ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 15 (2025) No. 2, pp. 225-244
DOI:10.33168/JSMS.2025.0214

Enhancing Cyber Crisis Preparedness in Indonesia: A RACI-based Approach to Formulating a National Cyber Crisis Task Force

Prabaswari [1], Yusuf Ali [1], Rudy A.G. Gultom [1], Luhut Simbolon [1], Ahmad Faridi [2]

[1] Postgraduate Programme, Republic of Indonesia Defence University

[2] Graduate Programme, Johns Hopkins University

Abstract. The escalating frequency and severity of cyberattacks in Indonesia pose significant challenges to national security, underscoring the necessity for a cohesive national approach to cyber crises. To address these contingencies, this study aims to formulate a National Cyber Crisis Task Force (NCCTF) using the Responsibility, Assignment, Consultation, and Informed (RACI) matrix approach. By conducting interviews with key stakeholders and reviewing exemplary practices, the study identifies 15 stakeholders within the NCCTF, categorized into technical and strategic levels. The RACI analysis delineates the specific roles and responsibilities of each stakeholder, with the President holding ultimate authority and the Head of the National Cyber and Crypto Agency (BSSN) chairing the task force. Additionally, the research proposes an organizational framework and operational procedures for the NCCTF, aligned with legislative prerequisites. The findings provide a framework for establishing a national cyber crisis task force in Indonesia, which can serve as a model for other countries facing similar challenges. Future research directions include exploring and categorizing cyber crises to further strengthen the task force's effectiveness.

Keywords: Cyber crisis, Crisis management, Incident Response, RACI Matrix Analysis, Task Force.

1. Introduction

Cyberthreats represent a concrete manifestation of the challenges confronting Indonesia and the global community in the era of the Fourth Industrial Revolution and the Internet of Things (IoT). This period is characterized by the extensive integration of Internet connectivity into virtually all facets of human activity (Yerina et al., 2021). A cyber crisis occurs when critical infrastructure is damaged or exploited by an extraordinarily large-scale cyberattack, leading to severe damage, disruption of public activities, reputational harm, economic losses, and threats to national security (Prevezianou, 2021; Skierka, 2023). Ordinary incident management mechanisms cannot handle such situations, necessitating rapid institutional adaptation and coordination (Prevezianou, 2021). Cyber warfare has emerged as a significant social phenomenon within international relations, presenting formidable challenges to all nations in their efforts to construct global stability (Xu & Lu, 2021). In light of the escalating severity of cyber threats, numerous international platforms, encompassing both multilateral and regional forums, have prioritized cyber issues as a critical subject for discussion, necessitating consensus (Prabaswari et al., 2022). This indicates that the international community continues to make significant efforts to mitigate the catastrophic effects of disasters, particularly those caused by technology (Halizahari et al., 2023).

In recent years, the urgency of cybersecurity has evolved from an IT security concern to a national security issue for modern nations, encompassing ongoing diplomatic, financial, and political activities (Backman, 2021). Significant cyber incidents have unfolded throughout history, precipitating crises that have impacted various sectors, organizations, and even entire nations (Mott et al., 2023). Noteworthy examples include the WannaCry ransomware attack in 2017, which targeted thousands of organizations globally (Bahuguna et al., 2019), and the NotPetya cyberattack in the same year, initially aimed at Ukrainian organizations but which rapidly proliferated worldwide (Sufi, 2023). Additional incidents, such as the vulnerabilities discovered in Microsoft Exchange Server in 2021, further illustrate the pervasiveness of cyber threats (Shaked et al., 2023). Several countries have endured notable cyber crises, including the United States with the Equifax data breach and the SolarWinds supply chain attack, Iran with Stuxnet, and Ukraine, South Korea, and Estonia with Distributed Denial of Service (DDoS) attacks, among others (Lehto & Limnéll, 2021). Given this backdrop, the imperative for effective cyber crisis management becomes evident, underscoring the necessity to mitigate the repercussions of such incidents and safeguard critical infrastructure (Ezioni & Siboni, 2021).

Cyberattacks in Indonesia have escalated significantly, especially after the COVID-19 outbreak, which markedly altered global internet usage patterns (Alawida et al., 2022; Santoso et al., 2023). According to data from the National Cyber Security Operations Center (Pusopkamsinas) of the National Cyber and Crypto Agency (BSSN), Indonesia witnessed approximately 1.28 billion traffic anomalies and cyberattacks between January 2022 and August 2023. From 2019 to 2023, Indonesia has been subjected to various cyber incidents. The most frequent incidents were data breaches affecting the Ministry of Education and Culture, Ministry of Health, Vote Commission, National Police, Bank Syariah Indonesia, National Worker Insurance, and National Health Insurance. In 2022, Bjorka claimed to have obtained 1.3 billion registration records of SIM cards from the Ministry of Communications and Information Technology, along with personal information about government officials, secret letters from the President and the National Intelligence Agency, as well as personal data of public figures. Bjorka also admitted to being the mastermind behind a series of data leaks since 2019 (Sutikno & Stiawan, 2022). In 2023, Bank Syariah Indonesia (BSI) experienced an outage from May 8th to 11th caused by Lockbit ransomware, rendering its banking services inaccessible (Uly Yohana Artha; Sukmana Yoga, 2023). This outage affected various channels, including direct services at branch offices, automated teller machines (ATMs), and mobile service applications. As a result, this incident caused a decline in stocks due to a domino effect that led to customer panic (Solikhawati & Samsuri, 2023).

Notably, these significant cyberattacks have recently captured public attention, emphasizing the critical need for robust cybersecurity measures and infrastructure to mitigate such threats (Sutikno &

Stiawan, 2022). Moreover, this series of incidents has had substantial economic and reputational impacts, leading to a decline in public trust in the government and companies. Such major cyber incidents can even cause public unrest, threatening national security (Alawida et al., 2022). In response to these attacks, the government established a Temporary Special Data Security Team comprising the National Cyber and Encryption Agency (BSSN), the National Intelligence Agency (BIN), the Indonesian National Police (POLRI), and the Ministry of Communication and Information (Kemenkominfo). However, the roles and responsibilities within these teams have not been systematically defined, resulting in a situation where each institution shifts responsibility to others, thereby causing ineffectiveness in incident handling (Martha Warta Silaban, 2022). Consequently, the establishment of a dedicated national cyber crisis management team with a clear structure and defined functions has become an urgent necessity.

In July 2023, the Indonesian government passed Presidential Regulation Number 47 of 2023 regarding the National Cyber Security Strategy and Cyber Crisis Management to address increasingly significant cyber incidents (*Presidential Bill No. 47/2023 : National Cyber Security Strategy and Cyber Crisis Management*, 2023). Despite the enactment of Presidential Regulation Number 47 of 2023, there remains a lack of clarity regarding the composition and responsibilities of the cyber crisis task force. When an incident involves two or more functions, decision-making requires the consideration of multiple parties. Furthermore, effective Cyber Crisis Management requires collaboration among relevant stakeholders (Mott et al., 2023). Currently, BSSN is the sole actor responsible for maintaining national cyber security and handling all national-scale cyber incidents.

Therefore, conducting this research to proactively address cyber crises becomes imperative through the establishment of a national cyber crisis task force involving all relevant stakeholders. This study aims to formulate a task force to address cyber crises, identify the necessary and relevant parties, and delineate their respective roles and responsibilities. To achieve this, the Responsibility, Assignment, Consultation, and Informed (RACI) method will be employed. The RACI method is most often used in the context of IT Governance (Matshaba & Nxozi, 2023) and can facilitate a clear delineation of roles and responsibilities among involved parties (Fitriani et al., 2023). By utilizing the RACI framework, this study seeks to elucidate the stakeholders involved and their interactions in forming a task force to effectively mitigate cyber crises in Indonesia.

Prior research often lacks comprehensive frameworks for establishing national-level cyber crisis task forces. For example, research conducted by Boeke explains public and private partnerships in handling cyber crises in the European Union but does not detail their roles and responsibilities (Boeke, 2018). Mikušová and Horváthová (2019) mentioned that one of the basic elements in anticipating crises is establishing a crisis management team, but this is not specifically designed for cyber crisis situations. Another study conducted by Lai and Cai (2023) highlights the urgent need for crisis management teams during the COVID-19 pandemic. Most research emphasizes the importance of forming a crisis management team; however, it has not specifically addressed the crisis management team, particularly in the context of Indonesia. By elucidating the roles and interactions of stakeholders within such a task force, our study aims to fill this gap and provide valuable insights for policymakers, practitioners, and researchers in the field of cybersecurity and crisis management. These identified roles and responsibilities will be benchmarked against established standards such as the NIST Special Publication 800-61 Rev.2 and ISO 27305-2:2023, which provide comprehensive Computer Security Incident Handling guidelines. This comparison aims to ensure that the task force's operations align with international best practices and standards, enhancing the efficacy of cyber crisis management and recovery efforts. Ultimately, our research contributes to a more robust understanding of effective strategies for mitigating cyber crises and safeguarding national security in an increasingly digitalized world.

2. Literature Review

2.1.Cyber Crisis Management

The European Union Agency for Cybersecurity (ENISA) examines various definitions of cyber crisis. According to the European Union, a cyber crisis is an anomalous and chaotic circumstance that threatens an organization's strategic goals, credibility, or existence, making it an incident that strikes at the organization's core (Panagiotis Trimintzios; Razvan Gavrila; Makrodimitris Georgios, 2014). A cyber crisis represents a major threat to a system's core structure, principles, and norms in cyberspace, necessitating critical decisions under significant time pressure and uncertainty (Ezioni & Siboni, 2021). The Netherlands defines a cyber crisis as an IT-related problem affecting critical infrastructure that a standard crisis management organization cannot manage. In Czechoslovakia, a "cyber crisis" can be declared if the security of information systems is in jeopardy and could threaten national interests (Sergei Boeke, 2018).

Cyber crisis refers to crises in general but within the cyberspace context. According to the USA Patriot Act, critical infrastructure includes systems and assets, both physical and virtual, that, if damaged, would affect national security, the economy, public safety, health, or a combination of these factors (Gultom et al., 2021). Based on the definitions provided, a cyber crisis is a cyber incident targeting national critical infrastructure that paralyzes essential business processes, threatens national interests, and creates uncertainty, necessitating urgent technical and strategic decisions. A cyber crisis begins with a cyber incident that escalates to an unusual scale and has a harmful impact on organizations and even countries (Dykstra & Orr, 2017). These crises can result in significant financial losses, irreparable damage to reputations, and disruptions to essential services. They may also involve compromised data, prolonged system outages, or threats to national security (Knight & Nurse, 2020).

Advancements in crisis management have underscored the importance of effectively managing crises, emphasizing the significance of preparation through the implementation of a crisis management plan (Ezioni & Siboni, 2021). Cyber Crisis Management is a logical extension of Major Incident Management (Mott et al., 2023). When a significant event occurs, there is a clear flow of communication between Crisis Management and Incident Management, both upstream and downstream (Chandrasekar et al., 2021). The main goal of a Crisis Management Plan is to strengthen operational resilience and delineate the necessary involvement of national-level leadership during the event. A crisis management strategy prioritizes decision-making and communication concerning associated risks (Danet & Weber, 2020). Based on expert interviews and focus group discussions, it was determined that major incidents are prone to evolve into cyber crises when they result in substantial harm, economic repercussions, casualties, or a tarnished reputation for the government or nation, particularly if they impact critical public infrastructure. For example, a ransomware containment strategy may require temporarily or permanently deactivating vital infrastructure, which could result in revenue losses, diminished customer confidence, or disruptions in business services. The implementation of such a strategy is a strategic choice that the cyber crisis task force should carefully consider.

2.2.Cyber Crisis Team

Cyber crises primarily originate from technological sources, yet their impact extends across society as a whole. Therefore, it is imperative that companies are adequately prepared to effectively address such crises. The establishment of a proficient team of experts, tasked with policy planning, strategic thinking, oversight, and readiness for impending crises, is crucial to ensuring a heightened state of preparedness (Pearson & Mitroff, 1993). By leveraging such a team, prioritization should be given to the implementation of a crisis preparedness plan and conducting exercises that simulate real-world scenarios. To effectively prepare for a crisis, the crisis management team, in collaboration with employees and through active engagement in simulations of actual situations, must comprehensively assess the risks the organization may encounter throughout its current and upcoming life cycle (Deloitte, 2016).

When a specialized team convenes with executives and stakeholders across all departments within the company, each department has the opportunity to identify risks within its respective domain, thereby mitigating the likelihood of potential incidents (Frykmer & Becker, 2023). Key personnel, who will assume critical roles as part of the cyber crisis team, must enhance their analytical abilities to (Ezioni & Siboni, 2021) :

a. Better grasp, synthesize, and capitalize on intricate scenarios that may emerge;
b. Identify and formulate intelligence needs using methodologies such as threat modeling;
c. Acquire proficiency in tactical, operational, and strategic-level threat intelligence;
d. Generate threat intelligence to detect, respond to, and counter focused and targeted threats;
e. Familiarize themselves with diverse threat sources to gather adversary data and effectively utilize it to safeguard against competitors or malicious actors;
f. Implement structured analytical methodologies applicable across various security roles through cross-organizational collaboration.

In addition to internal organizational members, on a national scale, the cyber crisis team also comprises parties from external organizations, particularly related stakeholders from the government, private sector, and experts. As an illustration, the Government of the Republic of Croatia has established the "Operational and Technical Cyber Security Coordination Group," tasked with:

a. Monitoring the security status of national cyberspace to detect potential threats leading to cyber crises.
b. Issuing reports concerning the state of cybersecurity.
c. Proposing action plans for addressing cyber crises.
d. Undertaking other responsibilities outlined in the provided programs and activity plans.

Representatives within this interdepartmental entity, the Operational and Technical Cyber Security Coordination Group, collaborate to ensure mutual access to operational information within their respective domains, facilitating coordinated responses during cyber crises (Control et al., 2018). Based on Presidential Regulation Number 47 of 2023 in Indonesia, this joint team is also known as a cyber crisis task force.

The primary responsibility of the Cyber Crisis Task Force has transitioned to managing the crisis stage. This encompasses various tasks, including conducting cyber crisis management by identifying and analyzing the extent of electronic systems affected by cyber crises, isolating impacted systems, gathering and preserving evidence from affected systems, investigating and eliminating the root causes of cyber crises, fortifying unaffected systems, and collaborating with stakeholders to establish protocols for cyber crisis communication and information flow control to the public. Additionally, the task force undertakes efforts for cyber crisis recovery by restoring data or utilizing backup and alternative resources. Subsequently, it tests vital and supporting functions to ensure recovery objectives are met within specified timeframes, taking into account the amount of successfully recovered data and the functionality of restored vital and supporting functions. In the concluding phase, the task force submits a report to the President for evaluation to determine whether the crisis situation can be resolved or not (*Presidential Bill No. 47/2023 : National Cyber Security Strategy and Cyber Crisis Management*, 2023).

2.3.RACI Method

The RACI matrix is one of the commonly used tools in project management (Dwi et al., 2021). A widely utilized approach in defining stakeholder roles involves the application of interest and influence to categorize stakeholders through a "responsibility assignment matrix." This model assigns authority, thereby illuminating power dynamics by delineating roles within a task, project, or management endeavor. It was selected for this study due to its suitability in broadly categorizing the varying levels of significance in decision-making processes. This aids in maintaining order, transparency, and accountability in project implementation. Moreover, it is intuitive, easily comprehensible, and readily understood by individuals unacquainted with the RACI model. A RACI chart comprises four roles

(Hirmer et al., 2021):

- **Responsible:** Who is responsible for performing or completing the task?
- **Accountable:** Who owns, authorizes, and makes the ultimate decision for the task?
- **Consulted:** Who can provide additional information or input during the task's execution?
- **Informed:** Who needs to be updated on the progress of the task?

The application of the RACI framework within research contexts serves as a mechanism to explicitly define the areas of responsibility associated with each designated task, thereby enhancing production time efficiency (Hasle, 2023), supporting managerial decisions concerning energy project operations in Sierra Leone (Hirmer et al., 2021), improving the cyber incident handling procedure within the Business Process Model and Notation (BPMN) model (Aguilar et al., 2023), and facilitating communication flow among diverse stakeholders (Trani et al., 2022).

RACI is also frequently employed in the realm of IT governance, such as in delineating the tasks and accountability of managers in the development of interoperable health information systems (Matshaba & Nxozi, 2023), as well as in implementing the digital transformation roadmap for the Punjab Government (Sarwar et al., 2023). Furthermore, the RACI framework plays a pivotal role in identifying stakeholders within the Health Emergency and Disaster Management System, thereby enabling clear delineation of roles and responsibilities among involved parties (Fitriani et al., 2023). Despite previous studies exploring the roles and responsibilities of cyber crisis teams, there exists limited research on the application of the RACI matrix in this context, particularly within the Indonesian setting.

3. Methodology

This study employs primary and secondary sources, including observational data, interviews, and literature reviews, to conduct a qualitative analysis. While some qualitative studies may forgo the explicit use of a theoretical framework, they provide a descriptive exploration of the central phenomenon under investigation (John W. Creswell; J. David Creswell, 2022). Primary data were gathered via semi-structured interviews with five respondents from the BSSN, the Ministry of Defence (MoD), and IT security experts, using purposive sampling methods. This technique involves deliberately selecting respondents who possess the specific expertise for the research objectives. In this case, we targeted five individuals working in key positions and known for their expertise in cybersecurity and crisis management. All of them have worked in their field for more than 15 years, often speak at seminars and conferences related to defense and cybersecurity, and have held middle to top-manager positions. The interview data were analyzed using thematic analysis to identify key roles and responsibilities for the task force. Subsequently, in alignment with the study's objectives, the Responsibility, Assignment, Consult, and Informed (RACI) framework were utilized to develop an assignment matrix for every stakeholder in the Task Force. Using the conceptual model depicted in Figure 1, it is feasible to understand the interrelation of each data point within this research process, thereby facilitating the construction of the RACI Matrix.

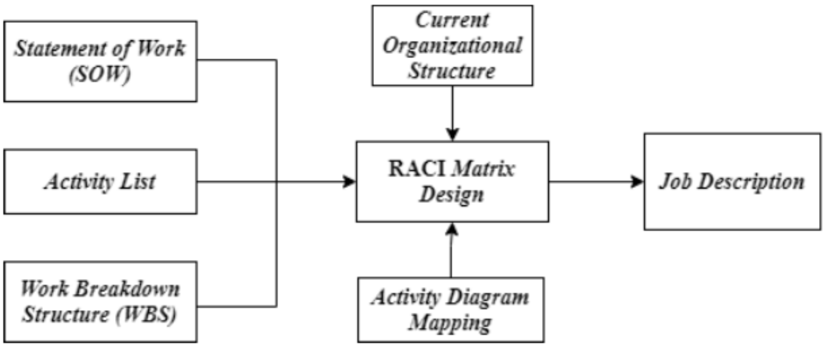

Fig 1. Research's Conceptual Model (Dwi et al., 2021)

During the preliminary phase, data are collected and analyzed to identify the various responsibilities of the task force. This process is facilitated through the utilization of a Work Breakdown Structure (WBS) to delineate distinct tasks and responsibilities, which serves as a pivotal guide for defining the business process. The roles and responsibilities of each stakeholder are pinpointed through the assignment matrix, which is derived from the results obtained during the analysis of the underlying business processes. The gathered data include a detailed record of all involved parties, the organizational hierarchy, the work breakdown structure, and the schedule of activities. The data processing phase commences with a thorough review of business process documentation for each designated job position within the task force. Subsequently, an assignment matrix is formulated using the RACI Matrix Method, ensuring a systematic approach to defining and allocating responsibilities.

Best practice references were examined to ascertain the prerequisites for roles, responsibilities, and participation within the task force, primarily focusing on the NIST Special Publication 800-61 rev. Two and ISO 27305-2:2016. These two standards emerge as the primary benchmarks frequently employed and serve as foundational guidelines in managing cybersecurity incidents (Tøndel et al., 2014). Additionally, secondary data utilized in this study are derived from comprehensive literature reviews of academic journals, best practices, and publications, alongside an analysis of relevant Indonesian government policy regulations. This diverse array of sources enriches the research by incorporating a broad spectrum of insights and regulatory frameworks pertinent to the study's focus.

4. Analysis and Discussion

While each crisis exhibits unique characteristics, they can be effectively managed through a structured approach and the implementation of essential measures before, during, and after their occurrence. As delineated in Presidential Regulation Number 47 of 2023, we have organized and classified the process into three distinct phases: pre-crisis, crisis response, and post-crisis. During the pre-crisis phase, the incident response protocol unfolds through sequential stages orchestrated by the organization's cyber incident response team, the sector-specific cyber incident response team, and the national cyber incident response team. Early detection of a cyber crisis entails issuing alerts to operators of electronic systems concerning the escalation of cyber incidents that may precipitate a full-fledged cyber crisis. Following a recommendation from the Head of the Indonesian National Cyber and Crypto Agency, the President declared the status of the cyber crisis and subsequently instituted a Cyber Crisis Task Force.

The primary responsibility of the task force is to execute cyber crisis response activities until stability is restored. Subsequently, a comprehensive report on cyber crisis management is submitted, detailing the analysis outcomes and achievements of crisis management, along with recommendations for subsequent actions in managing cyber crises, to the President. Based on the cyber crisis task team's report, the President declares the end of the cyber crisis. The third stage in the cyber crisis management process is the post-cyber crisis phase. During this phase, the estimated value of damages and losses resulting from the cyber crisis is calculated, recovery costs are determined, and BSSN's response to the crisis is evaluated in collaboration with the system owner. Given this explanation, our focus will be on identifying the tasks and responsibilities that need to be undertaken by the task force and then comparing them with established standards such as NIST Sp. 800-61 rev.2 and ISO 27305-2:2016.

4.1.Analysis of the RACI Matrix

The conceptual model is employed to conduct a RACI Matrix Analysis, which identifies the stakeholders in a task force and their respective roles and responsibilities. An exhaustive narrative detailing the activities undertaken by the task force is encapsulated within the Statement of Work (SOW). This document clearly articulates the task force's objectives and operational framework, enabling potential vendors or stakeholders interested in contributing to the project to assess their capability to fulfill these requirements. The following is the statement of work for the task force:

- Task Force Creator : President

- Title : The National Cyber Crisis Task Force (NCCTF).
- Profile : Constituted to combat cyber crises at the national level, the cyber crisis task force comprises entities vested in national cyber crisis mitigation efforts and those directly involved in such efforts.
- Location : Jakarta, Indonesia.
- Duration : The task force's mission will be fulfilled once the President declares an end to the cyber crisis.
- Description : The NCCTF is tasked with facilitating the management of cyber crises. This encompasses the implementation of countermeasures, recovery processes, compiling reports on the situation, and the formal conclusion of crisis activities..

The Work Breakdown Structure (WBS) constitutes a methodical breakdown of all tasks necessary for project teams to attain the project's objectives (Kountur & Sari, n.d.). An indispensable facet of project management, the WBS elucidates the partitioning of the project's scope into manageable work packages. This fosters a methodical approach to project execution and streamlines the allocation of resources and responsibilities. The WBS, a case study on the NCCTF, is exemplified in Figure 2.

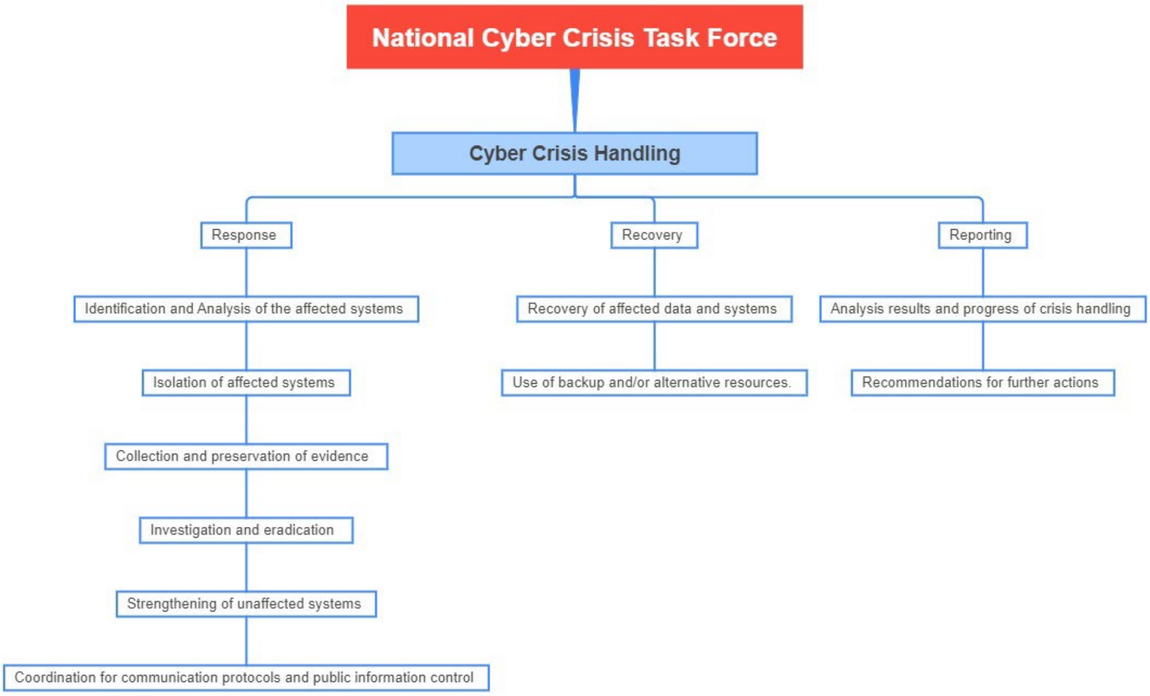
National Cyber Crisis Task Force
Cyber Crisis Handling
Response
Recovery
Reporting
Identification and Analysis of the affected systems
Isolation of affected systems
Collection and preservation of evidence
Investigation and eradication
Strengthening of unaffected systems
Coordination for communication protocols and public information control
Recovery of affected data and systems
Use of backup and/or alternative resources.
Analysis results and progress of crisis handling
Recommendations for further actions

Fig 2. Work Breakdown Structure of the NCCTF

The Stakeholder Register holds paramount importance in project management as it serves to identify, assess, and categorize the stakeholders involved in the task force (Tumuhe & Kiguli, 2019). It offers a comprehensive overview of each role within the Stakeholder Register, thereby facilitating clear communication and the formulation of effective engagement strategies. The stakeholders engaged in the Task Force are categorized into Technical and Strategic Teams. The Technical Team bears responsibility for executing technical incident responses, while the Strategic Team oversees the coordination of cyber crisis management execution, ensuring a holistic approach to addressing and mitigating cyber threats (Gyllencreutz et al., 2020; Sittig & Singh, 2016). As part of the NCCTF's technical stakeholder—the incident response team—we adhere to NIST Special Publication 800-61 Rev. 2 and ISO 27305-2:2023 as our guiding principles. These standards not only govern the operations of the technical response team but also outline the involvement of other groups, both internal and external to the affected organization, that may be essential to the incident response process. A comparison between the guiding principles utilized and the proposed NCCTF is presented in Table 1 below.

Table 1. Comparison of Best Practice and Proposed Stakeholders of NCCTF

NIST Special Publication 800-61 Rev. 2	ISO 27305-2:2023	Proposed NCCTF
Incident Response Personel : • Team Manager • Deputy Manager • Technical lead • Incident lead • Members of technical team (system admin, network admin, programming, technical support, intrusion detection) Expertise includes in Incident Response Team : • Management • Information Assurance • IT Support • Legal Department • Public Affairs and Media Relations • Human Resources • Business Continuity Planning • Physical Security and Facilities	Incident Response Personel : • IRT Manager or team lead • Assistant Managers or Supervisors or Group leaders • Help desk or triage staff • Incident handlers • Vulnerability handlers • Technical writers • IRT Staff (policy, auditing, coordinating, advancing technical skills) Representatives from internal organization can include : • Top Management/Business managers • Representatives from IT • Representatives from legal department • Representatives from HR • Representatives from PR • Physical Security • Audit and Risk Management specialist • Any law enforcement liaisons or investigators • General representatives from the constituency External interested parties can include: • Contracted external support personel • Other CSIRTs • Service Providers	NCCTF Personnel : • Head Of Task Force • Deputy Head • Help Desk • Incident Response Team • Vulnerability Handlers • Technical Writers • The Leader of the Affected Organization • Information Assurance/Audit and Risk Management Specialist • IT Technical Support • Legal personnel, Law Enforcement Liaisons, Or Investigator • Public Affairs and Media Relations • Business Continuity Planning Team • General Representatives from The Constituency • Physical Security • Others CSIRT Organization • General Public

	• Law enforcement organizations • Emergency authorities • Appropriate government organizations • Legal personnel • Public relations or Media • Business partners • Customers • General Public • Technical Support	

As outlined, the Stakeholder Register for the National Cyber Crisis Task Force has been meticulously compiled, as depicted in Table 2. Drawing on insights gleaned from expert interviews, we have also identified the specific institutions or organizations assigned to each role within the task force. Public or private institutions can fulfill the allocation of these positions, contingent upon the requirements and objectives of the task force at any given time. This flexibility ensures that the task force's composition can adapt to the diverse and dynamic nature of cyber crises, leveraging the unique capabilities and resources of both sectors to effectively manage and mitigate such incidents. In addition to public-private partnerships, involving external parties such as professional experts, as explained in Table 1, and other CSIRTs(domestic or/and international) is crucial, especially during escalated cyber crises requiring additional resources. For example, research by Skierka (2023) found that during the 2017 eID Crisis in Estonia, networked cooperation and collaboration capital were instrumental. Estonia established the eID working group comprising government entities, IT manufacturers, infrastructure operators, end users from various organizations and sectors to manage the crisis. Furthermore, Estonia sought assistance from the European Union's CSIRT and experts for consultation and technical support, resulting in the successful restoration of eID services through collective collaboration.

Table 2. Stakeholder Register

NO.	STAKEHOLDER	ASSIGNED ORGANIZATIONS	STAKEHOLDERS CATEGORY
1	Head Of Task Force	Head of National Cyber Agency (BSSN)	Strategic
2	Deputy Head	Deputy Head of National Cyber Agency	Strategic
3	Help Desk	National CSIRT	Technical
4	Incident Response Team	Joint Operation by National CSIRT, Sectoral CSIRT, Organizational CSIRT	Technical
5	Vulnerability Handlers	Joint Operation by National CSIRT, Sectoral CSIRT, Organizational CSIRT	Technical
6	Technical Writers	Task Force Secretariat	Technical
7	The Leader of the Affected Organization	The Leader of the Affected Organization (Leader of Affected Vital Infrastructure)	Strategic
8	Information Assurance/Audit and Risk	Public: Ministry of communication and information, BSSN Private: expert auditor	Technical

	Management Specialist		
9	IT Technical Support	Public: Ministry of communication and information, BSSN Private: ISP vendors, Telco vendors, IT vendors.	Technical
10	Legal personnel, Law Enforcement Liaisons, Or Investigator	Public: Appointed personnel from legal bureau, prosecutor, police, National Intelligence Agency Private: expert lawyer	Strategic
11	Public Affairs and Media Relations	Public: appointed spokesperson Private: media support	Strategic
12	Business Continuity Planning Team	Public: Ministry of communication and information, BSSN Private: ISP vendors, Telco vendors, IT vendors.	Technical
13	General Representatives from The Constituency	Business Partners and Customers	Strategic
14	Physical Security	MoD, National Army, National Police	Strategic
15	Others CSIRT Organization	International or domestic CSIRT partners	Strategic
16	General Public	General public	Strategic

4.2.Structure of the Task Force Organization

The organizational structure plays a pivotal role in project management (Rieger & Tjoa, 2019), elucidating the interaction between the strategic and technical teams in addressing cyber crises (Mubarok et al., 2020). It also delineates the extent of authority, communication supervision, and coordination and collaboration mechanisms among each team. This clarity is indispensable for ensuring efficient task execution, with explicit directives and a streamlined process for decision-making and problem-solving. Despite the absence of a defined structure for the task force in Presidential Regulations No.47/2023, the need for an organized framework is undeniable. Consequently, we have proposed an organizational structure that aligns with the roles and responsibilities outlined within the regulation. Figure 3 illustrates a structure aimed at enhancing the task force's capacity to manage cyber crises by fostering robust coordination and collaboration between its technical and strategic levels, thereby ultimately enhancing the overall response to cyber incidents.

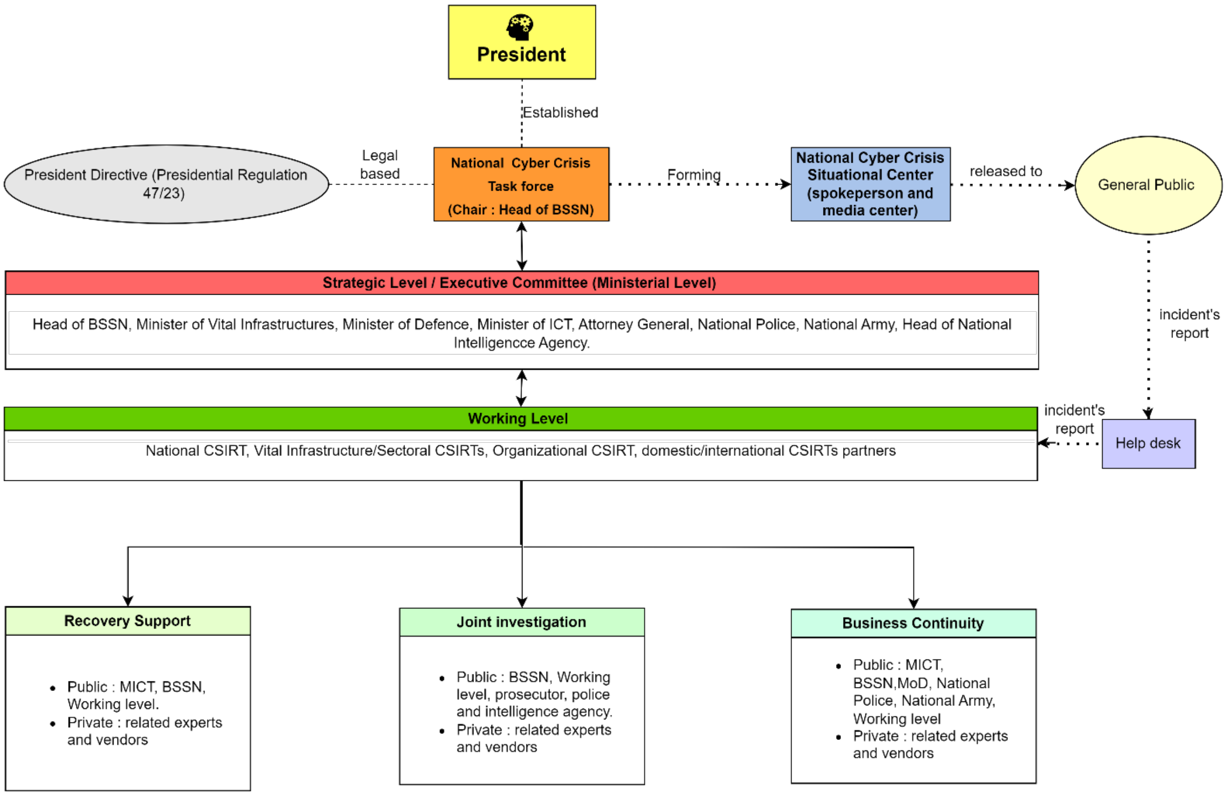
President
Established
President Directive (Presidential Regulation 47/23)
Legal based
National Cyber Crisis Task force (Chair : Head of BSSN)
Forming
National Cyber Crisis Situational Center (spokeperson and media center)
released to
General Public
incident's report
Strategic Level / Executive Committee (Ministerial Level)
Head of BSSN, Minister of Vital Infrastructures, Minister of Defence, Minister of ICT, Attorney General, National Police, National Army, Head of National Intelligencce Agency.
Working Level
National CSIRT, Vital Infrastructure/Sectoral CSIRTs, Organizational CSIRT, domestic/international CSIRTs partners
incident's report
Help desk
Recovery Support
Public : MICT, BSSN, Working level.
Private : related experts and vendors
Joint investigation
Public : BSSN, Working level, prosecutor, police and intelligence agency.
Private : related experts and vendors
Business Continuity
Public : MICT, BSSN,MoD, National Police, National Army, Working level
Private : related experts and vendors

Fig. 3. National Cyber Crisis Task Force Structure

Following the establishment of the organizational structure, the next step involves defining the Activity List, formulated based on the stipulations of the regulations and insights garnered from interviews. The Activity List serves as a comprehensive guide for task force members, clarifying the scope of work and detailing job responsibilities for every phase of cyber crisis management. This document is instrumental in clarifying the expected outcomes, procedures, and responsibilities, enabling members to execute their tasks clearly understanding their roles and the objectives to be achieved. Through this systematic approach, the task force is better equipped to navigate the complexities of handling cyber crises efficiently and effectively (Dwi et al., 2021). Table 3 illustrates the activity list undertaken by the NCCTF.

Table 3. Activity List

Function	List of Activities	Appointed Actors
Leadership	• Organize and direct activities • Establish the working team and define the crisis scope, setting up the national cyber crisis center. • Submit the final report to the President.	Head of BSSN and High-Level leaders from MoD
Strategic Level	• Assign guidelines and select working team representatives. • Engage domestic and international stakeholders. • Receive operational updates and disseminate information through the situational center.	Ministerial Level Committee
Recovery Support	• Identify, assess, and isolate compromised systems. • Re-test critical and supporting functions.	BSSN, Kemenkominfo and working level
	If necessary, involve experts.	Experts
	Assist in incident recovery if required.	CSIRT partners

Joint investigation	• Investigate and eliminate the sources of crises. • Gather and preserve evidence.	Working team
	• Conduct digital forensics, take legal actions, raise public awareness, and collaborate with domestic and international stakeholders.	POLRI
	• Implement regulations, prosecute offenders, and advocate the government's stance.	Prosecuting attorney
	• Conduct counterintelligence; collect, analyze, and share CTI (cyber threat intelligence); attribute incidents to state or non-state threat actors.	BIN
	Involve expert forensic investigators, lawyers, or detectives if required	Experts
	Assist in the incident investigation process if necessary.	CSIRT partners
Business Continuity	• Strengthen unaffected systems. • Implement crisis communication procedures and manage public information releases. • Recover data using backups.	Working team
	• Support backup and DRP infrastructures.	Kemenkominfo
	• Coordinate defense assets to ensure critical business operations continue.	MoD
	• Provide protection for critical infrastructures.	POLRI
	• Support physical protection for critical infrastructures. • Assist in deploying defense resources as reserves.	National Army (TNI)
	• Provide expertise in information assurance.	Auditor
Help Desk	• Receive reports, assist with technical issues, track tickets, and maintain security systems.	Appointed working team
National Cyber Crisis Situational Center	• Supervise and manage operations. • Make strategic decisions, communicate effectively, analyze data, monitor situations, and report as necessary.	Head of Task Force/Deputy Head and Ministerial level committee
	Provide crisis updates.	Appointed spokesperson
	Draft final reports on cyber crisis handling.	Technical writer/Secretariat

4.3.Graphical Results

The explanation below details the outcomes of establishing the Stakeholder Assignment Matrix for the NCCTF.

4.3.1. Activity Diagram Context

An activity diagram is a graphical tool that utilizes various symbols to represent the stepwise progression of multiple tasks, elucidating the interconnections among distinct processes within an activity. As a potent instrument for exhaustively delineating a process, an activity diagram integrates squares, diamonds, and other geometric figures interconnected by arrows to symbolize different elements of the process. Through the amalgamation of flow lines and symbols, activity diagrams effectively convey the dynamics of an operation, facilitating a comprehensive understanding of the workflow and interactions inherent in an activity (Dwi et al., 2021). The activity diagram in Figure 4 describes how the workflow of the NCCTF has been identified.

4.3.2. RACI Matrix.

After conducting interviews and reviewing regulations, Table 4 presents the RACI matrix results, identifying the specific roles and responsibilities of each stakeholder in the task force. The matrix reveals that the President holds the ultimate authority, while the Head of BSSN chairs the task force.

TABLE 4. *RACI MATRIX RESULTS*

No	Activity	President	TF Head or Deputy Head	Strategic level	Working level	BSSN	MoD	Kemenkominfo	BIN	prosecutor	TNI	POLRI	CSIRT partners	helpdesk	spokesperson	External experts
1	Establish a task force	🟥	🟨	🟩	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
2	Organize and direct the task force	🟦	🟥 🟩	🟨	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
3	Establish working level	🟦	🟥 🟩	🟨	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
4	Create working-level representatives	🟦	🟩	🟥	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟩
5	Providing guidelines and strategy to working level	🟦	🟨	🟥	🟩	🟩	🟩	🟩	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩
6	Decide the parties involved	🟦 🟩	🟨 🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟦	🟦
7	Recovery supports	🟦	🟩	🟨	🟥	🟨	🟩	🟨	🟦	🟦	🟦	🟦	🟩	🟦	🟦	🟩
8	Joint investigation	🟦	🟩	🟨	🟥	🟩	🟦	🟩	🟨	🟨	🟦	🟨	🟩	🟦	🟦	🟩
9	Business Continuity Process	🟦	🟩	🟨	🟥	🟨	🟨	🟨	🟦	🟦	🟨	🟨	🟩	🟦	🟦	🟩
10	Make final report of cyber crisis	🟦	🟨	🟥	🟩	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟩
11	Provide updates on crises to the public	🟦	🟩	🟨	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟦
12	Receive reports of incidents	🟦	🟩	🟩	🟨	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟦	🟦
13	Receive final reports and end the cyber crisis status	🟥	🟨	🟩	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

🟥 : Responsible, 🟨 : Accountable, 🟩 : Consulted, 🟦 : Informed

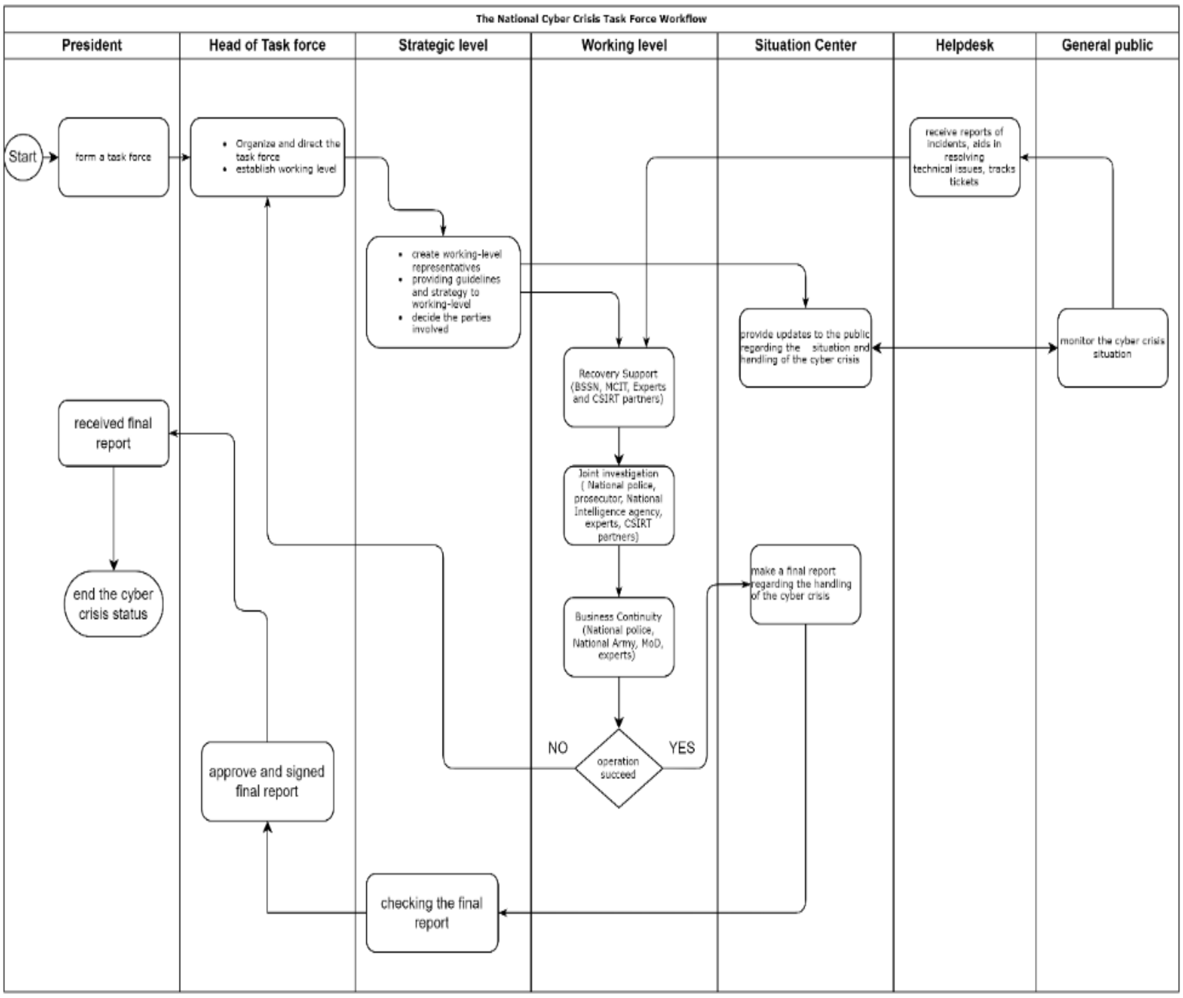
The National Cyber Crisis Task Force Workflow
President
Head of Task force
Strategic level
Working level
Situation Center
Helpdesk
General public
Start
form a task force
Organize and direct the task force
establish working level
receive reports of incidents, aids in resolving technical issues, tracks tickets
create working-level representatives
providing guidelines and strategy to working-level
decide the parties involved
provide updates to the public regarding the situation and handling of the cyber crisis
monitor the cyber crisis situation
Recovery Support (BSSN, MCIT, Experts and CSIRT partners)
received final report
Joint investigation (National police, prosecutor, National Intelligence agency, experts, CSIRT partners)
end the cyber crisis status
make a final report regarding the handling of the cyber crisis
Business Continuity (National police, National Army, MoD, experts)
NO
operation succeed
YES
approve and signed final report
checking the final report

Fig.4. Activity Diagram of NCCTF

4.4.Discussion

This research employs the RACI approach in preparing the Cyber Crisis Task Force, as mandated by Indonesia's regulations. Each element of the RACI matrix is established by delineating the roles and responsibilities designated to individual stakeholders throughout the business process (Trani et al., 2022). The Indonesian NCCTF was formulated using the RACI matrix method, categorizing 15 stakeholders into strategic and technical groups. The government institutions involved include BSSN, the Ministry of Defence, the Ministry of Communication and Information, the National Intelligence Agency, the Prosecutor, the National Army, and the National Police. Non-governmental involvement can be facilitated by CSIRT partners and experts.

The ultimate authority resides with the President, who possesses the prerogative to determine the imposition and termination of cyber crisis status. The task force is chaired by the Head of BSSN, while the deputy head of the task force may be selected from the Ministry of Defence, given the close nexus between cyber crises and national security and defense (S Boeke, 2016), which falls under the primary purview of the Ministry of Defence (DPRRI, 2002). Furthermore, at the strategic level, representatives from each executive of the relevant Ministries, including Ministries from vital sectors affected by massive cyber-attacks, such as the Ministry of Defence and the Ministry of ICT, are included. The Ministry of ICT oversees ICT resource utilization, infrastructure management, and personal data protection. The Attorney General provides legal counsel and addresses legal considerations that may arise during cyber crises, while the National Police addresses cybercrime elements and anticipates their impact during such crises. The National Army contributes insights into conducting cyber operations and maintaining national order, whereas the State Intelligence Agency furnishes intelligence related to cyber threats. This committee serves as a platform for interagency coordination, facilitating expedited decision-making processes grounded in comprehensive considerations (Ezioni & Siboni, 2021). Additionally, apart from its strategic role for executives, this agency also serves as a contributor at the operational level by engaging its personnel as active members in operational tasks.

The operational aspect in this scenario is primarily managed by a unified CSIRT consisting of CSIRT entities from the affected agencies, the CSIRT sector, and the National CSIRT. At this level, the operational team functions as a cohesive unit to address technical facets of cyber crises (Sergei Boeke, 2018). Should the collaborative efforts of this amalgamated CSIRT prove insufficient, they can seek assistance from other CSIRTs, both domestically and internationally, with established collaborative agreements (Ramluckan et al., 2019). Additionally, as an auxiliary measure to mitigate the cyber crisis, the task force may also solicit support from relevant experts, encompassing strategic, managerial, technical, and legal expertise, among others (Staves et al., 2022). It is anticipated that the delineation of NCCTF members and their responsibilities will constitute one of the preparatory steps for confronting the threat of cyber crises in the future, thereby establishing a secure and adaptable cyber domain. The proposed structure of the task force, featuring strategic and technical teams, aligns with best practices identified in prior studies (e.g., Ezioni & Siboni, 2021). Nevertheless, the efficacy of this framework within the Indonesian context remains untested, warranting further research to examine its implementation and outcomes.

5. Conclusion

This study contributes to the burgeoning field of research on cyber crisis management by proposing a framework for establishing a National Cyber Crisis Task Force in Indonesia. Utilizing the RACI matrix approach, the study identifies key stakeholders, roles, and responsibilities essential for an effective response to cyber crises. The findings underscore the significance of collaboration between strategic and technical teams, as well as the involvement of both public and private sector entities.

The proposed organizational structure and workflow of the NCCTF offer a practical guide for policymakers and practitioners in Indonesia and other nations grappling with similar challenges. By clearly defining the roles and responsibilities of each stakeholder, the NCCTF can ensure a synchronized and efficient response to cyber crises, thereby minimizing damage and bolstering national security.

Nonetheless, the study acknowledges the limitations of its approach, including the necessity for a more comprehensive delineation of roles and responsibilities and the potential for unidentified processes. Future research endeavors could address these lacunae by conducting more exhaustive interviews with a broader spectrum of stakeholders, particularly from the private sector and international spheres.

Furthermore, the efficacy of the proposed NCCTF framework requires validation in real-world scenarios. Subsequent studies could scrutinize the framework's implementation during actual cyber crises, assessing its strengths and weaknesses, and pinpointing areas for enhancement. Additionally, forthcoming research could explore communication protocols, business continuity processes, and the categorization of cyber crises to further fortify the task force's effectiveness.

In conclusion, this study represents a significant stride towards fortifying Indonesia's national security through the proposition of a structured approach to establishing a National Cyber Crisis Task Force. By building upon this groundwork and addressing identified limitations and future research directions, Indonesia can cultivate a robust and resilient system for managing cyber crises, thereby safeguarding its critical infrastructure and citizenry.

Acknowledgements

We extend our sincere gratitude to the National Cyber Agency of the Republic of Indonesia (BSSN), the Ministry of Defence of the Republic of Indonesia, the Republic of Indonesia Defense University (Universitas Pertahanan RI), and all respondents for their invaluable assistance in completing this research.

References

Aguilar, A. I., Li, R., Pereira, R., & Lee, W.-. (2023). Responsibility Assignment Matrix in Responding to Critical Outages : A Case Study of IT Incident Management Activity Process Design. *MSIE*, 1–8. https://doi.org/10.1145/3603955.3603956

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Backman, S. (2021). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, *29*(4), 429–438. https://doi.org/10.1111/1468-5973.12347

Bahuguna, A., Bisht, R. K., & Pande, J. (2019). Don't wanna cry: A cyber crisis table top exercise for assessing the preparedness against eminent threats. *International Journal of Engineering and Advanced Technology*, *9*(1), 3705–3710. https://doi.org/10.35940/ijeat.A9893.109119

Boeke, S. (2016). First responder or last resort? The role of the Ministry of Defence in national cyber crisis management in four European countries. *First Responder or Last Resort? The …*, *September*.

Boeke, Sergei. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449–464. https://doi.org/10.1111/gove.12309

Chandrasekar, K., Selvanayagam, K., & Rehman, V. (2021). Responsibility Finds A Way: A Typology and Framework Development Approach Towards Public Sector Crisis Management. *International Journal of Strategic Communication*, *15*(4), 328–356. https://doi.org/10.1080/1553118X.2021.1872081

Control, J., Galinec, D., Možnik, D., & Guberina, B. (2018). *Cybersecurity and cyber defence : national level strategic approach*. *1144*. https://doi.org/10.1080/00051144.2017.1407022

Danet, D., & Weber, C. (2020). Cyber Crisis Management and Leadership. *19th European Conference on Cyber Warfare and Security*. https://doi.org/10.34190/EWS.20.032

Deloitte. (2016). *Readiness, response, and recovery*. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf

DPRRI. (2002). *UU Nomor 3 Tahun 2002 tentang Pertahanan Negara*. *September*, 1–2.

Dwi, R., Suhanda, P., & Pratami, D. (2021). RACI Matrix Design for Managing Stakeholders in Project Case Study of PT . *International Journal of Innovation in Enterprise System*, *02*, 122–133.

Dykstra, J. A. B. S., & Orr, S. R. (2017). Acting in the unknown: The cynefin framework for managing cybersecurity risk in dynamic decision making. *2016 IEEE International Conference on Cyber Conflict, CyCon U.S. 2016*. https://doi.org/10.1109/CYCONUS.2016.7836616

Ezioni, L., & Siboni, G. (2021). Cyber crisis management and regulation. *Cybersecurity And Legal-Regulatory Aspects*, 1–22. https://doi.org/10.1142/9789811219160_0001

Fitriani, W. R., Sutanto, J., Handayani, P. W., & Hidayanto, A. N. (2023). User Compliance With the

Health Emergency and Disaster Management System: Systematic Literature Review. *Journal of Medical Internet Research*, *25*, 1–23. https://doi.org/10.2196/41168

Frykmer, T., & Becker, P. (2023). Emergence and institutionalization of interorganizational coordination structures in crises. *Journal of Contingencies and Crisis Management*, *September*, 1–9. https://doi.org/10.1111/1468-5973.12510

Gultom, R. A. G., Wadjdi, A. F., Poniman, A., Martha, S., & Kristijarso. (2021). Sixware Cybersecurity Framework Development To Protect Defense Critical Infrastructure And Military Information Systems. *International Journal of Scientific & Technology Research*, *10*(01).

Gyllencreutz, L., Rådestad, M., & Saveman, B. I. (2020). Templates for handling multi-agency collaboration activities and priorities in mining injury incidents: a Delphi study. *International Journal of Emergency Services*, *9*(3), 257–271. https://doi.org/10.1108/IJES-06-2019-0026

Halizahari, M., Wong, M. R., Ahmad, N. D. F., Zain, R., & Zainol, N. A. H. (2023). Scenario Planning and Simulation in Disaster Response. *International Journal on Advanced Science, Engineering and Information Technology*, *13*(4), 1235–1241. https://doi.org/10.18517/ijaseit.13.4.17403

Hasle, P. (2023). Reduction of changeover time through SMED with RACI integration in garment factories. *International Journal of Lean Six Sigma*. https://doi.org/10.1108/IJLSS-10-2021-0176

Hirmer, S. A., George-williams, H., Rhys, J., Mcnicholl, D., & Mcculloch, M. (2021). Stakeholder decision-making : Understanding Sierra Leone ’ s energy sector. *Renewable and Sustainable Energy Reviews*, *145*, 111093. https://doi.org/10.1016/j.rser.2021.111093

John W. Creswell; J. David Creswell. (2022). *Research design : qualitative, quantitative, and mixed methods approaches* (6th editio). SAGE Publication. edge.sagepub.com/creswellrd6e

Presidential Bill No. 47/2023 : National Cyber Security Strategy and Cyber Crisis Management, (2023) (testimony of Jokowi).

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers and Security*, *99*, 102036. https://doi.org/10.1016/j.cose.2020.102036

Kountur, R., & Sari, M. R. (n.d.). *structure and business process*. *2023*, 1–7. https://doi.org/10.1057/s41599-023-02028-8

Lai, Y. L., & Cai, W. (2023). Enhancing post-COVID-19 work resilience in hospitality: A micro-level crisis management framework. *Tourism and Hospitality Research*, *23*(1), 88–100. https://doi.org/10.1177/14673584221075182

Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal*, *30*(3), 139–148. https://doi.org/10.1080/19393555.2020.1813851

Martha Warta Silaban. (2022, September 13). Saling Lempar Tanggung Jawab Atasi Kebocoran Data Pribadi. *Tempo.Co*. https://fokus.tempo.co/read/1634420/saling-lempar-tanggung-jawab-atasi-kebocoran-data-pribadi

Matshaba, L., & Nxozi, M. (2023). Guiding the Development of Interoperable Health Information Systems : A Guiding the development of interoperable health information systems : A conceptual IT governance framework. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 13873 LNCS*, *September*, 143–156. https://doi.org/10.1007/978-3-031-32808-4

Mikušová, M., & Horváthová, P. (2019). Prepared for a crisis? Basic elements of crisis management in an organisation. *Economic Research-Ekonomska Istrazivanja* , *32*(1), 1844–1868. https://doi.org/10.1080/1331677X.2019.1640625

Mott, G., Nurse, J. R. C., & Baker-Beall, C. (2023). Preparing for future cyber crises: lessons from governance of the coronavirus pandemic. *Policy Design and Practice*, *6*(2), 160–181. https://doi.org/10.1080/25741292.2023.2205764

Mubarok, S., Zauhar, S., Setyowati, E., & Suryadi, S. (2020). Policy Implementation Analysis: Exploration of George Edward III, Marilee S Grindle, and Mazmanian and Sabatier Theories in the Policy Analysis Triangle Framework. *Journal of Public Administration Studies*, *005*(01), 33–38. https://doi.org/10.21776/ub.jpas.2020.005.01.7

Panagiotis Trimintzios; Razvan Gavrila; Makrodimitris Georgios. (2014). *Report on cyber-crisis cooperation and management* (Issue November). ENISA. https://doi.org/10.2824/34669

Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: a framework for crisis management. *Academy of Management Perspectives*, *7*(1), 48–59. https://doi.org/10.5465/ame.1993.9409142058

Prabaswari, P., Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. *Matra Pembaruan*, *6*(1), 1–14. https://doi.org/10.21787/mp.6.1.2022.1-14

Prevezianou, M. F. (2021). Beyond Ones and Zeros: Conceptualizing Cyber Crises. *Risk, Hazards and Crisis in Public Policy*, *12*(1), 51–72. https://doi.org/10.1002/rhc3.12204

Ramluckan, T., Niekerk, B. van, & Leenen, L. (2019). Research challenges for cybersecurity and cyberwarfare: A south african perspective. *European Conference on Information Warfare and Security, ECCWS*, *2019-July*, 372–378.

Rieger, D., & Tjoa, S. (2019). A Readiness Model for Measuring the Maturity of Cyber Security Incident Management. *Lecture Notes on Data Engineering and Communications Technologies*, *23*, 283–293. https://doi.org/10.1007/978-3-319-98557-2_26

Santoso, B., Rahaja, J., & Purnomo, M. (2023). An Empirical Study on The Entrepreneurial Factors Influencing Collaborative Innovation to Cope with Crisis Situations. *Journal of System and Management Sciences*, *13*(5), 497–512. https://doi.org/10.33168/JSMS.2023.0532

Sarwar, M. I., Abbas, Q., Alyas, T., Alzahrani, A., Alghamdi, T., & Alsaawy, Y. (2023). Digital Transformation of Public Sector Governance With IT Service Management-A Pilot Study. *IEEE Access*, *11*(January), 6490–6512. https://doi.org/10.1109/ACCESS.2023.3237550

Shaked, A., Cherdantseva, Y., Burnap, P., & Maynard, P. (2023). Operations-informed incident response playbooks. *Computers and Security*, *134*(July), 103454. https://doi.org/10.1016/j.cose.2023.103454

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, Mitigating, and recovering from Ransomware attacks. *Applied Clinical Informatics*, *7*(2), 624–632. https://doi.org/10.4338/ACI-2016-04-SOA-0064

Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, *40*(1), 101781. https://doi.org/10.1016/j.giq.2022.101781

Solikhawati, A., & Samsuri, A. (2023). *Evaluasi Bank Syariah Indonesia Pasca Serangan Siber : Pergerakan Saham dan Kinerja Keuangan*. *9*(03), 4201–4208.

Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. *International Journal of Critical Infrastructure Protection*, *37*(March 2021), 100505. https://doi.org/10.1016/j.ijcip.2021.100505

Sufi, F. (2023). Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges. *Information (Switzerland)*, *14*(9). https://doi.org/10.3390/info14090485

Sutikno, T., & Stiawan, D. (2022). Cyberattacks and data breaches in Indonesia by Bjorka: hacker or data collector? *Bulletin of Electrical Engineering and Informatics*, *11*(6), 2989–2994. https://doi.org/10.11591/eei.v11i6.4854

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers and Security*, *45*, 42–57. https://doi.org/10.1016/j.cose.2014.05.003

Trani, M. L., Minotti, N. M., & Farnetti, B. (2022). OPTIMIZING COMMUNICATION FLOWS USING A STANDARD BIM ORIENTED RACI MATRIX. *Proceedings of International Structural Engineering and Construction*, *9*(2), 1–6. https://doi.org/www.doi.org/10.14455/ISEC.2022.9(2).CPM-04

Tumuhe, C. L., & Kiguli, J. (2019). *Tree Planting Stakeholder analysis in the Ugandan Albertine Rift*. *7*(March).

Uly Yohana Artha; Sukmana Yoga. (2023, May 11). Layanan “Error” 4 Hari, BSI Temukan Dugaan Serangan Siber. *Kompas.Com*. https://money.kompas.com/read/2023/05/11/203836226/layanan-error-4-hari-bsi-temukan-dugaan-serangan-siber

Xu, M., & Lu, C. (2021). China–U.S. cyber-crisis management. *China International Strategy Review*, *3*(1), 97–114. https://doi.org/10.1007/s42533-021-00079-7

Yerina, A. M., Honchar, I. A., & Zaiets, S. V. (2021). Statistical indicators of cybersecurity development in the context of digital transformation of economy and society. In *Science and Innovation* (Vol. 17, Issue 3). https://doi.org/10.15407/scine17.03.003