JRSSEM 2021, Vol. 04, No. 10, 1600 – 1612
E-ISSN: 2807 - 6311, P-ISSN: 2807 - 6494

The Role of National Computer Security Incident Response Team (Nat-CSIRT) in Threat Intelligence Sharing Through National Cyber Threat Intelligence System and Cyber Incident Database Center

Andi Yusuf[1], Basuki Erwin Setiyadi[2], Muhamad Al Fikri[3],Claudia Dwi Amanda[4]
[1] Sekolah Staf dan Pimpinan Tinggi Kepolisian Negara Republik Indonesia (SESPIMTI POLRI)
[24] Badan Siber dan Sandi Negara
[3] Pusat Sistem informasi dan Teknologi Keuangan, Kementerian Keuangan Republik Indonesia

*e-mail: andi.yusuf@bssn.go.id, basuki.erwin@bssn.go.id, claudia.amanda@bssn.go.id, al.fikri@kemenkeu.go.id
Correspondence:

Submitted: Mei 2025, *Revised*: Mei 2025, *Accepted*: Mei 2025

Abstrak. In 2021 and 2022, the stakeholder response rate to notifications sent by BSSN was only 9% of the total notifications delivered. In establishing the Nat-CSIRT, BSSN needs to implement breakthroughs to increase the number of responses and follow-ups to these notifications, thereby enhancing situational awareness and strengthening the national cybersecurity posture. Therefore, the role of Nat-CSIRT is crucial in optimizing threat intelligence sharing at the national level. The implementation of threat intelligence sharing has been mandated by various national and organizational policies, which underscores the urgency of executing the established policy directions. This paper focuses on strategies for the role of Nat-CSIRT in the implementation of national-level threat intelligence sharing by delving into the root causes of the suboptimal sharing using a problem tree analysis. Furthermore, the paper determines the strategic optimization of Nat-CSIRT's role through a SWOT analysis, resulting in a strategy that leverages strengths to seize opportunities (S-O Strategy). This strategy is carried out through a three-phase action plan—short-term, medium-term, and long-term—targeting the development of human resources, governance, and technology. In addition, the paper presents a model for a national-level threat intelligence sharing scheme for the National Cyber Threat Intelligence System and National Cyber Incident Database Center, enabling stakeholders to automatically implement standardized information exchange in a secure, swift, and accurate manner, while applying the Traffic Light Protocol. This approach is expected to lead to more effective cyber threat response and mitigation.

Keywords: Threat Intelligence Sharing, National Cyber Threat Intelligece System, National Cyber Incident Database Center, CSIRT, Traffic Light Protocol, Problem Tree, SWOT.

DOI :

INTRODUCTION

According to the *Indonesian Cybersecurity Landscape 2022* published by the National Cyber and Crypto Agency (BSSN), there were approximately 976.4 million anomalous traffic activities, with malware attacks being the most common type of anomaly. The government sector was identified as the most impacted by cyberattacks. Based on data collected by the Cybersecurity Operations Directorate of BSSN, the most frequent types of cyber incidents included web defacement and data breaches. Throughout 2024, a total of 1,288 indications of web defacement and 95 indications of data breach incidents were detected.

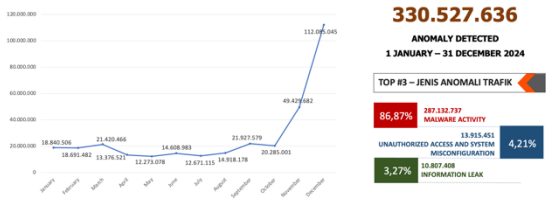

Figure 1. Traffic Anomaly Trend in 2024

Based on BSSN Regulation Number 6 of 2021 concerning the Organization and Work Procedures of the National Cyber and Crypto Agency (BSSN), the agency—through the Directorate of Cybersecurity Operations—carries out the management of national and government-sector cyber incident response, national cyber contact, and national cyber crisis management. In accordance with BSSN Regulation Number 10 of 2020 concerning the Cyber Incident Response Team, BSSN established the National CSIRT (Nat-CSIRT), whose main services include issuing cybersecurity alerts and managing cyber incidents, which are carried out by sending notifications of suspected cyber incidents and early warnings of cyber threats.

In 2024, BSSN, through Nat-CSIRT, sent 1,367 notifications of indicated cyber incidents to affected stakeholders. Out of the 1,367 notifications, only 741—or 58%—received a response from stakeholders. Therefore, in order to increase the number of responses and follow-ups to these notifications—thus enhancing situational awareness and strengthening the national cybersecurity posture—there is a need to optimize the role of Nat-CSIRT in national-level threat intelligence sharing.

Moreover, the mandate for threat intelligence sharing has been outlined in several national policies, including:

a. Presidential Regulation Number 18 of 2020 on the National Medium-Term Development Plan 2020–2024, Annex 3, which designates the development of an Information Sharing and Analysis Center (ISAC) as one of the priority programs for strengthening cyber resilience and security.
b. Presidential Regulation Number 82 of 2022, Article 18, which regulates the organization of cyber threat intelligence analysis and exchange forums in accordance with applicable laws and regulations.
c. Presidential Regulation Number 47 of 2023 on the National Cybersecurity Strategy, Article 9 letter (d), which emphasizes the strengthening of secure information exchange.
d. BSSN Regulation Number 5 of 2020 on the BSSN Strategic Plan for 2020–2024, specifically Policy Direction and Strategy Number 1 on Strengthening Cyber Infrastructure Security, which includes

the strategic target of establishing an Information Sharing and Analysis Center (ISAC).

This paper focuses on identifying the root causes of the issue and formulating strategies to optimize the role of Nat-CSIRT in implementing national-level threat intelligence sharing in order to enhance situational awareness and strengthen the national cybersecurity posture.

The objectives of implementing national-level Threat Intelligence Sharing are to accelerate cyber incident response and recovery times and to increase stakeholder participation in information sharing activities. For BSSN's internal organization, the benefits include enhancing stakeholder trust and credibility in Nat-CSIRT through the Directorate of Cybersecurity Operations and BSSN as a whole, as well as fostering security awareness within BSSN itself. On a broader scale, accelerating the implementation of threat intelligence sharing is expected to improve organizational situational awareness, optimize incident response with faster reaction and recovery times, support the prevention and mitigation of cyberattacks, and strengthen cybersecurity posture by reducing the number of incidents. An additional benefit is the preservation of organizational branding and the prevention of financial losses resulting from cyber incidents.

MATERIALS AND METHODS

This study employs a qualitative descriptive research method to analyze and formulate strategies for optimizing the role of Nat-CSIRT in implementing national-level threat intelligence sharing. Data were collected through a literature review of relevant regulations, official reports, and policy documents issued by BSSN and other national authorities. The analysis was conducted using a problem tree method to identify the root causes of suboptimal threat intelligence sharing, followed by a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis to develop strategic recommendations. The resulting strategy adopts a Strength-Opportunity (S-O) approach and is formulated into a three-phase action plan: short-term, medium-term, and long-term, focusing on improvements in human resources, governance, and technology.

RESULTS AND DISCUSSION

Current Condition

The issues and challenges faced in the implementation of national-level threat intelligence sharing are as follows:

a. Based on the Cybersecurity Landscape Reports for 2024 and 2025, there were 1.288 web defacement cases recorded in 2024, with the highest number occurring in January (249 cases). In 2025, a total of 342 web defacement cases were recorded, with the highest number occurring in February (93 cases).

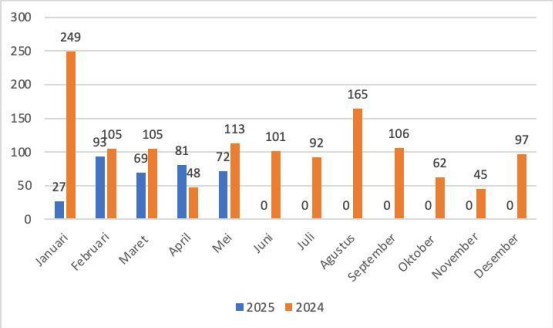

Figure 2. Web Defacement Incident Chart in 2024 and 2025

The data above indicates that web defacement attacks continue to occur frequently, particularly in the government sector. This is mainly due to the lack of follow-up from government stakeholders on early warning notifications of cyber threats related to web defacement sent by BSSN as a preventive measure.

b. Based on the *Cybersecurity Landscape Reports* for 2024 and 2025, there were 95 data breach incidents recorded in 2024, with 61 incidents affecting the government administration sector. In 2025, 207 data breach incidents were recorded, with 158 incidents affecting the government administration sector.

Table 1. Summary of Data Breach Incidents

Data Breach Incidents			
Sector	**2024**	**2025**	**Notes**
All Sectors	95	207	37% increase in cases
Government Sector	61	158	44% increase in cases

Table 1. Summary of Data Breach Incidents

The data in the summary table shows a significant increase in data breach incidents from 2024 to 2025. This rise is attributed to the lack of follow-up on early warning notifications of cyber threats related to data breaches sent by BSSN, especially by government stakeholders as a preventive effort.

c. Based on the *Cybersecurity Landscape Reports* for 2024 and mid 2025, in 2024 a total of 1,367 notifications were sent to stakeholders, but only 741 were followed up, while 513 notifications were not addressed. In mid 2025, 618 notifications were sent, with 407 receiving a response and 211 left unaddressed. The notification data shows that stakeholder response rates to notifications sent by BSSN remain low and stagnant at around 9% over the two-year period, indicating that threat intelligence sharing is still not optimal.

d. According to data from the Directorate of Cybersecurity Operations, in 2024 there were 741 notifications followed up by stakeholders with an average response time of 5 days, while in mid 2025, 513 notifications were followed up with an average response time of 3 days. This data indicates that the response times are still quite long, especially when considering the rapid spread of cyber threats. Below is the business process of threat intelligence sharing from internal sources.

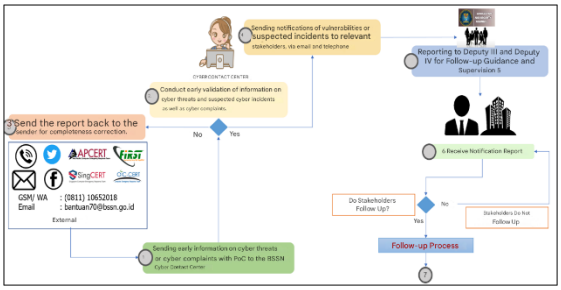

Figure 3. Business Process of Threat Intelligence Sharing from Internal Sources

The business process flow of threat intelligence sharing originates from internal information sources within the Directorate of Cybersecurity Operations, with the following steps:

1. The national cybersecurity monitoring team detects cyber threats and indications of cyber incidents through detection devices installed at the internet gateway and infrastructure owned by stakeholders. Early warnings of cyber threats and indications of incidents are then sent to the Cyber Contact Center via a task management application.
2. The Cyber Contact Center processes the early warning information and incident indications into a notification document. This notification document is sent to stakeholders via email.
3. The Cyber Contact Center forwards the notification document and/or a summary of the notification document through official letters and email to the sector deputies for follow-up guidance and supervision of the related stakeholders.
4. Stakeholders receive the notification documents sent by the Cyber Contact Center via email.
5. Stakeholders either follow up or do not follow up on the notification documents provided by the Cyber Contact Center via email and instant messaging applications.

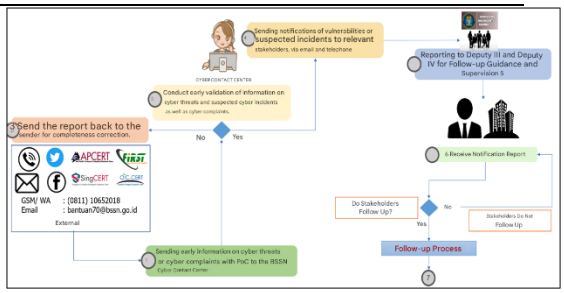

Figure 4. Business Process of Cyber Threat Intelligence Sharing from External Sources

The business process flow of threat intelligence sharing with information originating from external sources, such as other countries' CSIRTs and cyber complaints, consists of the following steps:

1. External parties send early warning information on cyber threats or cyber complaints to the Cyber Contact Center in the form of cyber threat intelligence.
2. The Cyber Contact Center receives and validates the early warning information or cyber complaints from external parties.
3. The Cyber Contact Center either accepts or rejects the early warning information or cyber complaints from external parties after validation.
4. The Cyber Contact Center processes the early warning information and indications of cyber incidents into a notification document, which is then sent to stakeholders via email.
5. The Cyber Contact Center forwards the notification document and/or a summary of the notification document through official letters and emails to the sector deputies

for follow-up guidance and supervision of the related stakeholders.

6. Stakeholders receive the notification documents sent by the Cyber Contact Center via email.
7. Stakeholders either follow up or do not follow up on the notification documents provided by the Cyber Contact Center via email and instant messaging applications.

The smooth operation of the above business process heavily depends on the use of email. According to the 2022 Digital Literacy Status Survey in Indonesia, published by the Ministry of Communication and Information Technology and Kata Data, only 11% of Indonesians frequently use email for work, while 48% never use email. This shows that using email for sending notifications is ineffective. Furthermore, the process of sending and following up notifications still relies on different applications, causing the business process to be non-integrated.

To explore more deeply the root causes of the suboptimal national-level threat intelligence sharing, a problem tree method was employed. This method illustrates cause-and-effect relationships, where the factors causing the problem can be broken down into several levels: main causes, primary causes, and specific causes.

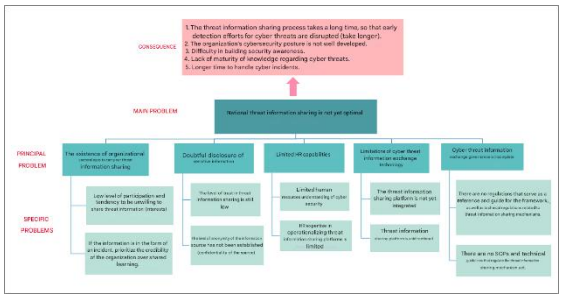

Figure 5. Analysis Process Using Problem Tree

From the analysis above, several key issues need to be addressed: organizational sectoral ego hindering threat intelligence sharing, hesitation to disclose sensitive information, limited human resource capabilities, insufficient threat intelligence sharing technology, and incomplete governance of threat intelligence sharing. These problems converge into an idea that must be implemented to resolve all the issues.

Based on this analysis, it can be concluded that the recommendation to solve these problems is to develop a strategy to optimize the role of Nat-CSIRT in conducting national-level threat intelligence sharing. The optimization aspect not only emphasizes effectiveness and efficiency but also aims to transform and change the paradigm of all entities involved in threat intelligence sharing comprehensively. This would accelerate detection, improve organizational cybersecurity posture, facilitate building security awareness, achieve good maturity regarding cyber threat knowledge, and speed up cyber incident handling time.

Desired Ideal Conditions

Based on the problem identification results within the organization, a solution has been designed to create an ideal condition after the implementation of national-level threat intelligence sharing runs optimally, as follows:

a. A decrease in the number of government sector web defacement incidents compared to the previous year (<885 cases).
b. A decrease in the number of suspected

data leakage incidents in the government sector compared to the previous year (<120 cases).

c. An increase in the frequency of follow-up actions on cyber threat notifications by 100% from the previous year (to 17.6%).
d. A faster response time for cyber threat notifications by stakeholders, ideally within 1 calendar day (including weekends and public holidays).

SWOT Analysis

To achieve these ideal conditions, a comprehensive strategy involving all stakeholders is required. Therefore, a broader strategy is needed to accurately and carefully map the environment. After conducting the problem mapping using the problem tree method, a SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats) approach was carried out as follows:

Table 2. SWOT Analysis Diagram

Internal Factors			
Strengths		**Weaknesses**	
1	BSSN carries out government duties in cybersecurity, performing identification, detection, protection, response, recovery, and monitoring of national cybersecurity incidents, as well as managing national cyber crisis.	1	Current threat intelligence sharing processes are still one-way and not integrated.
2	BSSN can hold analysis forums and threat intelligence sharing as regulated by law, involving relevant parties.	2	Communication regarding threat intelligence sharing programs among sector stakeholders and cybersecurity operational holders is not yet optimal.
3	Establishment of National Cybersecurity Operation Center (NSOC), Security Operation Center (SOC), and 121 Cyber Security Incident Response Teams (CSIRT) as major projects to strengthen political-security stability and public service transformation.	3	Automated and integrated threat intelligence sharing platform implementation is still under development.
4	Cyber Threat Intelligence Platform has been developed for collecting and analyzing	4	Implementation of policies/regulations on threat intelligence sharing is not

	cyber threat data.		yet optimal.
External Factors			
Opportunities		**Threats**	
1	National resources including academia, business/industry, government, communities, and practitioners can collaboratively engage in the national threat intelligence sharing strategy.	1	Cyber threat and crime trends constantly change rapidly, along with uneven stakeholder capabilities in early threat identification and detection.
2	Development of an international CSIRT ecosystem as a source of cyber threat intelligence.	2	Geopolitical interests of various countries in Indonesia and the region.
3	The establishment of CSIRTs as major projects supports the implementation of threat intelligence sharing using well-implemented and secure technology/platforms.	3	Lack of situational awareness among end users/public regarding the importance of data security (personal and organizational).
4	Implementation of threat intelligence sharing in other countries as indicators of improved cybersecurity capacity that can serve as benchmarks for Indonesia.	4	Persistent high sectoral ego remains a challenge in applying threat intelligence sharing.

From the internal and external factors, 16 components were identified, with 4 components each under strengths, weaknesses, opportunities, and threats. Each component was compared and assessed for urgency to determine priority values. Then, each component's importance to the strategy for optimizing Nat-CSIRT's role in national threat intelligence sharing was rated on a scale of 0–5, along with relevance weighting on the same scale. The rating values were on a scale of 1–10.

The results of urgency weight evaluation were then used in the next stage to obtain final scores for quadrant determination based on the pre-defined factors. The evaluation results are:

- Strengths factor: 5.48
- Weaknesses factor: 2.86
- Opportunities factor: 5.18
- Threats factor: 3.25

Next, the X-axis and Y-axis point calculations are:

X-axis point = Opportunities value – Threats value
= 5.18 – 3.25
= 1.93

Y-axis point = Strengths value – Weaknesses value
= 5.48 – 2.86

= 2.82

The results show that the strategic approach to optimize Nat-CSIRT's role in national threat intelligence sharing lies in Quadrant I at the coordinate (1.93; 2.82) as follows:

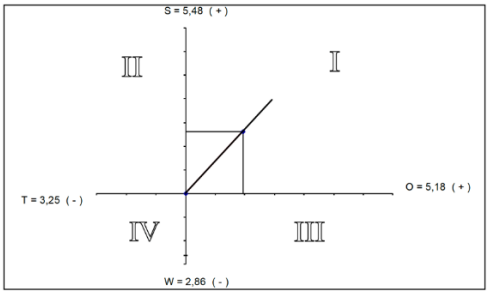

Figure 6. SWOT Analysis Quadrant Results

Based on the calculation from the components S = Strengths, W = Weaknesses, O = Opportunities, and T = Threats, the strategy that BSSN can use falls into Quadrant I (S-O), which applies the approach of "optimizing strengths by leveraging opportunities." The strategies that Nat-CSIRT can adopt are:

a. Organizing analysis forums and threat intelligence sharing by coordinating with established sectoral or organizational CSIRTs as well as coordinating with international CSIRTs.
b. Coordinating threat intelligence sharing as Nat-CSIRT by implementing technology or a threat intelligence sharing platform properly and securely, involving all national resources comprehensively (Human Resources, Governance, and Technology).
c. Establish a Cyber Incident Database Center as a living infrastructure that ensures the availability of accurate and comprehensive threat intelligence information based on stakeholder contributions.

Cyber Threat Intelligence Sharing Scheme

The following is the scheme of the threat intelligence sharing.

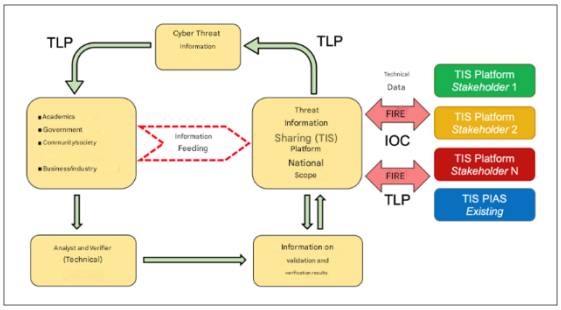

Figure 7. Threat Intelligence Sharing Scheme

The threat intelligence sharing scheme is a form of collaboration among different stakeholders aimed at enhancing mitigation and response capabilities against occurring cybersecurity threats. The platform operated by Nat-CSIRT as the central hub enables analysts to monitor and process standardized information such as Indicators of Compromise (IoC), Tactics, Techniques, and Procedures (TTP), and cybersecurity reports shared by participating stakeholders.

Each participating stakeholder also operates their own threat intelligence sharing platform to monitor cybersecurity threats within their networks and exchange this information with the central platform operated by Nat-CSIRT. These stakeholders can come from various sectors, such as academia, government, community, and business/industry.

Connections between the threat intelligence sharing platforms within this network use the Traffic Light Protocol (TLP) to regulate the security levels of shared

information. TLP categorizes cybersecurity threat intelligence into several levels such as Clear, Green, Amber, Amber+Strict, and Red, with each category representing different levels of information sensitivity.

With the existence of the threat intelligence sharing scheme, stakeholders can automatically implement standardized information exchange quickly and accurately, enabling more effective mitigation and response to cybersecurity threats. Furthermore, with TLP, stakeholders can ensure that the information they share is only received by authorized parties and not misused by unauthorized ones.

National Cyber Threat Intelligence System and National Cyber Incident Database Center

Cyber Threat Intelligence Sharing can achieve its full potential with two enablers. First, is a Cyber Threat Intelligece System (CTIS) which is a platform used to maintain the Cyber Threat Intelligence Sharing Scheme. And the second, is a Cyber Incident Database Center (CIDBC). CTIS serves as a centralized platform for cyber threat intelligence where cyber threat intelligence data can be shared, while CIDBC functions as a repository for real-world cyber incidents. Together, these systems provide essential data to support the detection, analysis, and prosecution of cybercrimes both domestically and internationally.

Figure 8. Structure of Local and International Cyber Threat Intelligence Data

Figure 9 illustrates the structure of local and international cyber threat intelligence data, which focuses on cyber threat actors, both local and international. The data collected includes identifiers such as names, aliases, or account names; IP addresses or domains used; malware signatures (hashes); and TTPs (tactics, techniques, and procedures) employed in cyberattacks. CTIS enables the systematic collection and categorization of this information, allowing security teams to proactively monitor emerging threats and take preventive action.

Figure 9. Structure of Local and International Cyber Threat Intelligence Data

Figure 10 presents the structure of cyber incident data in CIDBC, which documents actual cyber incidents such as ransomware attacks and data breaches. Each incident record includes a detailed timeline, indicators of compromise (IOCs), and the TTPs used by the attackers. PPDIS not only logs incidents occurring in Indonesia, but also incorporates lessons learned from incidents in other countries. This broader perspective enriches national understanding and improves the ability to respond effectively to a wide range of cyber threats.

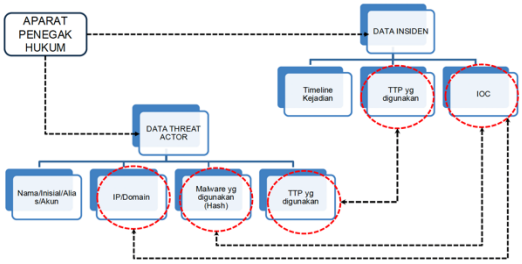

Figure 10. Correlation Between Cyber Threat Intelligence Data and Cyber Incident Data stored in CIDBC

Finally figure 10 explains the correlation between cyber threat intelligence data and cyber incident data stored in CIDBC, particularly in the context of law enforcement. Investigators can leverage data from both platforms to establish links between cyber incidents (recorded in CIDBC) and potential threat actors (tracked in CTIS). For example, IOCs from an incident may match IP addresses or malware hashes previously identified in CTIS. Similarly, recurring TTPs may indicate repeated activity by the same actor or group. This integrated approach enables faster and more accurate investigations, supported by robust digital evidence.

Together, CTIS and CIDBC form a complementary architecture for early threat detection, comprehensive threat mapping, and coordinated incident response. The synergy between tactical data (from incidents) and strategic intelligence (on threat actors) provides a strong foundation for building national cyber threat intelligence capabilities. It also enhances the effectiveness of law enforcement in combating digital crime, reinforcing Indonesia's resilience in an increasingly complex cyber threat landscape.

Roadmap/Action Plan

To realize breakthroughs and innovations to optimize the role of Nat-CSIRT in national-level threat intelligence sharing through the National CTIS and National CIDBC, the implementation is divided into three stages: 1) Short Term, 2) Medium Term, and 3) Long Term. The achievements will be carried out through the following steps:

1. Short Term
   a. Strengthening HR competencies through Technical Guidance & Workshops related to threat intelligence sharing (internal and external);
   b. Drafting BSSN Head Regulations, Technical Guidelines, Standard Operating Procedures, and Non-Disclosure Agreements;
   c. Conducting formal (FGD) and informal meetings with related stakeholders;
   d. Building and maintaining a website-based (open source) CTIS;
   e. Building the CIDBC and integrates it to the CTIS.
   f. Conducting trials of the CTIS;
   g. Installing and utilizing the threat intelligence sharing platform at 7 stakeholders.
2. Medium Term
   a. Strengthening competencies through seminars and improving skills via benchmarking & technical discussions (domestic and international);
   b. Drafting an action plan document for the information exchange program

as a derivative of Presidential Regulation Number 47 of 2023 concerning the National Cybersecurity Strategy and Cyber Crisis Management;

c. Developing a mobile app-based CTIS;
d. Implementing comprehensive security;
e. Installing and utilizing the threat intelligence sharing platform on cybersecurity threat intelligence at 25 stakeholders.

3. Long Term
   a. Strengthening HR competencies through national and international certification, including monitoring & evaluation of HR competency development programs;
   b. Drafting regulations and frameworks to serve as references and guidelines for implementing national-level cyber threat intelligence sharing;
   c. Monitoring & evaluating the implementation of technical policies related to threat intelligence sharing;
   d. Integrating CTIS based on hardware and software;
   e. Conducting phased and continuous testing of the CTIS;
   f. Utilizing the CTIS and its governance in national drill test activities (National Cyber Crisis Management);
   g. Installing and utilizing the CTIS at 50 stakeholders.

CONCLUSIONS

To build awareness, preparedness, and enhance Indonesia's cybersecurity posture, a comprehensive, broad, and well-coordinated threat intelligence sharing strategy—led by the Nat-CSIRT—is essential. By leveraging internal strengths and external opportunities, global cybersecurity threats and challenges can be addressed more effectively. This effort is further supported by the involvement of all layers of cybersecurity resources across various sectors, as cybersecurity threats and challenges can only be tackled through collaborative functions and synergy, which are the core essence of threat intelligence sharing. The strategy to optimize the role of Nat-CSIRT in threat intelligence sharing through the CTIS and CIDBC serves as a solution to address urgent needs, offering direct and actionable benefits for all stakeholders.

REFERENCES

1) *Peraturan Presiden Republik Indonesia Nomor 18 Tahun 2020 Tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024*. Lembaran Negara Republik Indonesia Tahun 2020, Nomor 10. Sekretariat Kabinet. Jakarta. 2020.
2) *Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital*. Lembaran Negara Republik Indonesia Tahun 2022, Nomor 129. Kementerian Sekretariat Negara. Jakarta. 2022.
3) *Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasiona dan Magagemen Krisis Sibel*. Lembaran Negara Republik Indonesia Tahun 2023, Nomor 99. Kementerian

Sekretariat Negara. Jakarta. 2023.

4) *Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2020 tentang Rencana Strategis BSSN Tahun 2020-2024*. Berita Negara Republik Indonesia Tahun 2020 Nomor 843. Direktur Jenderal Peraturan Perundang-Undangan, Kementerian Hukum Dan Hak Asasi Manusia Republik Indonesia. Jakarta. 2020.
5) *Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber*. Berita Negara Republik Indonesia Tahun 2020 Nomor 1488. Direktur Jenderal Peraturan Perundang-Undangan, Kementerian Hukum Dan Hak Asasi Manusia Republik Indonesia. Jakarta. 2020.
6) *Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara*. Berita Negara Republik Indonesia Tahun 2021 Nomor 803. Direktur Jenderal Peraturan Perundang-Undangan, Kementerian Hukum Dan Hak Asasi Manusia Republik Indonesia. Jakarta. 2021.
7) BSSN, *Laporan Tahunan Monitoring Keamanan Siber*, Jakarta. 2021.
8) BSSN, *Dokumen Lanskap Keamanan Siber Indonesia 2022*, Jakarta. 2022.
9) Kementerian Komunikasi dan Informatika, Kata Data. *Status Literasi Digital di Indonesia Tahun 2022*, Jakarta. 2022.
10) Vesely, A. *Problem Tree: A Problem Structuring Heuristic*. Central European Journal of Public Policy. 2008.
11) Sarsby. A., *SWOT Analysis: A Guide to SWOT for Business Studies Students*, Leadership Library. 2016.
12) L. Nweke and S. Wolthusen, *Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection*. 2020.
13) CISA, *Traffic Light Protocol 2.0 User Guide*. 2022.