of technology and address the shortage of high-quality resources for e-government transformation. E-government is seen as a potential opportunity for improving the efficiency and effectiveness of state administration using information technology, in line with principles of public administration (Attajer et al., 2022). However, the implementation of e-government in Indonesia has fallen short of expectations. Based on the 2022 E-government Development Index data, Indonesia's e-government readiness index exceeds the global average of 0.7160. However, Indonesia's position needs to surpass that of other ASEAN countries (Douzet & Gery, 2021). Challenges to implementing e-government in Indonesia include insufficient regulatory framework, scarcity of skilled informatics engineers, lack of data integration among government agencies due to varying formats, inadequate funding, absence of infrastructure standards, and low levels of information security (Delerue et al., 2020).

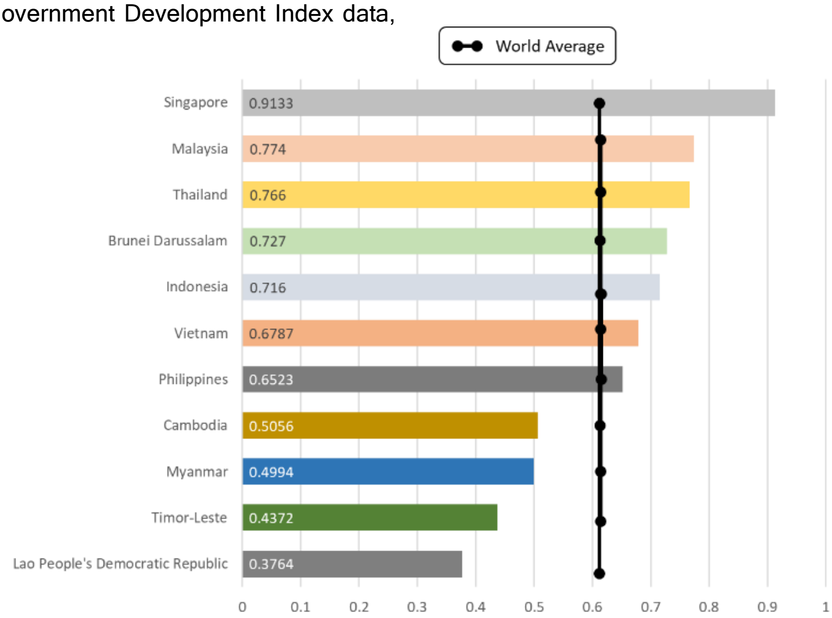

Figure 4: The Value of the E-Government Development Index of ASEAN Countries.

The government of the Republic of Indonesia recognises the need for a comprehensive and forward-thinking policy to regulate the safe, reliable, and responsible implementation of electronic systems (Bellini et al., 2021). The National Cyber Security Strategy (SKSN) is a policy that specifically addresses the advancements in the Industrial Revolution 4.0 and Information and Communication Technology (ICT). The National Cyber Security Strategy is being established through Presidential Regulation Number 47 of 2023 to guide Indonesia's cybersecurity management policy in the absence of a specific Cybersecurity Law. The SKSN policy aims to safeguard Indonesian cyberspace, aligning with the nation's strategic objectives to protect and promote its national interests as outlined in the Preamble to the 1945 Constitution (1945 Constitution), "protecting the entire Indonesian nation and all Indonesian bloodshed; promote general welfare and educate the life of the nation; and participate in the implementation of world order".

The National Cyber Security Strategy (SKSN) aims to establish a comprehensive national policy for effectively utilising cybersecurity resources to protect and promote national interests. Cybersecurity is a dynamic and creative endeavour aimed at safeguarding all aspects of cyberspace, including the information assets it holds, from technical and social threats and cyber-attacks. Implementing eight focus areas by stakeholders, known as the Quad Helix, based on the vision, mission, goals, and foundation of SKSN implementation significantly contributes to the realisation of

Indonesia's national cybersecurity objectives.

To ensure the effectiveness of the National Cyber Security Strategy (SKSN), it is necessary to outline the implementation of the national cybersecurity strategy through the National Action Plan (NAP) for Cyber Security (Valinejad & Mili, 2022). The National Action Plan (NAP) for cybersecurity is a crucial component that needs to be developed following the identification of the Security Knowledge Sharing Network (SKSN) as outlined in Presidential Regulation (Aji, 2023). The approach in SKSN involves quad-helix stakeholders, namely the Government, Business Actors, Academics, and Communities. Therefore, the formulation of the NAP for cybersecurity should be based on the commitment and agreement of all stakeholders (Njoga, 2022).

The NAP for cybersecurity spans two periods of the National Medium-Term Development Plan (RPJMN), namely 2020-2024 and 2025-2029. It is important to mention the Long-Term Development Plan (RPJP) 2025-2045 in addition to the current period. The National Action Plan (NAP) for cybersecurity is expected to address the challenges of each RPJMN period and ensure the sustainability of RPJP. Therefore, a policy recommendation is necessary to effectively address the challenges and provide guidance for the NAP for Cyber Security. Furthermore, due to the dynamic nature of cyber threat trends, it is imperative to establish a prioritised action plan for implementing SKSN, which encompasses eight distinct focus areas (Kopczewski et al., 2022).

To ensure national security stability, it is imperative to establish a comprehensive defence system capable of countering both domestic and foreign threats (Asmadi et al., 2023). Indonesia encounters a dynamic strategic environment characterised by volatility, uncertainty, complexity, and ambiguity. Arms procurement trends in regional Asia remain high due to ongoing tensions on the Korean Peninsula and the South China Sea, which could potentially lead to open conflict. Despite efforts to increase weapons of mass destruction, these tensions persist. Furthermore, in the realm of national defence, the country continues to encounter instances of interference that challenge its sovereignty in specific domains (Navas-Camargo & Ardila Castro, 2022).

The widespread use of technology and internet connectivity has important implications for potential cyber threats. The prevalence of malware cyberattacks in Indonesia indicates the escalating national security threats (Kolosok & Gurina, 2022). The severity of the threat is increasing due to regulations, infrastructure, and human resources. To address these potential threats, it is crucial to evaluate the progress of the NAP (National Action Plan) for cybersecurity instrumentation and modelling. This evaluation will help determine the compatibility between the focus area and the objectives of the National Cyber Security Strategy (SKSN) (Whyte, 2023).

This study aims to address the issue of the National Action Plan (NAP) for cybersecurity. It is expected to provide recommendations for the NAP for cybersecurity policy, priority action plans within the NAP, and thematic maps related to cybersecurity. This study aims to compile academic manuscripts to establish a scientific foundation for guiding the preparation of the National Action Plan on Cyber Security (Shull & Hilt, 2021).

Literature Review

Cyberspace and Threats in Cyberspace

Cyberspace is a global domain that is interconnected through interactions between elements in Information and Communication Technology (ICT) infrastructure (Pawar et al., 2021). Cyberspace can be considered as a component of the information environment, which encompasses individuals, organisations, and systems involved in collecting, processing, disseminating, and acting on information. This environment also relies on physical domains like land, air, sea, and space (Amedzro St-Hilaire & Amedzro St-Hilaire, 2020). The dependence mentioned is linked to the structure of cyberspace, comprising three layers: the physical layer, the logic network layer, and the social layer.

- The physical layer consists of two primary components: the geographical and physical network components. The geographic component pertains to the physical location of the network component, which comprises two subcomponents: hardware and infrastructure (including cable, wireless, and optical infrastructure). The integration of geographical components and physical networks results in strategic hardware and information technology infrastructure. We strategically position this infrastructure on land, sea, air, and space to store, disseminate, and process information in cyberspace. It also facilitates the connection and movement of data between sub-components in the physical network. The physical layers encompass computer equipment, data storage facilities, internet network equipment, and cables. The physical layer plays a crucial role in cyberspace operations as it determines the geographical location and jurisdiction of cyberspace. It is important to protect this layer to prevent physical damage to devices and infrastructure, as well as to avoid unauthorised access that can lead to operational failures.
- The second layer is the technical logic network layer, which is an abstract component of the physical layer. The second layer comprises interconnected logical relationships in computer programming code that facilitate the operation, exchange, and processing of data between different networks. Logic networks in cyberspace are commonly known as software connected to hardware at the initial layer.
- The social layer as third layer pertains to the cognitive aspects of individuals (heart and mind). The layer is composed of two primary components: personal and cyber components. The persona component refers to the human subject or actor within the network system in cyberspace. The cyber-persona component is an extension of the logic layer that represents the user's identity in the cyberspace network system. Cyber-persona components encompass email addresses, social media accounts, usernames, and passwords, which can potentially portray fictitious, concealed, or anonymous identities of individuals within networked systems in cyberspace.

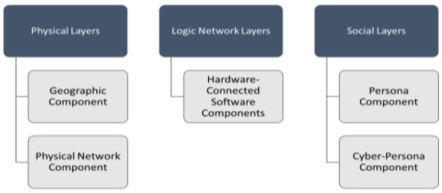

Figure 5: Visualization of Three Layers of Cyberspace.

Meanwhile, dangers in the digital realm or online dangers are the desires and abilities of specific entities, including both governments and non-government entities, that can potentially materialise as cyber-attacks. These attacks occur across three layers: the physical layer, which includes geographical and network components; the logical networks; and the social layer, which consists of personal and online personas (Azmi, 2020). Instances of cyberattacks involve deliberate actions by specific individuals or groups aimed at inflicting damage and harm on the targeted party (Kör & Metin, 2021). There are three main categories of threats and attacks in the cyber domain: information control, cyber espionage, and cyber sabotage. These can be observed in Table 1.

Table 1: Cyber Trends at The Global Level in The Context of Future Wars.

Trend	Attacking Actor	How to Fix	Warfare Domain	Why Countries Will Go to War in Cyberspace
Information Control	State and non-state actors	War and information operations to counter the offensive narrative	Cyberspace	Prevent propaganda that can influence public opinion and result in the disharmony of the nation
Spionase Cyber	State and non-state actors	Strengthen cyber defences, and continue to build various detection methods against cyber intrusions	Cyberspace	Protect national interests, intellectual property, and research and development activities in each country
Sabotage Cyber	State and non-state actors	Build a resilient, layered network	Cyberspace	Protect critical infrastructure and communication networks, and prevent data corruption

Source: Adapted from The Future of Warfare in 2030 (RAND, 2020).

In addition, considering the current cyber trends worldwide, it can be inferred that cyber-attacks can take on various forms, encompassing both technical and social aspects, depending on the specific circumstances in which the attack occurs. These implications extend to the three layers of cyberspace. In addition, considering the increasing frequency of cyber-attacks, it is possible to classify them into different categories such as cyber-crime, cyber extraordinary crime, or cyber warfare. The classification is based on the motivation, purpose, and intensity of the attack (Bahtiar et al., 2021). Cyberattacks can occur at any time, regardless of the prevailing circumstances.

Technical Cyberattacks

- These attacks are focused on infiltrating the logic network of cyberspace, using intrusive technical methods to gain unauthorised access to the target's network and systems. The goal is to cause damage, manipulate data, steal information, or insert malicious content, which in turn affects the overall cyberspace environment. When it comes to impact, technical attacks can be classified into three different levels of intensity: low, moderate, and high.
- The range of low-intensity technical attacks involves cyberattacks that aim to create confusion or disorientation, spread propaganda, undermine trust in the target party, and disrupt their activities. Instances of low-intensity technical attacks include Denial of Service (DoS) and Distributed Denial of Service (DDoS), website defacement, unauthorised access to social media accounts, and the act of revealing personal information online (taking confidential information from an individual, organization, or country that is then used to embarrass that individual, organization, or country publicly).
- A range of medium-intensity technical attacks refers to a type of cyberattack that seeks to unlawfully access information systems of a targeted party to manipulate information or for other purposes, such as extortion. Instances of moderate-intensity technical attacks include hacking and malware (Trojans, viruses, worms, or rootkits).
- The spectrum of high-intensity technical attacks is a high-difficulty cyberattack that uses a variety of sophisticated methods to attack industrial control systems (SCADA) that can cripple the target party's National Vital Information Infrastructure (IIVN). An example of a high-intensity technical attack is the use of malware assembled in such a way with a high level of sophistication, such as logic bombs or zero-day exploits.

Overall, technical cyberattacks can impact other layers of cyberspace, namely the physical layer (especially physical network components consisting of hardware and infrastructure such as cables, routers, and servers), logic network layer (system and how software works), or information contained in that cyberspace.

Social Cyberattacks

There is a strong connection between cyberattacks that target humans and activities such as political warfare, information warfare, psychological warfare, and propaganda. The primary focus of cyberattacks with a social aspect is the third layer of cyberspace, which involves the mindset, belief systems, and attitudes of individuals engaging with cyberspace. Information plays a crucial role in social cyberattacks, as it is strategically crafted to enhance the impact of various activities conducted by the attacker. These activities can encompass political, diplomatic, economic, and military aspects, among others. Examples of manifestations of cyberattacks with a social focus include socio-cognitive hacking, social hacking, pseudo-social hacking, disinformation, forgery and leaks, Potemkin villages of evidence, false identities, bots, and botnets, trolling and flaming, and even humour and memes. There are at least six strategies commonly used in cyberattacks of a social nature, such as the following:

- Black propaganda is a strategy to create and spread false evidence through social media to cause social unrest in society.
- Point and shriek are a strategy to exploit issues very sensitive to specific groups of people.
- Information flooding is the strategy of flooding the information space with conflicting information so that the public can no longer judge the credibility of the data of a phenomenon.
- Cheerleading is a strategy to deliberately affect the target party's brain or cognitive capacity so that it can no longer distinguish credible and non-credible information.
- Raiding is a strategy that takes the form of a coordinated attack on an information arena to extinguish the influence of a particular opinion that is developing in society.

Polarisation is a deliberate strategy aimed at dividing society into two opposing categories of opinions that strongly contradict each other. Polarisation frequently arises during a democratic competition.

In the study entitled Factors Related to Cyber Security Behavior (Ana1, Nenad Putnik1,) *"... The environment is a very important factor when analysing cyber security, ... It was shown that the effects of cyber security perceptions, knowledge, and experiences are stronger than the effects of socio-demographics for cell phone related behaviour..."*. So applicable policies can be used as protection in activities in cyberspace and form awareness and influence the improvement of human resource capacity.

Artificial Intelligence

Intelligence encompasses the information necessary for shaping and implementing government policies to safeguard national security and address challenges posed by actual or potential adversaries. For information to be considered "intelligence," it is essential to establish a systematic process that allows government officials to access and utilise publicly available information effectively. Intelligence agencies frequently carry out this task (Hromada et al., 2021).

In Germany, there is a lot of discussion about industry 4.0, a term that was introduced at the 2011 Hannover Fair to describe the transformative impact of this industrial revolution on a global scale. The Industrial Revolution 4.0, also known as the Fourth Industrial Revolution, marks the fourth phase of industrial development following the initial revolution in the 18th century. In the era of the 4IR, there is a convergence of technologies that are blurring the boundaries between the physical, digital, and biological realms. This fusion is referred to as cyber-physical systems or CPS. Various new technologies also surfaced during the fourth industrial revolution. Furthermore, the rise of technological advancements in different fields has signalled the arrival of the fourth industrial revolution (Murdoch & Leaver, 2015). These areas encompass a wide range of cutting-edge fields, such as robotics, artificial intelligence, nanotechnology, quantum computing, biotechnology, internet of things, industrial internet of things, fifth-generation wireless technology, 3D manufacturing and additive printing, and the fully autonomous vehicle industry.

As a pursuit, intelligence entails the gathering and examination of intelligence information. It also involves activities carried out to counter the intelligence activities of an adversary, either by preventing them from accessing information or by misleading them about its truth or importance (Czejdo et al., 2014). Thus, intelligence as an activity can be described as a crucial element in a battle between opponents focused primarily on information (as an opponent, for example, economic competition, diplomatic maneuvering or negotiation, or the threat or use of military force) (Presidential Regulation of the Republic of Indonesia Number 47 of 2023).

Artificial intelligence, also known as AI, is a field of computer science that holds great potential for meeting future human needs. The term "intelligence" is derived from the Latin word "intelligo", which translates to "I understand". Thus, comprehending, and acting lies at the heart of intelligence. In addition, Budiharto mentioned that intelligence is a complex concept that can be characterised by qualities like comprehension, reasoning, self-awareness, adaptability, strategizing, and critical thinking (Gupta et al., 2021). Nevertheless, "artificial" is often used to describe things that are not genuine, like deception, as they arise from imitation (Colabianchi et al., 2021). Sapitri described artificial intelligence (AI) as a subfield of computer science that is dedicated to creating machines that can mimic human intelligence and behaviour. The progress of this field was incredibly fast during the time of the fourth industrial revolution. Furthermore, Budiharto and Suhartono highlighted the wide range of applications for artificial intelligence, spanning from broad areas like learning and perception to more specialised tasks such as playing chess, proving mathematical theories, composing poetry, driving cars, and diagnosing diseases (Patriarca et al., 2022). Sterling Miller explains that the foundation of artificial intelligence lies in cognitive computing, which involves instructing computers to communicate, reason, learn, and make decisions.

Research Methodology

This study was conducted using qualitative methods using primary data and secondary data. Primary data were obtained from the results of Focus Group Discussion (FGD) and interviews with representatives of work units at BSSN RI.

The analytical approach utilised in this study incorporates the Rollet model along with the MICMAC and MACTOR methods. The MICMAC method is a structural analysis method that was first introduced by Dupperin and Michael Godet in 1973 (Soesanto, 2021). This approach provides a solution to the complexity by systematically and structurally ranking the elements of a system and analysing the relationships between variables. The MICMAC method is commonly used to identify key factors.

The MACTOR (Multi-Issue Actor) method is utilised to analyse the relationships between stakeholders in understanding the issues and objectives to be accomplished. The MACTOR method utilises three primary inputs that pertain to the influence relationship between one actor and another. There are three key factors to consider: (1) the position of the actors, (2) their interests, and (3) the influence they have on each other (Godet, 2001). The inputs are analysed using a position matrix known as the Actor-Objective Matrix (1MAO) and 2MAO. The Salience variable is used to determine the priority of goals set by the actor to achieve the objective. The third matrix, known as the Matrix of Influence Direct (MID), provides a description of the influence variable. Additionally, we compute the influence variables of the MID matrix using the Matrix of Indirect and Direct Influence to evaluate the degree of direct and indirect influence among various actors (MIDI).

Research Results

Cyberattack Data in Indonesia

Several instances of cyber-attacks in Indonesia involve the unauthorised disclosure of personal information of Indonesian residents, airline passengers, e-commerce users, and fintech users. These compromised data sets are then traded on illicit websites on the dark web. According to the National Cybersecurity Operations Centre report until October 2023, Indonesia experienced a total of 333,182,709 traffic anomalies. The most common anomalies were malware activity (42.9%), trojan activity (35.6%), and data leaks (9.38%). There was a total of 22 instances of data leaks reported between 2020 and 2022, resulting from cyber incidents. There were a significant number of cyber complaints in 2022, totaling 1000.

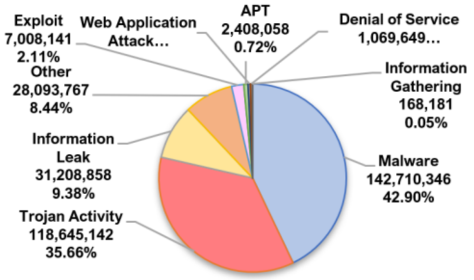

Figure 6: Traffic anomaly 1 January - 1 October 2023 (Directorate of Cyber Security Operations, 2023).

In addition, the Indonesian government has observed a significant number and level of social cyber-attacks. These attacks are evident in the way Indonesian individuals engage with information online, including its creation, storage, and distribution. The implications of these attacks on public behaviour at a national level have raised concerns about Indonesia's national security interests. According to the latest data from the Ministry of Communication and Informatics (Kominfo) Negative Content

Statistics until May 2023, there have been a significant number of negative content incidents on online platforms. The top three categories of negative content include pornography, gambling, and fraud. Meanwhile, according to the latest data, the primary concerns identified by BSSN monitoring from January to June 2023 include politics, cybercrime, terrorism, narcotics, and pornography.

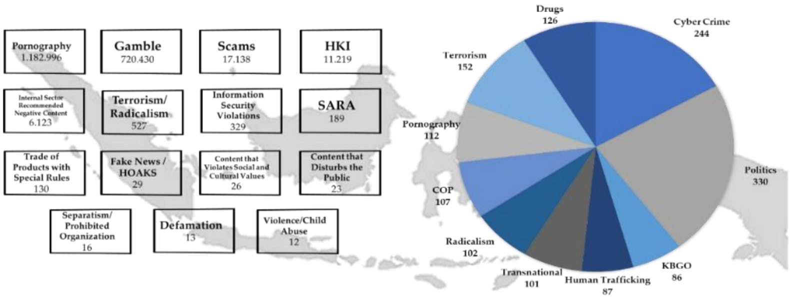

Figure 7: Proportion of Social Cyberattacks (Handling of Negative Content of Communication and Information and BSSN Monitoring).

Based on the above data, the Indonesian government predicts that the trend of cyber-attacks of a technical and social nature in 2024-2028 will continue to experience a significant increase that requires the formulation and implementation of an integrative, synergistic, innovative, adaptive, flexible, and futuristic NAP for cybersecurity.

National Cybersecurity Strategy

To achieve national goals in the digital era, it is crucial for countries to develop and execute effective strategies in the cyber domain. These strategies play a vital role in defending, fighting, and advancing a country's national interests. In connection with this, SKSN identifies three key characteristics that a strategy should have: It is crucial to recognise that academic endeavours should serve as the foundation for ongoing and evolving efforts. By formulating and implementing effective strategies, we can work towards creating the desired conditions for the future. This involves actively influencing and engineering both internal and external factors within the Indonesian nation to achieve our national goals.

Thus, the Indonesian nation's pursuit of national cybersecurity is intricately connected to the analysis, refinement, and engineering of the internal and external strategic landscape that impacts the nation's pursuit of its goals in cyberspace. In simple terms, this SKSN focuses on the current capabilities of the Indonesian nation to make the necessary decisions and actions to reach the desired national objectives in the future (Heck et al., 2016). The SKSN combines two different approaches to strategic thinking: system-1, which focuses on creativity and future-oriented perspectives, and system-2, which emphasises critical analysis and historical context. These two systems work together to form a comprehensive national strategy, as outlined in the components of SKSN. These components include ensuring cybersecurity, safeguarding the national digital economy ecosystem, enhancing the strength and effectiveness of cybersecurity measures, and prioritising national interests. A global cyberspace that is open, secure, stable, and responsible (Pham, 2022).

The foundation for the implementation of SKSN is a fundamental modality and the key to the successful implementation of SKSN. The basis for the implementation of SKSN has three sub-components, namely law, totality of potential strength, and real nation as well as synergy of all components of the nation.

National cybersecurity stakeholders play a crucial role in implementing SKSN. Stakeholders in the context of SKSN represent the active participation of all elements of the Indonesian nation. These are categorised into four groups or known as the Quad Helix: the government; business actors; Academics; and community. The stakeholders are crucial in the development and execution of SKSN as all the activities in the focus area are closely tied to the responsibilities of each Quad Helix component. In the realm of academia, every aspect of the Quad Helix plays a vital role. However, it is at the practical level where these roles intersect and require seamless collaboration and cooperation.

The National Cybersecurity Strategy comprises various focus areas and a comprehensive national action plan for Cybersecurity. The implementation of the Cybersecurity Strategy is accomplished through eight key areas of focus. These areas include governance of cybersecurity, managing risks, enhancing preparedness and resilience, bolstering the protection of critical information infrastructure, ensuring national cryptographic independence, improving capability, capacity, and quality, developing effective cybersecurity policies, and fostering international cooperation. The Cyber Security action plan is a comprehensive strategy that outlines specific goals and initiatives to effectively address the focus areas of the National Cybersecurity Strategy. The action plan has been prepared for a duration of five years. It is crucial to consider the national development plan, advancements in science and technology, and the evolving strategic environment.

Discussion

Cybersecurity Policy

The successful implementation of SKSN's goals in enhancing cybersecurity in Indonesia is evident in its dedicated focus on 8 key areas outlined in the action plan. The chosen focus of this area will be elaborated upon to effectively achieve the objectives of SKSN. The goals of SKSN are to achieve cybersecurity, safeguard the national digital economy ecosystem, enhance the resilience and effectiveness of secure cyberspace, prioritise national interests, and promote the development of an open, secure, stable, and responsible global cyberspace.

The implementation of the action plan's focus area is crucial to attain the desired national cybersecurity conditions. The action plan emphasises various areas including governance, risk management, preparedness, and resilience, strengthening the protection of vital information infrastructure (IIV), national cryptographic independence, increased capability, capacity and quality, cyber security policy, and international cooperation. The eight focus areas of the action plan will be implemented by stakeholders (Quad Helix) from 2020 to 2024. Area of focus, Quad Helix, and interactions within a specific timeframe.

Various challenges and risks are the focus in addressing each Focus Area of the Action Plan. The following describes the challenges, risks, and objectives of each of the eight focus areas in implementing the Action Plan:

Focus Area 1: Governance

The primary area of focus in the action plan is governance. In this context, governance refers to a collection of factors that emphasise the state's formal involvement in actively leading the national cyberspace. In this case, governance is a field of work that primarily focuses on the strategic and national levels, with a strong emphasis on the role of government. Essentially, this factor plays a crucial role in achieving a country's cybersecurity objectives. It is essential to implement two strategies in this area of focus.

The focus area presents several challenges and risks. One of them is the lack of government efforts to establish standards across all sectors in strengthening the cybersecurity ecosystem. Additionally, there are numerous international standards in the field of cybersecurity, which adds complexity to the landscape. The coordination related to cybersecurity between stakeholders is still weak, hindering effective collaboration. Furthermore, the implementation of cybersecurity measures to stakeholder.

Focus Area 2: Risk Management

The risk management factors in national cybersecurity involve a range of initiatives aimed at safeguarding the country from cyber threats and attacks, as well as mitigating the potential losses that these threats can inflict on a national level.

In this field of interest, there are several challenges and potential risks that need to be addressed. One of these challenges is the lack of comprehensive implementation of cyber security risk management across all sectors. Additionally, there is a low level of awareness regarding the importance of implementing risk management strategies. Another issue is the lack of standardised understanding of cyber risks among different risk owners, including at the K/L level. Furthermore, there ‘Collaboration among stakeholders in the field of cybersecurity mitigation needs improvement, as does the formulation of risk-based cybersecurity policies. Additionally, existing cybersecurity policies have not adequately addressed the risks at hand.

Focus Area 3: Preparedness and Resilience

Preparedness and resilience factors encompass a range of measures aimed at mitigating risks associated with cyber threats and attacks. This variable is closely tied to the efforts aimed at preserving the uninterrupted flow of national economic activity and recovering from any potential attack or cyber incident. The goal is to achieve the desired level of cyber resilience.

There are several challenges and risks in this area of focus. One of them is the lack of coordination and optimal management when it comes to handling cyber incidents. Additionally, the number of cyber incidents is on the rise, and there is no contingency plan in place for managing cyber crises. The coordination and management of cybersecurity emergency response also need improvement, as well as maximising the culture of sharing information related to cybersecurity emergency response.

Focus Area 4: Strengthening Vital Information Infrastructure Protection (IIV)

Factor of protection IIV refers to a range of initiatives aimed at safeguarding and enhancing the capabilities of the IIVN sector in the realm of cybersecurity. The challenges and risks in this area involve the constant threat of cyber-attacks, which often target important information and systems. It is important to note that the implementation of certain measures has not been fully completed.

Focus Area 5: National Cryographic Independence

Ensuring the confidentiality and authenticity of information or data is a crucial aspect of cybersecurity. It is essential to prioritise national cryptographic independence and maintain independence in the policy or application of cryptography at a national level. The challenges and risks in this area revolve around incomplete and insufficient policies governing cryptography, limited research and innovation in the field, underdeveloped cryptographic industry, lack of widespread planning and application of cryptographic functions to support electronic system security, and low adoption of cryptography.

Focus Area 6: Capability Improvement, Capacity, and Quality

Efforts to enhance knowledge and skills in cybersecurity are aimed at developing a strong understanding of the subject and improving the quality of human resources. The significance of this factor cannot be overstated, as it directly impacts the nation's progress and competitiveness in the cyber domain on a global scale. It serves as a crucial aspect of national cyber security and resilience, hinging upon the calibre and ethical values of the nation's human resources.

The challenges and risks in this focus area include low public understanding of cyberspace security, lack of comprehensive regulation on ethics in cyberspace education in Indonesia, limited availability of Professional Certification Bodies in cybersecurity, limited expertise in cybersecurity, low public awareness of cybersecurity, increasing cyber incidents, limited players in the cybersecurity technology industry, low research and innovation in cybersecurity technology, and limited application of common criteria. Cybersecurity technology remains limited, with low levels of research and innovation. Education programmes for vulnerable groups lack regulation in the field of cybersecurity. Vulnerable groups are specifically targeted by cyber threats and crimes.

Focus Area 7: Cybersecurity Policy

Cybersecurity policy aims to establish legal norms to address various forms of criminal activities in cyberspace. The challenges and risks in this focus area encompass the growing complexity of cybersecurity issues, accompanied by increasing opportunities and threats. In Indonesia, cyber law only regulates electronic information, transactions, and prohibited acts. Implementing regulations for cybersecurity are mandated by various laws and regulations. However, public legal awareness regarding cybersecurity remains low, while cyber incidents and threats continue to rise. There has been a lack of coordination in law enforcement efforts concerning cyber incidents.

Focus Area 8: International Cooperation

The international cooperation factor refers to the Indonesian nation's active role in promoting an open, safe, stable, and responsible global cyberspace. Implementation of four variables is necessary in this cybersecurity focus area.

The challenges and risks in this focus area include the lack of policies and roadmaps for international cooperation in cybersecurity, increasing foreign initiatives for collaboration in security, low levels of information sharing forums between countries for addressing cyber crises, limited experience, and knowledge in handling cyber crises domestically, underutilization of Indonesia's contribution in international forums, and the growing number of international forums on cybersecurity.

Cyber NAP Matrix Analysis

The NAP for cybersecurity encompasses eight focus areas and aims to establish the state's presence in cyberspace to mitigate the risk of potential cyber crises. The national cyber crisis in Indonesia is characterised by cyber threats that encompass both technical and social-based cyber-attacks. Failure to effectively address these threats poses a significant risk to Indonesia's national interests.

A matrix analysis was conducted to determine the priority level of each activity in the cybersecurity NAP. This study compared the National Action Plan (NAP) for cybersecurity matrix with the priority activities outlined in the 2020-2024 RPJMN matrix. The priority activities in the NAP for cybersecurity are those that intersect in the two matrices. The figure below presents the results of the comparative analysis between the NAP for cybersecurity matrix and the 2020-2024 RPJMN matrix.

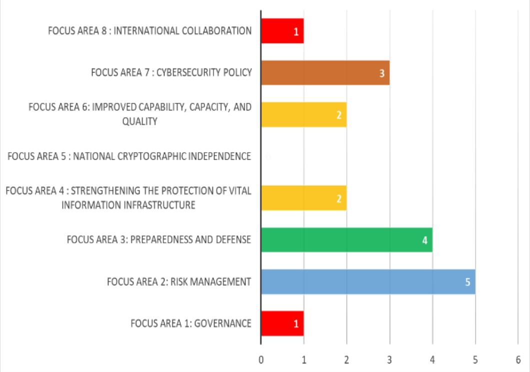

Figure 8: Distribution of priority programs of NAP for cybersecurity.

The findings indicate that there is a significant overlap between 18 activities in the NAP for cybersecurity and priority activities in the 2020-2024 RPJMN. There are a total of 18 priority activities in the Cyber-Communications NAP, highlighting its significance in the academic field. Table 2 provides a comprehensive overview of the priority activities for each focus area.

Table 2: Priority Activities of Each Focus Area.

Focus Area	Activity
Governance	• Develop national cybersecurity criteria and standards. • Develop cyber governance mechanisms that include policy, monitoring, testing, escalation, incident response, and performance metrics from cyber stakeholders.
Risk Management	• Appointment of Risk Champion as Coordinator of cybersecurity risk implementation in Ministries / Institutions / Agencies. • Develop a cybersecurity risk profile in the IIV sector including IIV operators in the private sector. • National Cybersecurity Risk Assessment including validation of controls. • Implementation of Risk Treatment Plan according to National Risk Assessment Results • Collaborate in the preparation of a list of common threat vectors in the sector. • Conduct technical guidance in the preparation of risk-based cybersecurity policies to IPPS
Preparedness and Resilience	• Establishment of a cyber incident response team • Improving the Implementation of Cyber Incident Management nationally • Organizing national emergency response • Cyber Information Sharing Guidelines • Risk-based cyber incident reporting from private and government parties.
Strengthening Vital Information Infrastructure Protection	• Identify IIV organizers in each sector. • Strengthening cybersecurity operating systems for PIIV • Assessment of cybersecurity practices of IIV operators in the private and government sectors. • Adoption of international standards and best practices on cybersecurity at IIV operators.
Increased Capability, Capacity, and Quality	• Encouraging the improvement of the quality of Cybersecurity Human Resources in the IIV sector • Building a cybersecurity culture
Cybersecurity Policy	• Conduct analysis and evaluation of laws and regulations related to cybersecurity. • Forum koordinasi penegakan hukum dalam penanganan aduan siber • Providing a means of legal complaints in the field of cybercrime for the public
International Cooperation	• Increase bilateral cooperation in the field of cybersecurity, especially intelligence sharing to mitigate threat actors

Rollet Model Analysis

The Rollet Model explores two different perspectives when it comes to implementing an activity in the Action Plan: the process point of view and the interaction point of view. The interaction viewpoint considers the interconnections between various "agents" as they interact with one another to achieve cybersecurity. The process perspective prioritises the utilisation of knowledge as the focal point. Process point of view analysed by category below:

1. Planning: Effective planning is a crucial aspect of managing cybersecurity. It is important to establish clear objectives for each aspect of Cybersecurity, ensuring they align with the broader cybersecurity strategy. Effective planning in the field of cybersecurity ensures that the expectations of all parties are understood and encourages agreement and dedication.
2. Creating: There are two methods for an organisation to enhance its Cybersecurity portfolio: either by developing new Cybersecurity solutions or by acquiring established ones.
3. Integrating: Exploring the integration of cybersecurity involves examining the different methods through which a country can access existing cybersecurity measures. This involves obtaining Cybersecurity from external sources (such as recruiting new IT staff, sending IT staff to conferences, hiring IT consultants, conducting Cybersecurity research through market or software research reports, etc.) or internal sources, such as integrating existing Cybersecurity (e.g. by discovering previously non-existent Cybersecurity).
4. Organizing: Organising Cybersecurity enhances its value by constructing various structures for Cybersecurity that organisations can utilise. In the academic realm, the Cybersecurity context is often analysed and organised using methods such as hierarchical classification or Cybersecurity mapping.
5. Transferring: Cybersecurity Transfer involves purposeful and organised exchanges of cybersecurity information, as well as the sharing of cybersecurity resources as needed, e.g. Cybersecurity transfer using internal training.
6. Maintaining: Cybersecurity Maintenance consists of reviewing, correcting, updating, refining, preserving, to remove/replacing Cybersecurity.
7. Assessing: There are various forms of cybersecurity assessment. When evaluating Cybersecurity at an individual level, it is important to consider ratings for relevance, accuracy, completeness, and timeliness criteria. From a more advanced perspective, the measurement of intellectual capital aims to portray the comprehensive understanding of Cybersecurity that is accessible to society. Evaluating cybersecurity assessment involves analysing the level of success in meeting cybersecurity objectives.

An analysis was conducted on the Rollet model, focusing on all activities outlined in the NAP for cybersecurity. Figure 13 displays the visualisation of the results obtained from analysing the Rollet model. In general, the activities planned have been deemed suitable for supporting each strategic goal in every focus area, with the aim of enhancing cybersecurity. The activities conducted are highly integrated and meticulously organised. However, there is a need to enhance the process of transferring, maintaining, and assessing as a long-term strategy for implementing the planned activities.

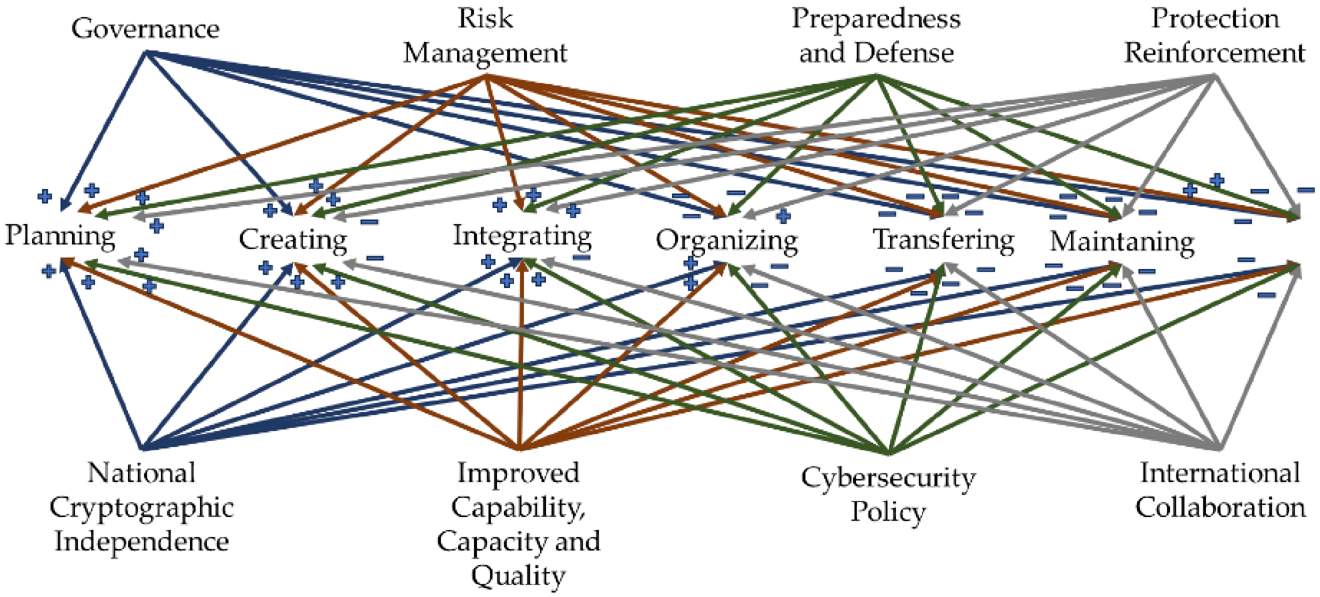

Figure 9. Distribution of Priority Programs of NAP for Cybersecurity.

Cyber National Action Plan (NAP) Matrix Analysis

The formulation and implementation of the NAP for cybersecurity, as described in eight focus areas, is the presence of the state in cyberspace from the risk of cyber crises that may occur. In this case, the national cyber crisis manifests as cyber threats into technical and social-based cyber-attacks, which, if not appropriately managed, threaten Indonesia's national interest.

MICMAC, also known as Matrix of Cross Impact Multiplications Applied to A Classification, is an operational method of structural analysis developed by Godet. It serves as a platform for conducting development scenario analysis studies, with a particular focus on sustainable development and future studies (AlMajali et al., 2016). The MICMAC approach emphasises the importance of analytical thinking and systematic problem-solving. Thus, MICMAC initiates the process by defining the problem and subsequently recognising both internal and external variables. In the upcoming phase, MICMAC will thoroughly examine the connection between variables and evaluate their significance by considering the level of dependence between them. An analysis was conducted on the 18 priority activities of the Cyber-NAP to examine the interconnections between each activity that has been developed. The results of the MICMAC analysis are displayed in this Figure.

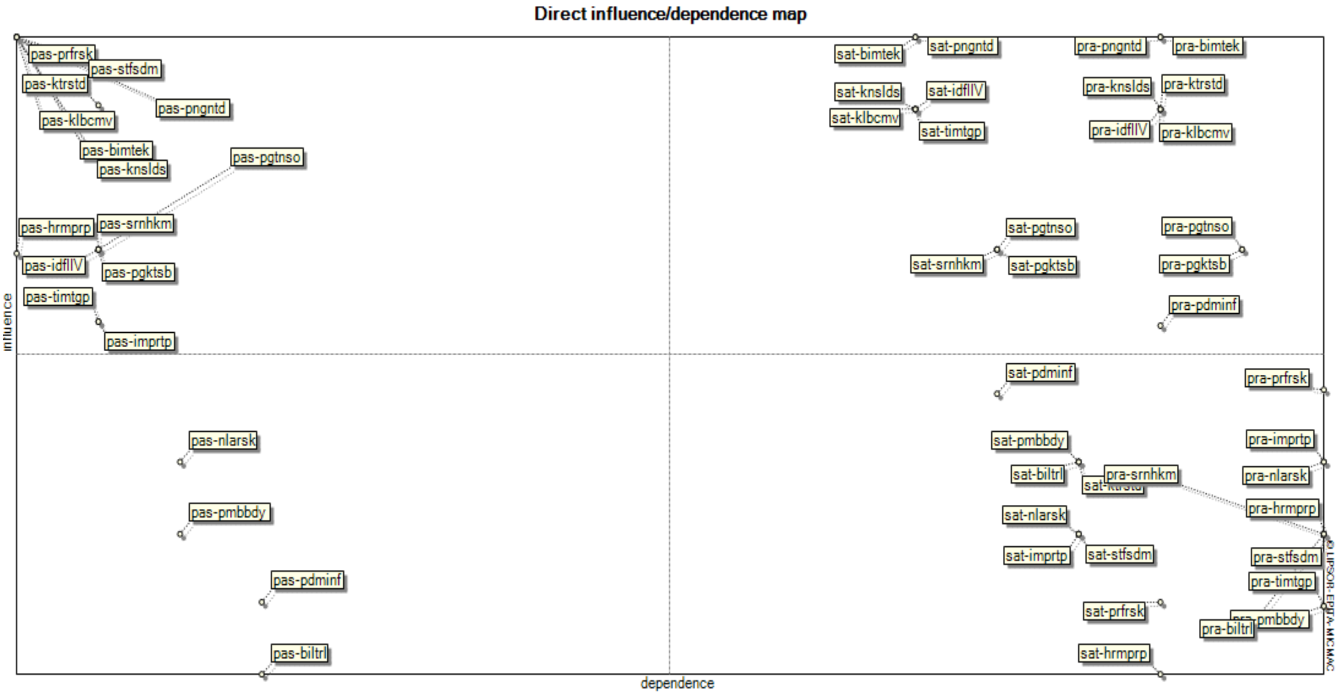

Figure 10: Distribution of Priority Programs of NAP for Cybersecurity.

The description of each variable code is explained in the following table.

Table 3. Tabel label of MICMAC.

No	Code	Information
1	pra-ktrstd	pre-Develop national cybersecurity criteria and standards
2	sat-ktrstd	on-Develop national cybersecurity criteria and standards
3	pas-ktrstd	post-Develop national cybersecurity criteria and standards
4	pra-prfrsk	pre-Develop a cybersecurity risk profile in sector IIV
5	sat-prfrsk	on-Develop a cybersecurity risk profile in sector IIV
6	pas-prfrsk	post-Develop a cybersecurity risk profile in sector IIV
7	pra-nlarsk	pre- National Cybersecurity Risk Assessment
8	sat-nlarsk	on-National Cybersecurity Risk Assessment
9	pas-nlarsk	post-National Cybersecurity Risk Assessment
10	pra-imprtp	pre-Implementation of Risk Treatment Plan according to National Risk Assessment Results
11	sat-imprtp	on-Implementation of Risk Treatment Plan according to National Risk Assessment Results
12	pas-imprtp	post-Implementation of Risk Treatment Plan according to National Risk Assessment Results
13	pra-klbcmv	pre-Collaborate in the preparation of a list of common threat vectors in the sector
14	sat-klbcmv	on-Collaborate in the preparation of a list of common threat vectors in the sector
15	pas-klbcmv	post-Collaborate in the preparation of a list of common threat vectors in the sector
16	pra-bimtek	pre-Conduct technical guidance in the preparation of risk-based cybersecurity policies to IPPS
17	sat-bimtek	on-Conduct technical guidance in the preparation of risk-based cybersecurity policies to IPPS
18	pas-bimtek	post-Conduct technical guidance in the preparation of risk-based cybersecurity policies to IPPS
19	pra-timtgp	pre-Establishment of a cyber incident response team
20	sat-timtgp	on-Establishment of a cyber incident response team
21	pas-timtgp	post-Establishment of a cyber incident response team
22	pra-pgktsb	pre-Improved Implementation of Cyber Incident Management
23	sat-pgktsb	on-Improved Implementation of Cyber Incident Management
24	pas-pgktsb	post-Improved Implementation of Cyber Incident Management
25	pra-pngntd	pre-Organizing emergency response
26	sat-pngntd	on-Organizing emergency response
27	pas-pngntd	post-Organizing emergency response
28	pra-pdminf	pre-Cyberthreat Information Sharing Guidelines
29	sat-pdminf	on-Cyberthreat Information Sharing Guidelines
30	pas-pdminf	post-Cyberthreat Information Sharing Guidelines
31	pra-idfIIV	pre-Identify IIV organizers in each sector
32	sat-idfIIV	on-Identify IIV organizers in each sector
33	pas-idfIIV	post-Identify IIV organizers in each sector
34	pra-pgtnso	pre-Strengthening cybersecurity operating systems for PIIV
35	sat-pgtnso	on-Strengthening cybersecurity operating systems for PIIV

36	pas-pgtnso	post-Strengthening cybersecurity operating systems for PIIV
37	pra-stfsdm	pre-Encourage certification of Cybersecurity Human Resources in sector IIV
38	sat-stfsdm	on-Encourage certification of Cybersecurity Human Resources in sector IIV
39	pas-stfsdm	post-Encourage certification of Cybersecurity Human Resources in sector IIV
40	pra-pmbbdy	pre-Building a cybersecurity culture
41	sat-pmbbdy	on-Building a cybersecurity culture
42	pas-pmbbdy	post-Building a cybersecurity culture
43	pra-hrmprp	pre-Harmonization, analysis and evaluation of laws and regulations related to cybersecurity
44	sat-hrmprp	on-Harmonization, analysis and evaluation of laws and regulations related to cybersecurity
45	pas-hrmprp	post-Harmonization, analysis and evaluation of laws and regulations related to cybersecurity
46	pra-knslds	pre-Consolidation between law enforcement in handling cyber complaints
47	sat-knslds	on-Consolidation between law enforcement in handling cyber complaints
48	pas-knslds	post-Consolidation between law enforcement in handling cyber complaints
49	pra-srnhkm	pre-Providing a means of legal complaints in the field of cybercrime for the community
50	sat-srnhkm	on-Providing a means of legal complaints in the field of cybercrime for the community
51	pas-srnhkm	post-Providing a means of legal complaints in the field of cybercrime for the community
52	pra-biltrl	pre-Enhancing bilateral cooperation in the field of cybersecurity
53	sat-biltrl	on-Enhancing bilateral cooperation in the field of cybersecurity
54	pas-biltrl	post-Enhancing bilateral cooperation in the field of cybersecurity

Variables in the quadrant I possess a significant degree of influence and exhibit minimal reliance on external factors. Quadrant I encompass the essential activities of the NAP for cybersecurity that require follow-up or are contingent upon the completion of these tasks. The post-activity variables of the cybersecurity risk profile constituents in sector IIV have a significant impact but minimal reliance on other factors. This indicates that it is crucial to ensure the long-term sustainability of the Cyber NAP's priority activities to successfully achieve the objectives of SKSN. Specifically, it is important to address any cybersecurity risks in sector IIV.

Quadrant II contains variables with a high level of influence and dependence, often called relay variables, that describe the instability of a system. Overall, the variables in quadrant II are dominated by the priority activities of the NAP for cybersecurity before and when these activities are carried out. This shows that the preparation and execution of activities will affect other activities (especially post-activity) and interdependence between one another.

Variables in Quadrant III exhibit a strong dependence on other variables but have limited influence themselves. They are vulnerable to changes in influential variables and variable relays. There are four variables in this quadrant: the National Risk Assessment, the development of a cybersecurity culture, increased bilateral cooperation in cybersecurity, and the Cyber Threat Information Sharing guidelines.

Quadrant IV consists of excluded or autonomous variables with minimal influence and dependence. These variables play a crucial role in achieving the objectives of SKSN by carrying out various activities in line with the priorities set by the NAP for cybersecurity in this quadrant. The visual representation of the relationship between each variable is depicted in Figure 11.

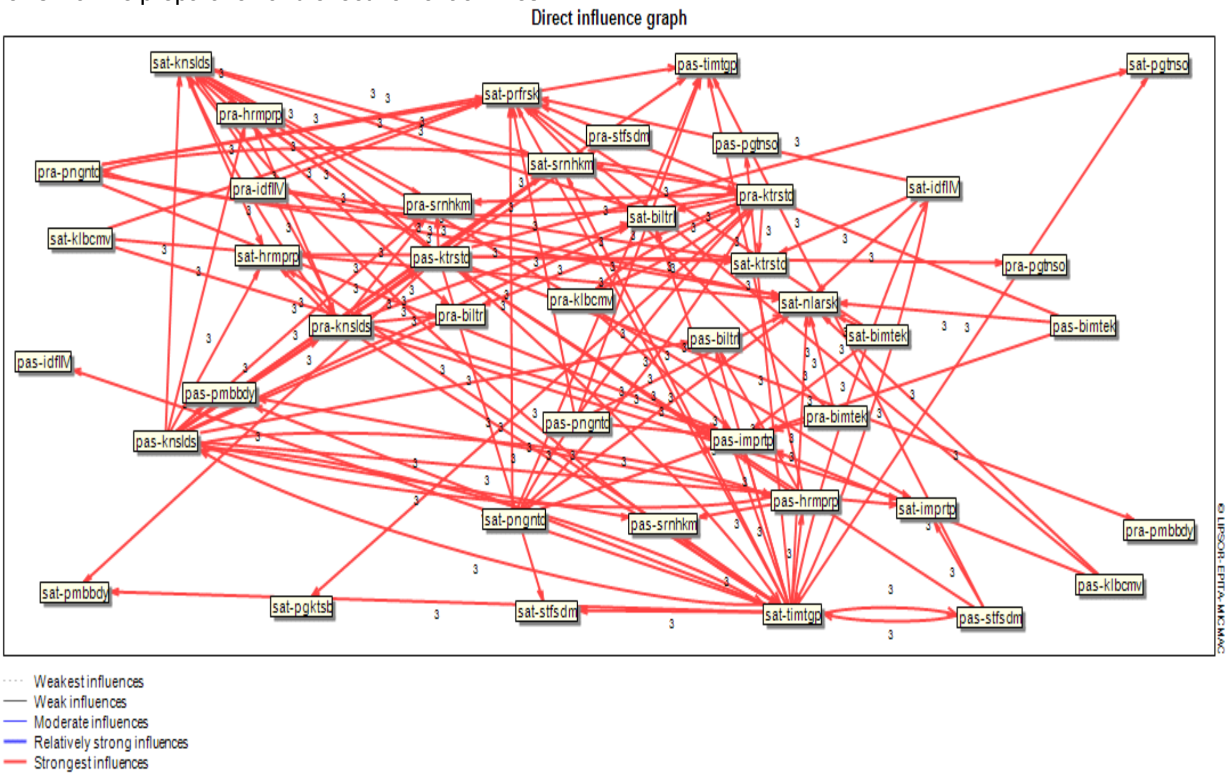

Figure 11: Visualization of Relationships Between Priority Activities and Cyber Camps.

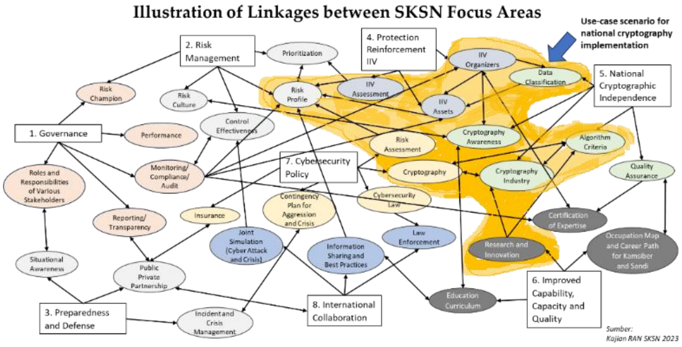
Illustration of Linkages between SKSN Focus Areas
Use-case scenario for national cryptography implementation
1. Governance
2. Risk Management
3. Preparedness and Defense
4. Protection Reinforcement IIV
5. National Cryptographic Independence
6. Improved Capability, Capacity and Quality
7. Cybersecurity Policy
8. International Collaboration
Risk Champion
Risk Culture
Prioritization
Risk Profile
IIV Assessment
IIV Organizers
IIV Assets
Data Classification
Control Effectiveness
Performance
Roles and Responsibilities of Various Stakeholders
Monitoring/ Compliance/ Audit
Reporting/ Transparency
Insurance
Situational Awareness
Public Private Partnership
Incident and Crisis Management
Joint Simulation (Cyber Attack and Crisis)
Contingency Plan for Aggression and Crisis
Information Sharing and Best Practices
Risk Assessment
Cryptography
Cryptography Awareness
Cryptography Industry
Algorithm Criteria
Quality Assurance
Cybersecurity Law
Law Enforcement
Certification of Expertise
Research and Innovation
Occupation Map and Career Path for Kamsiber and Sandi
Education Curriculum

Sumber: Kajian RAN SKSN 2023

Figure 12: Visualization of the Relationship Between SKSN Focus Areas.

The picture above is an illustration that shows the relationship between the 8 SKSN Focus Areas, where each output result in each focus area can be an input or requirement for fulfilling other focus areas. Here is a narrative of linkage with practical examples in its implementation, as follows:

A crucial foundation for a robust national cyber posture is establishing a strong governance framework that prioritises transparency, accountability, responsibility, independence, and fairness (TARIF) among cyber stakeholders. Concentrate The governance area has specific requirements for the formulation and implementation of cyber policies, as well as job descriptions. It also involves monitoring the performance of cyber stakeholders, ensuring compliance, reporting cyber metrics, and overseeing governance, risk management, and compliance in cybersecurity. Therefore, it is crucial to designate an executive coordinator from each ministry to oversee governance, risk management, and compliance in implementing this specific focus area, known as the Risk Champion. It is crucial to make the cybersecurity performance transparent and publicly available so that the public can evaluate and trust the national cybersecurity posture. The reporting context can include the number of escalations, satisfactory results, the effectiveness of cyber control, cyber risk profile, cyber risk trends, and national cyber awareness.

a) This position is vital to the Risk Management Focus Area, where the Risk Champion will be crucial in implementing the National Cyber Risk Assessment and preparing the cyber risk profile of the K/L/I. They will also coordinate risk reporting, including risk registers, indicator risks, incidents, and cyber issues. Additionally, they will play a key role in risk awareness campaigns in K/L/I and monitor the effectiveness of control over identified cyber risks. This Risk Champion will also collaborate and engage with Risk Champions from other K/L/I to ensure that cybersecurity priorities can be adapted, and potential cyber risk trends can be addressed in line with the risk appetite of the organisation. Within the Risk Management Focus Area, BSSN can analyse the risk profile of each K/L/I. This includes examining risk trends and identifying any controls that require attention. By doing so, BSSN can effectively prioritise and allocate resources to address cyber risk matters that require immediate attention.

b) The implementation of risk management will align with the Focus Area of Cyber Security Policy. This includes identifying IIV operators in the focus area of Strengthening Protection IIV, identifying cyber risks in each K/L/I according to the regulated cyber risk taxonomy, and identifying control over cyber risks in terms of type, nature, and timing of implementation. The risk management focus area requires constant monitoring of risk priorities to ensure effectiveness and security measures. It also involves assessing and auditing cybersecurity in IIV, as well as promptly reporting any incidents or risk issues to the relevant cyber stakeholders in the government sector, private sector, and IIV operators. It is essential to have a periodic risk register in the risk management focus area and IIV protection focus area. This register should include a list of IIV assets, operators, types of cyber security measures, cybersecurity certifications, and data classifications managed in the IIV. Ensuring consistency in IIV safeguards across all sectors is crucial, which involves reviewing all IIV sectors to guarantee that all IIV operators adhere to international standards.

c) In addition, to ensure the effectiveness of control over identified cyber risks, the internal control unit (APIP) coordinates with the Risk Champion to implement a periodic control testing process in K/L/I. This test is also addressed in the Focus Area of Readiness and Resilience, emphasising the significance of contingency plans as the main control, incident management process, escalation process, and crisis management in the context of cyber-attacks. These aspects are explored through national simulations involving the private sector, and if necessary, international cooperation from the Focus Area of International Cooperation. It is essential to publish the results of control testing as part of the implementation of the Governance Focus Area. The K/L/I Risk Profile needs to be updated within the framework of the Risk Management Focus Area and the Cybersecurity Policy Focus Area. This update should also serve as validation for the national cyber risk assessment results.

d) In its implementation, the criteria formulated in the focus area of cybersecurity policy encompass various aspects. This includes technology criteria, international cyber security standards, best practices of the cybersecurity process, cryptographic criteria based on the level of data classification, and laws related to cybersecurity that authorise law enforcement in the field. These laws also grant the authority to cooperate with international parties in terms of information sharing, investigat in this field, it is crucial to establish a cyber mandate within the Cyber Law to serve as a guiding principle for BSSN in fulfilling its responsibility of upholding Indonesia's cyber security, which includes law enforcement and safeguarding cyber sovereignty on the global stage.

e) The criteria outlined in this cybersecurity policy form the foundation for the advancement of cyber capabilities in the field of Cyber Capability Improvement. Our primary objective is to embrace cutting-edge technology, incorporate international cyber certification into our curriculum, provide appealing career paths and incentives for cyber professionals, and encourage exchanges or internships between government sectors, private sector, and international partners. By implementing best practices and adhering to international standards, it is possible to establish a comprehensive cyber ecosystem. This ecosystem would encompass various aspects such as raising awareness about cyber threats, promoting the use of cryptography in the private sector, fostering the development of a local market for cyber technology and insurance, and ensuring the availability of skilled cyber professionals. The independence of technology and the strength of the local cyber industry will contribute to the achievement of national cryptographic independence. This will allow for the fulfilment of local cyber needs while still adhering to industry best practices.

f) Furthermore, by working together with the government and private sector, the academia can play a crucial role in enhancing capabilities. This collaboration can lead to the development of priorities and the establishment of a clear direction for cyber technology. These decisions can be informed by research findings, innovation labs, and quality assurance measures resulting from the implementation of risk management and cryptography.

Therefore, all focus areas are crucial and can be executed simultaneously, as they are interdependent on the masking of both input and output for each focus area. It is essential to establish a clear rule and mechanism for the implementation of the National Action Plan (NAP) and the Cyber Law's cybersecurity mandate. This requires prioritising the governance focus area, the risk management focus area, and the cybersecurity policy focus area as the starting point. The upcoming priorities include the IIV Strengthening Focus Area, Capability Enhancement Area Focus, and Cyber Resilience Area Focus. The Focus Area of International Cooperation and Cryptographic Independence should be considered a lower priority, following the optimal implementation of the priority (Governance, Policy, and Risk Security) and the second priority (Resilience, Capability and IIV). The primary focuses of International Cooperation are information exchange and law enforcement. The primary concern regarding cryptographic independence is to address the local need for cryptography while adhering to cybersecurity best practices considering advancements in Quantum Computing.

Policy Analysis Tools for Strengthening Human Resources in the Era of Artificial Intelligence

Utilising policy analysis tools to enhance human resources is essential for tackling national cybersecurity challenges. The analysis of national cybersecurity policies indicates that information security threats are becoming more intricate and advanced, necessitating the enhancement of human resources capable of addressing these evolving challenges. Cybersecurity skills training and development prioritise the cultivation of competent human resources in the AI era (Vinichenko et al., 2020). The training programme should cover intelligence technologies, cyber threats, and information security defence strategies comprehensively. Enabling HR to effectively respond to increasing cyberattacks.

The collaboration among government, industry, and educational institutions is crucial for developing a significant workforce in the field of cybersecurity. Policies promoting strategic partnerships between the public and private sectors should be established by governments. Conversely, educational institutions should modify their curricula to incorporate a more comprehensive comprehension of cybersecurity and human intelligence (Abdeldayem & Aldulaimi, 2020).

The government plays a crucial role in promoting research and innovation in the field of human intelligence, which is vital for human resource development. The provision of funding and incentives for cybersecurity and AI research can stimulate the development of innovative solutions and improve human resources expertise in these domains.

It is crucial to incorporate ethics and responsibility in artificial intelligence usage into HR training. HR can make informed decisions by considering the social, privacy, and cybersecurity implications of AI.

Regular monitoring and evaluation of HR progress in cybersecurity is crucial. Government agencies and industry collaboration in assessing training programme effectiveness and identifying development needs can ensure HR's relevance and preparedness for evolving cybersecurity challenges (Obeid et al., 2020).

Conclusions

The study of the national action plan for cyber security concluded that the policy recommendation for the 2024-2028 period is to complete the policy direction of RPJMN 2020-2024 in the field of cyber security and strengthen cybersecurity as the foundation of transformation. This recommendation considers the policy direction of RPJMN 2020-2024, RPJP 2025-2045, and digital transformation. The implementation of Presidential Regulation 82 of 2022 on IIV protection needs to be expedited in the National Action Plan (NAP) for cybersecurity activities.

The RPJMN prioritises seven focus areas, including governance and national cybersecurity criteria and standards, by conducting a Micmac analysis to set strategic objectives in terms of direction, focus, and priority. A cybersecurity risk profile will be developed in the IIV sector, focusing on risk management. This will involve conducting a national cybersecurity risk assessment, implementing a risk treatment plan based on the assessment results, collaborating on the creation of a list of common threat vectors in the sector, and providing technical guidance for the development of risk-based cybersecurity policies for IPPS.

The preparedness and resilience focus area includes the establishment of cyber incident response teams, enhanced implementation of cyber incident management, emergency response management, and guidelines for different types of cyber threat information. The focus area of strengthening vital information infrastructure (IIV) protection involved identifying IIV implementation in each sector and enhancing cybersecurity operating systems for PIIV. Additionally, cybersecurity policy was analysed and evaluated, laws and regulations related to cybersecurity were examined, a law enforcement coordination forum was established to handle cyber complaints/incidents, and legal complaint facilities were provided for the public in the field of cybercrime. The focus area of international cooperation will prioritise enhancing bilateral cooperation in cyber security.

According to industry and organisational best practices, it is important to prioritise certain areas to strengthen cybersecurity as a foundation for successful transformation. These areas include governance, risk management, and cybersecurity policy. These should be the starting point for implementing the National Action Plan (NAP), particularly the cybersecurity mandate of the Cyber Law. The upcoming priorities will be the IIV Strengthening Focus Area, Capability Enhancement Area Focus, and Cyber Resilience Area Focus Area. The Focus Area of International Cooperation and Cryptographic Independence can be the last priority after the priority (Governance, Policy, and Risk Security) and the second priority (Resilience, Capability and IIV) run optimally. For International Cooperation, information exchange and law enforcement are of utmost importance. When it comes to cryptographic independence, our focus is on meeting the local demand for cryptography while also staying up to date with the latest advancements in Quantum Computing and following cybersecurity best practices. The focus of the NAP for cybersecurity for the 2024-2028 period revolves around the effective implementation of cybersecurity measures to support the protection of critical infrastructure and information systems.

Considering the results and conclusions obtained, it is advisable to expand the preparation of the cybersecurity NAP study by incorporating additional planning documents. Regarding the timing of the preparation of the cybersecurity study, it was done before the formation of the 2025-2029 RPJMN document. Therefore, once the 2025-2029 RPJMN is established, additional research can be conducted by carefully considering the policy direction outlined in the document. The expectation is that due to the dynamic nature of the strategy and the fact that the NAP for cybersecurity is a living document, adjustments can be made to the NAP by considering the policy's direction.

References

Abdeldayem, M. M., & Aldulaimi, S. H. (2020). Trends and opportunities of artificial intelligence in human resource management: Aspirations for public sector in Bahrain. *International Journal of Scientific and Technology Research*, *9*(1), 3867-3871. https://www.researchgate.net/publication/340460650

Aji, M. P. (2023). Dynamics of encryption and cyber security policy in Indonesia as a socio-cultural change in the cyber age. *Jurnal Scientia*, *12*(03), 2307-2315. https://doi.org/10.58471/scientia.v12i03.1551

Alihosseini, H., Alikarami, H., & Ahmadifar, R. (2021). Civil Liability Regulations for Privacy in Cyberspace in line with Information Security. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *18*(4), 2135-2155. https://archives.palarch.nl/index.php/jae/article/view/6650/6443

AlMajali, A., Viswanathan, A., & Neuman, C. (2016). Resilience evaluation of demand response as spinning reserve under cyber-physical threats. *Electronics*, *6*(1), 2-14. https://doi.org/10.3390/electronics6010002

Amedzro St-Hilaire, W., & Amedzro St-Hilaire, W. (2020). How to Win the Digital Security Challenge in Terms of Governance? *Digital Risk Governance: Security Strategies for the Public and Private Sectors*, 131-141. https://doi.org/10.1007/978-3-030-61386-0_13

Amuda, O. K., Akinyemi, B. O., Sanni, M. L., & Aderounmu, G. A. (2022). A Predictive User Behaviour Analytic Model for Insider Threats in Cyberspace. *International Journal of Communication Networks and Information Security*, *14*(1), 150-159. https://doi.org/10.54039/ijcnis.v14i1.5208

Asmadi, A., Almutahar, H., Sukamto, S., Zulkarnaen, Z., Listiani, E. I., & Sikwan, A. (2023). Digital Information Security Policy in the National Security Strategy. *International Journal of Multidisciplinary Approach Research and Science*, *1*(02), 96-103. https://doi.org/10.59653/ijmars.v1i02.61

Attajer, A., Chaabane, S., Darmoul, S., Sallez, Y., & Riane, F. (2022). Evaluation of Operational Resilience in Cyber-Physical Production Systems: literature review. *IFAC-papersonline*, *55*(10), 2264-2269. https://doi.org/10.1016/j.ifacol.2022.10.045

Azmi, R. H. N. (2020). Indonesian Cyber Law Formulation in The Development Of National Laws In 4.0 Era. *Lex Scientia Law Review*, *4*(1), 46-58. https://doi.org/10.15294/lesrev.v4i1.38109

Bahtiar, A., Purwadianto, A., & Juwono, V. (2021). Analisa Kewenangan Badan Intelijen Negara (BIN) dalam Penanganan Pandemi Covid-19. *Jurnal Ilmiah Ilmu Pemerintahan*, *6*(2), 178-192. https://doi.org/10.14710/jiip.v6i2.11475

Bellini, E., Marrone, S., & Marulli, F. (2021). Cyber resilience meta-modelling: The railway communication case study. *Electronics*, *10*(5), 583. https://doi.org/10.3390/electronics10050583

Brantly, A. F. (2021). Risk and uncertainty can be analyzed in cyberspace. *Journal of Cybersecurity*, *7*(1), tyab001. https://doi.org/10.1093/cybsec/tyab001

Colabianchi, S., Costantino, F., Di Gravio, G., Nonino, F., & Patriarca, R. (2021). Discussing resilience in the context of cyber physical systems. *Computers & industrial engineering*, *160*, 107534. https://doi.org/10.1016/j.cie.2021.107534

Czejdo, B. D., Iannacone, M. D., Bridges, R. A., Ferragut, E. M., & Goodall, J. R. (2014). Integration of external data sources with cyber security data warehouse. Proceedings of the 9th Annual Cyber and Information Security Research Conference, 49-52. https://doi.org/10.1145/2602087.2602098

Delerue, F., Douzet, F., & Géry, A. (2020). The geopolitical representations of international law in the international negotiations on the security and stability of cyberspace. IRSEM/EU Cyber Direct, 13-63. https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/EOETDUfd/report-75-delerue-et-al-v2.pdf

Directorate of Cyber Security Operations. (2023). Traffic anomaly 1 January - 1 October 2023

Douzet, F., & Gery, A. (2021). Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace. *Journal of Cyber Policy*, *6*(1), 96-113. https://doi.org/10.1080/23738871.2021.1937253

Godet, M. (2001). *Creating Futures: Scenario Planning as a Strategic Management Tool* Economica, 280. http://en.laprospective.fr/dyn/anglais/articles/CreatingPressRelease.pdf

Gupta, K., Sahoo, S., Panigrahi, B. K., Blaabjerg, F., & Popovski, P. (2021). On the assessment of cyber risks and attack surfaces in a real-time co-simulation cybersecurity testbed for inverter-based microgrids. *Energies*, *14*(16), 4941. https://doi.org/10.3390/en14164941

Heck, H., Kieselmann, O., & Wacker, A. (2016). Evaluating connection resilience for self-organizing cyber-physical systems. 2016 IEEE 10th international conference on Self-Adaptive and Self-Organizing Systems (SASO), 114-141. https://doi.org/10.1109/SASO.2016.20

Hromada, M., Rehak, D., & Lukas, L. (2021). Resilience assessment in electricity critical infrastructure from the point of view of converged security. *Energies*, *14*(6), 1624. https://doi.org/10.3390/en14061624

Kolosok, I., & Gurina, L. (2022). Cyber resilience models of systems for monitoring and operational dispatch control of electric power systems. *IFAC-papersonline*, *55*(9), 485-490. https://doi.org/10.1016/j.ifacol.2022.07.084

Kopczewski, M., Ciekanowski, Z., Nowicka, J., & Bakalarczyk-Burakowska, K. (2022). Security threats in cyberspace. *Scientific Journal of the Military University of Land Forces*, *54*(3), 415-426. https://doi.org/10.5604/01.3001.0016.0040

Kör, B., & Metin, B. (2021). Understanding human aspects for an effective information security management implementation. *International Journal of Applied Decision Sciences*, *14*(2), 105-122. https://doi.org/10.1504/IJADS.2021.113532

Mat, B., Pero, S., Wahid, R., & Sule, B. (2019). Cybersecurity and digital economy in Malaysia: Trusted law for customer and enterprise protection. *International Journal of Innovative Technology and Exploring Engineering*, *8*(3), 214-220. https://www.ijitee.org/wp-content/uploads/papers/v8i8s3/H10610688S319.pdf

Murdoch, S., & Leaver, N. (2015). Anonymity vs. trust in cyber-security collaboration. Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, 27-29. https://doi.org/10.1145/2808128.2808134

Navas-Camargo, F., & Ardila Castro, C. A. (2022). Cyberspace, Artificial Intelligence, and the Domain of War. Ethical Challenges and the Guidelines Proposed by the Latin American Development Bank. In *Security and Defence: Ethical and Legal Challenges in the Face of Current Conflicts*. Springer, 37-55. https://doi.org/10.1007/978-3-030-95939-5_3

Nayyar, R. (2019). *The Evolution of Business in The Cyber Age*. Apple Academic Press: Australia, 115-116. https://www.appleacademicpress.com/the-evolution-of-business-in-the-cyber-age-digital-transformation-threats-and-security/9781771888103

Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A., & Dehghanian, P. (2020). Electric power grid resilience to cyber adversaries: State of the art. *IEEE Access*, *8*, 87592-87608. https://doi.org/10.1109/ACCESS.2020.2993233

Njoga, A. (2022). Critical Information Infrastructure Cyberspace Situational

Awareness: Measure it, Manage it. *International Journal of Scientific and Research Publications*, *12*(4), 175-184. https://doi.org/10.29322/IJSRP.12.04.2022.p12425

Obeid, H., Hillani, F., Fakih, R., & Mozannar, K. (2020). Artificial Intelligence: Serving American Security and Chinese Ambitions. *Financial Markets, Institutions and Risks*, *4*(3), 42-52. https://doi.org/10.21272/fmir.4(3).42-52.2020

Patel, K., & Chudasama, D. (2021). National security threats in cyberspace. *National Journal of Cyber Security Law*, *4*(1), 12-20. https://doi.org/10.37591/NJCSL

Patriarca, R., Simone, F., & Di Gravio, G. (2022). Modelling cyber resilience in a water treatment and distribution system. *Reliability Engineering & System Safety*, *226*, 108653. https://doi.org/10.1016/j.ress.2022.108653

Pawar, S. C., Mente, R., & Chendage, B. D. (2021). Cyber crime, cyber space and effects of cyber crime. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *7*(1), 210-214. https://doi.org/10.32628/CSEIT217139

Pham, L. N. H. (2022). Exploring cyber-physical energy and power system: Concepts, applications, challenges, and simulation approaches. *Energies*, *16*(1), 42. https://doi.org/10.3390/en16010042

RAND. (2020). Adapted from The Future of Warfare in 2030

Rimawi, D. (2022). Green resilience of cyber-physical systems. 2022 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), 105-109. https://doi.org/10.1109/ISSREW55968.2022.00048

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369

Shull, A., & Hilt, K. (2021). Securing Cyberspace in an Age of Disruption: A Glimpse at the Rising Threatscape. *Canadian International Council*, *69*(27), 1-13. https://thecic.org/wp-content/uploads/2021/10/Shull-and-Hilt-Paper.pdf

Siboni, G., & Sivan-Sevilla, I. (2019). *Regulation in Cyberspace*. The Institute for National Security Studies Tel Aviv University, 25. https://doi.org/10.31219/osf.io/zeqpk

Soesanto. (2021). Mapping of Variables Forming Regional Competitiveness Index Using MICMAC Method. *Journal of Regional Development Policy*, *5*(1), 1-18.

Strelicz, A. (2021). Risks and threats in cyberspace-The key to success in digitization. Journal of Physics: Conference Series, IOP Publishing, *1935*(1), 012009. https://doi.org/10.1088/1742-6596/1935/1/012009

Valinejad, J., & Mili, L. (2022). Community resilience optimization subject to power flow constraints in cyber-physical-social systems. *IEEE Systems Journal*, *17*(2), 2904 - 2915. https://doi.org/10.1109/JSYST.2022.3210075

Vinichenko, M. V., Melnichuk, A. V., & Karácsony, P. (2020). Technologies of improving the university efficiency by using artificial intelligence: Motivational aspect. *Entrepreneurship and sustainability issues*, *7*(4), 2696. https://doi.org/10.9770/jesi.2020.7.4(9)

Weiss, M., & Biermann, F. (2023). Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*, *26*(3), 250-267. https://doi.org/10.1080/17487870.2021.1905530

Whyte, C. (2023). Learning to trust Skynet: Interfacing with artificial intelligence in cyberspace. *Contemporary Security Policy*, *44*(2), 308-344. https://doi.org/10.1080/13523260.2023.2180882