SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 03 No. 02 (2026), pp. 112-125
Research Article
doi: https://doi.org/10.70710/sitj.v3i2.95

Developing a Competency Framework for Cyber Intelligence Professionals in Indonesia: An Analytical Perspective

Dwi Andriarto[1,a,*]

[1]Intelligence Studies, Sekolah Tinggi Intelijen Negara, Indonesia
[a]dwiandriarto@gmail.com
*Corresponding author

Article Info
Received: 7-May-2026
Revised: 22-May-2026
Accepted: 30-June-2026

Keywords
Competency Framework; Cybersecurity; Cyber Threat Intelligence; Indonesia; National Security

Abstract
The advancement of information and communication technology has led to logical consequences in the form of increasingly complex threats to national security, thus requiring an integrated and comprehensive role of cyber intelligence in addressing these various cyber threats. The management of cyber intelligence in Indonesia is still considered suboptimal due to the lack of basic references in the form of conceptual frameworks or competencies related to cyber intelligence. The purpose of this research is to provide an understanding of the framework of cyber intelligence and to develop a competency framework for cyber intelligence professionals in Indonesia, encompassing various necessary skills and expertise. The method used in this research is qualitative, collecting data through literature studies related to the research object and subsequently analyzed using descriptive analytical techniques. The results show that there are at least two cyber intelligence frameworks that can serve as a basis for use in Indonesia, namely the SEI model from Carnegie Mellon University and the FIRST Cyber Threat Intelligence SIG model. In addition, the Indonesian government may consider five core competencies needed to enhance the capabilities of domestic cyber intelligence, namely technical competency, analytic competency, knowledge management (information) competency, contextual domain competency, and communication and organizational competency. These five competencies need to be formulated clearly and specifically, considering the dynamics of cybersecurity domestically and the international geopolitical constellation.

1. Introduction

The rapid advancement of information and communication technology (ICT) has generated logical consequences in the form of increasingly complex threats to national security. Although increasingly sophisticated infrastructures have been developed to respond to the rapid pace of technological change, their existence has become highly critical. Graham (2009) argued that modern infrastructures are inherently more vulnerable to catastrophic failures because human dependence on technology continues to increase, making these infrastructures essential for fulfilling the needs of society. In this context, various critical infrastructures and data centers, both physical and non-physical, have become increasingly integrated into digital technologies and interconnected networks. While such integration provides greater accessibility and operational control, it simultaneously introduces new security risks that must be anticipated, particularly cyber intrusions capable of penetrating data security systems and critical infrastructures.

From the perspective of the state, cyber threats have become an increasingly important issue in the domain of national security. Cyberattacks and cyber warfare are currently regarded as highly effective instruments for disrupting national stability because they are relatively easy to execute, require minimal operational costs, and are capable of achieving strategic objectives effectively (Caplan, 2013). Furthermore, cyber threats continue to evolve in terms of methods, targets, and impacts, thereby increasing the likelihood that states may experience greater insecurity in the future (Astarini & Rofii, 2021). These vulnerabilities are exacerbated by the difficulty of establishing resilience against cyberattacks, as the complexity of interconnected networks creates opportunities for threat actors to conceal their identities and conduct attacks from multiple locations worldwide.

In Indonesia, cybersecurity has emerged as a new strategic domain within the national defense framework because cyber threats are considered capable of causing strategic losses to the state. The Indonesian Defense White Paper (2015) emphasized that cyber defense capabilities should be developed in an integrated and synergistic manner among all instruments of national power in order to reduce cyber risks and safeguard national security interests. However, in practice, many observers argue that the concept of cyber defense in Indonesia has not yet been implemented optimally. Rahim et al. (2023), for instance, identified the absence of comprehensive cybersecurity governance policies—including cyber policies, cybersecurity strategies, and cybersecurity frameworks—as one of the major challenges in Indonesia's cyber domain. Similarly, Septasari (2023) argued that the weakness of cybersecurity instruments in Indonesia has contributed to the increasing number of cyber incidents, which have reached millions of cases.

Based on their characteristics and forms, cyber threats may also be categorized as serious threats from an intelligence perspective. Cases involving the theft of strategic information, intrusions into internal government networks and servers, wiretapping of communications involving high-ranking state officials, and other cyberattacks demonstrate the seriousness of such threats (Djoyonegoro, 2018). In this regard, cyber intelligence management has become a strategic necessity, considering that all forms of threats, hostile activities, and malicious actions constitute the core business of intelligence in conducting early detection and warning efforts, as stipulated in Law Number 17 of 2011 concerning State Intelligence.

Considering the current conditions, Indonesia's readiness in terms of infrastructure, institutional capacity, human resources, budget allocation, and technological capability is still regarded as insufficient to address various challenges in cyberspace. Although the Indonesian government has initiated the establishment of a national cyber institution capable of formally accommodating cyber intelligence functions, these efforts have not yet been accompanied by the formal integration of cyber intelligence into the national intelligence governance system. Consequently, cybersecurity governance in Indonesia remains fragmented and insufficiently integrated (Astarini & Rofii, 2021). Therefore, there is an urgent need for a cyber intelligence framework or governance model in Indonesia, particularly regarding the competencies required to formulate effective strategies for addressing cybersecurity challenges.

Based on these issues, this study seeks to emphasize the importance of a competency framework for cyber intelligence professionals in order to support the establishment of an effective and efficient cybersecurity governance system in Indonesia. The objective of this research is to provide an understanding of cyber intelligence frameworks and to develop a competency framework for cyber intelligence professionals in Indonesia, encompassing the various competencies required in this field.

2. Literature Review

2.1. Intelligence Theory

The definition of intelligence varies considerably, resulting in the absence of a universally accepted academic consensus regarding its general meaning. Nevertheless, various literature studies as well as statements from scholars and practitioners may serve as references for understanding the concept of intelligence. In essence, these differences in definition are largely semantic in nature, meaning that the term "intelligence" can still be understood through meanings that share similar characteristics. Prunckun (2015) identified at least four definitions of intelligence based on a semantic approach derived from various literatures: (1) an action or process used to produce knowledge; (2) a body of knowledge generated through the intelligence process; (3) an organization concerned with knowledge, such as an intelligence

agency; and (4) reports produced for decision-makers through intelligence processes or by intelligence organizations.

According to Prunckun (2015) in his book Scientific Methods of Inquiry for Intelligence Analysis, intelligence as knowledge may refer to several contexts, including national security, military affairs, law enforcement, business, and other private sectors. Meanwhile, intelligence as a process is understood as a series of steps or procedures summarized within an intelligence cycle, commonly referred to as the intelligence cycle process. In practice, the intelligence cycle generally consists of several interrelated stages, including direction, collection, processing, analysis, dissemination, and feedback. These stages are designed to ensure that information is systematically transformed into intelligence products that support decision-making processes.

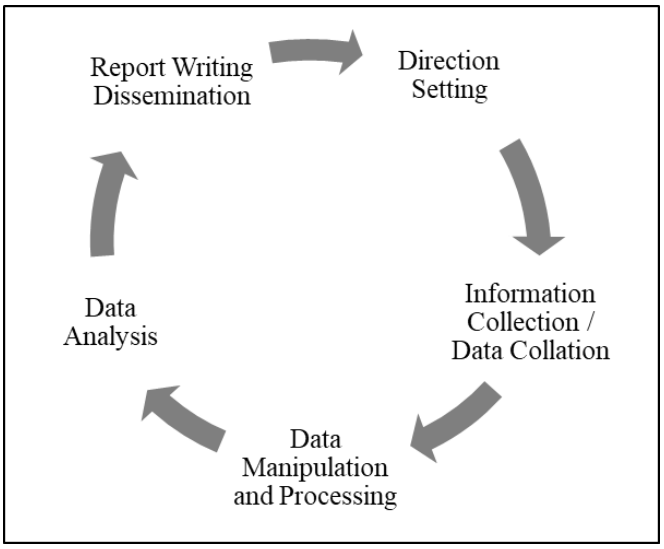

Figure 1. Intelligence Cycle or Intelligence Process

Michael Warner (2007) also argued in his presentation that intelligence carries multiple meanings for different actors, making it difficult to formulate a single universally accepted definition of intelligence. In this context, two general definitions are commonly used: "intelligence for decision-makers" and "secret intelligence activities conducted by a state to understand or influence foreign entities." In addition, Sun Tzu (1963) introduced the concept of "espionage" within the context of intelligence, referring to both information collection and covert action activities. Sun Tzu further emphasized the doctrine that intelligence operations must be conducted in secrecy in order to function as "The Divine Skein" and become a valuable asset for maintaining state sovereignty (Astarini & Rofii, 2021).

2.2. Cyber Intelligence Concept

Cyber intelligence may be defined as a process or product within the intelligence cycle aimed at assessing the capabilities, intentions, or activities of potential adversaries or hostile actors in cyberspace. In this regard, cybersecurity and cyber threats have become one of the primary concerns of intelligence operations. Astarini and Rofii (2021) identified several important aspects that must be considered in addressing cybersecurity issues from an intelligence perspective, including:

a. The necessity of utilizing the internet for collecting, processing, and storing intelligence information and data, thereby requiring a high level of security protection.

b. The need for specialized capabilities to anticipate and detect cyberattacks in support of national interests and national security.

c. The importance of anticipating emerging threats to state security arising from advances in cyber technology.

Within the context of cybersecurity, strengthening cyber intelligence capabilities—particularly among intelligence agencies and authorized institutions—constitutes a strategic measure to anticipate various actual and potential cyber threats. Although cybersecurity generally emphasizes the existence of cyber threats against a state, intelligence itself may function as both a defensive and offensive instrument (Brantly, 2013). In this context, cyber intelligence must be capable of controlling and managing cyber-related data and information to support national security strategies. Consequently, cyber intelligence possesses the capacity to provide strategic input for future-oriented decision-making processes and is not solely limited to passive or protective functions.

According to the study conducted by Ettinger et al. (2019), cyber intelligence is defined as the process of collecting, processing, analyzing, and disseminating information in order to identify, track, or predict threats, risks, and opportunities within cyberspace, thereby offering actionable recommendations for decision-making purposes. The study further highlighted that the concepts of cybersecurity and cyber intelligence are frequently misunderstood as interchangeable terms, which may create biases in efforts to address vulnerabilities within organizations. Cybersecurity itself refers to the measures and actions undertaken to ensure the confidentiality, integrity, and availability of data and computer systems against threats, attacks, and other forms of vulnerabilities.

2.3. Competency Framework Concept

Competency essentially has various definitions proposed by scholars and practitioners. The concept was first developed by David McClelland (1973), who argued that personal competencies or individual characteristics, such as motives and personality traits, are more significant predictors of employee performance and success than traditional IQ or aptitude tests. The findings of his study were considered controversial at the time because they shifted the focus toward personal competencies as the primary determinant of career success, differing from the psychometric approaches that were more commonly applied. Consequently, McClelland is widely regarded as a leading figure in the development of competency theory within human resource management. The concept of core competencies is frequently used to describe an organization's competitive advantage. In this regard, Richard Boyatzis and Boyatzis (1982) emphasized that competencies represent the underlying characteristics of individuals that contribute to superior and effective performance.

Zuzana Skorková (2016) summarized various interpretations of the competency concept into two major perspectives: (1) authority and responsibility, in which individuals possess the right to undertake certain actions and competencies are granted externally; and (2) an individual's capability to perform specific activities, referring to the qualities, skills, and abilities required to perform tasks competently. Furthermore, Amy Mooney (2007) concluded that competencies consist of skills, knowledge, and abilities as distinctive characteristics that are visible yet difficult to imitate. In addition, competencies may also be defined as the mobilization of knowledge, actions, and emotions used to create value (Bendassolli et al., 2016). From a strategic perspective, these competencies may generate sustainable competitive advantages, thereby making it important to develop them within structured frameworks or knowledge models.

Prior to the 1990s, competency studies primarily focused on observing individual competencies, which were generally interpreted as skills required to accomplish particular tasks or jobs. During the second phase of development (post-1990s), the concept of competency evolved toward the creation of competency models or frameworks within organizations. In the third phase (continuing to the present day), the primary focus has shifted toward identifying the core competencies necessary to achieve sustainable competitive advantage for organizations (Skorková, 2016). In this context, competencies may be utilized as instruments for assessment, selection, training and development, as well as succession planning for specific positions, because they explain the knowledge, capabilities, and characteristics required to perform organizational functions effectively and efficiently (Usman et al., 2023). Moreover, the competency-based approach is highly suitable for identifying individual potential in achieving efficient performance, thereby contributing positively to organizational performance.

Competency may also be applied as a conceptual foundation for developing the characteristics of cyber intelligence capabilities required to address various threats in cyberspace. In this regard, competency refers to the interrelationship among variables within organizational management studies, enabling the formulation of competency frameworks related to cyber intelligence. Such frameworks are considered effective instruments for identifying the expertise and qualifications necessary for organizational

development, particularly in the contexts of recruitment, training, and decision-making processes (Staškeviča, 2019; Daniali et al., 2022). Within the context of cyber intelligence, the participation of individuals, experts, and stakeholders, as well as integration among them, is necessary for developing a comprehensive competency framework. Efforts to establish such a framework may include building a shared consensus and common understanding regarding cyber intelligence competencies, as well as implementing systematic and scientific processes for identifying and defining those competencies.

3. Method

This study employed a qualitative research method using a descriptive-analytical approach. The research aimed to provide a comprehensive description and explanation of the phenomena related to cyber intelligence and competency frameworks. According to Sugiyono (2020), qualitative research methods are used to examine natural settings in which the researcher acts as the primary instrument, data collection techniques involve triangulation, data analysis is conducted inductively, and the main focus lies in understanding meaning based on the obtained data rather than generating generalizations. Meanwhile, the descriptive-analytical approach emphasizes the collection of data in the form of words or images rather than numerical data. The collected data are subsequently analyzed and described systematically in order to facilitate understanding by readers (Bogdan and Biklen, 1982, as cited in Sugiyono, 2020).

The focus of this study is to provide an understanding of cyber intelligence frameworks and to develop a competency framework for cyber intelligence professionals in Indonesia, encompassing the various competencies required in the field. Data collection was conducted through a literature review approach, in which data were obtained from books, scientific journals, research documents, and other relevant literature related to the research object. The collected data were then analyzed using a descriptive-analytical approach through three stages: data reduction based on the selection of relevant references from the literature review, data presentation in the form of narrative text and visual descriptions, and conclusion drawing. Considering the broad range of data sources collected, the qualitative research design employed in this study was inherently flexible and adaptable throughout the research process until valid and relevant data were obtained for the purposes of data analysis.

4. Results and Discussion

The intelligence approach employed to address cyber threats over the last decade has become increasingly essential. As explained by Uthoff (2015), cyber intelligence should now be regarded as an integral component of the intelligence domain due to the growing utilization of information and communication technologies. This idea was initially promoted by members of the international cybersecurity community, consisting of representatives from supranational institutions and agencies, public institutions, private organizations, and academics (Bonfanti, 2018). Nevertheless, there is still no universally accepted definition of the term “cyber intelligence,” primarily because scholarly studies specifically dedicated to formulating such a definition remain relatively limited. In general, cyber intelligence is used to convey the idea of broader and higher-quality knowledge regarding actual or potential conditions within cyberspace that may threaten an organization (Bonfanti, 2017).

Based on the conceptual framework proposed by Matteo Emanuele Bonfanti (2018), the term cyber intelligence may be distinguished into two meanings: a narrow interpretation and a broad interpretation. Cyber intelligence in the narrow sense, or stricto sensu, refers to knowledge generated through a series of analytical processes applied to valuable information collected both “within” and “through” cyberspace. From this perspective, cyber intelligence is not solely intended to address cyber threats, but may also be utilized in decision-making processes for governments, private sectors, and academic institutions. Consequently, cyber intelligence can support policymaking, strategic planning, foreign affairs, risk management, and strategic communication across various sectors, including those beyond the cybersecurity context.

In contrast, cyber intelligence in the broad sense, or lato sensu, refers to intelligence activities encompassing all aspects, including those “outside” the cyber domain itself. In this context, cyber intelligence may originate from any intelligence discipline capable of providing relevant and valuable knowledge, regardless of the source, method, or medium utilized. Thus, cyber intelligence may be produced through combinations of various intelligence disciplines, including Open Source Intelligence (OSINT),

Signals Intelligence (SIGINT), Geospatial Intelligence (GEOINT), Social Media Intelligence (SOCMINT), and Human Intelligence (HUMINT). From this perspective, cyber intelligence is understood more as an analytical practice rather than a standalone discipline. This practice relies on information gathered through other intelligence disciplines with the purpose of providing decision-makers with strategic information regarding issues within cyberspace.

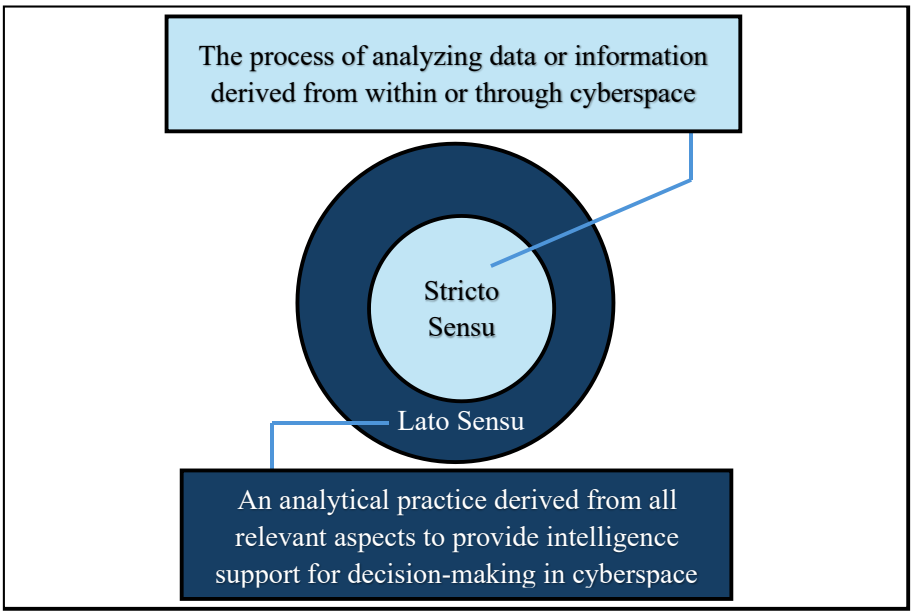

Figure 2. Cyber Intelligence in the Broad and Narrow Sense

A clear understanding of cyber intelligence is particularly important within the context of the state. Such understanding may assist stakeholders in maintaining consistency in decision-making processes related to cyber intelligence, including policy formulation, legal frameworks, operational activities, and other strategic matters. This understanding should be grounded in a strong conceptual definition through the establishment of a cyber intelligence framework. Such a framework functions to organize, manage, and integrate various conceptual differences and ideas related to cyber intelligence in order to provide a comprehensive understanding of the field.

4.1. Cyber Intelligence Framework

The increasing importance of cyber intelligence has made it imperative for states, as primary actors in international security, to possess strong capabilities in mastering information and communication technologies effectively. This is particularly important considering that cyberspace may serve as a source of potential threats and vulnerabilities capable of affecting state sovereignty and national resilience. In this context, cyber intelligence can reasonably be regarded as a strategic asset for the protection of national interests and national security (Astarini & Rofii, 2021). This view is consistent with the argument proposed by Borum et al. (2015), who stated that cyber intelligence may be utilized to detect increasingly complex cyber threats affecting both public and private sectors. For defense and national security institutions, cyber intelligence relates to knowledge generated through the processing and analysis of data and information, which is subsequently used by decision-makers to address cyber threats effectively and efficiently.

In Indonesia, cyber intelligence governance is still considered insufficiently coordinated and tends to remain sectoral or partial in nature, resulting in cybersecurity management that has not yet become fully integrated or comprehensive (Astarini & Rofii, 2021). In this regard, the implementation of cyber intelligence practices constitutes one of the key factors in establishing optimal cyber intelligence governance and is expected to function as an instrument for safeguarding national interests and national security from cyber threats. In order to achieve integrated and comprehensive cyber intelligence governance, a thorough and clear understanding of the cyber context is required. One strategic effort that should be undertaken by stakeholders in Indonesia is the development of a conceptual framework for cyber

intelligence that can serve as a common reference in formulating effective and efficient cyber intelligence governance mechanisms.

The conceptual understanding of cyber intelligence proposed by Matteo Emanuele Bonfanti (2018) may serve as an alternative approach for developing a cyber intelligence framework in Indonesia. Accordingly, cyber intelligence may be understood as a comprehensive concept encompassing activities of collection, processing, evaluation, analysis, integration, and interpretation of data or information available "within," "through," and/or "outside" the cyber domain as a strategic basis for decision-making in cyberspace. In general, cyber intelligence may be implemented at strategic, tactical, or operational levels (Borum, 2014), although there are no strict rules regarding what specific elements should be categorized within each level. Furthermore, despite the existence of these academic classifications, there are often no clear boundaries in practice, and the different levels frequently overlap and are implemented simultaneously.

Strategic cyber intelligence generally focuses on long-term objectives by examining trends related to actual or potential threats and exploring opportunities to mitigate such threats (Bonfanti, 2018). Strategic cyber intelligence also encompasses macro-level threats, including political, social, and economic factors that may influence organizations in identifying threat actors, their objectives, and their operational methods (Borum et al., 2015). Tactical cyber intelligence, on the other hand, concerns activities occurring within networks, including assessments of organizational strengths and vulnerabilities, as well as the tactics, techniques, and procedures employed by threat actors (Intelligence and National Security Alliance, 2015). Operational cyber intelligence consists of knowledge regarding immediate and proximate threats to an organization, thereby supporting day-to-day operations. At this level, cyber intelligence primarily examines internal processes and vulnerabilities within the organization itself (Mattern et al., 2014).

Based on existing literature, a team of experts and academics affiliated with the Software Engineering Institute (SEI) at Carnegie Mellon University introduced a cyber intelligence framework. The SEI model differs from traditional intelligence cycles because of its terminology, non-linear logic, and broader analytical significance. The framework consists of the following components:

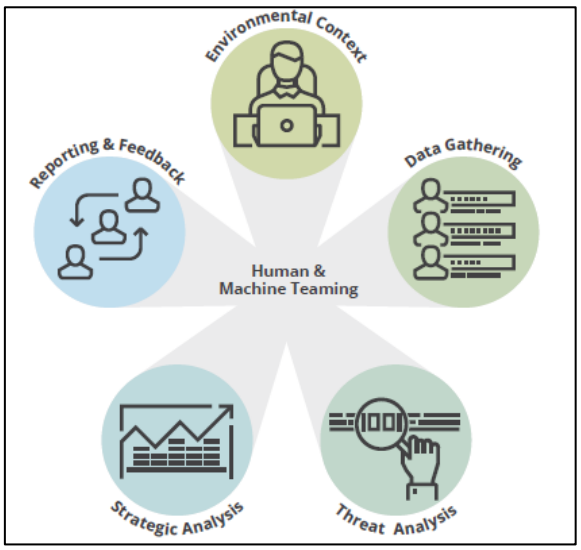

Figure 3. Cyber Intelligence Framework

a. "Environmental context," referring to the importance of organizational understanding regarding threats, risks, and opportunities targeting both internal and external organizational networks and operations;

b. "Data collection," conducted both automatically and manually while considering organizational needs and environmental conditions;

c. "Threat analysis," encompassing operational and tactical analyses related to cyber threats in order to support decision-making processes;

d. "Strategic analysis," referring to comprehensive and anticipatory analyses of threats, risks, and opportunities across various dimensions to improve executive-level decision-making concerning vital organizational interests;

e. "Reporting and feedback," involving the distribution of cyber intelligence products to decision-makers as well as the collection of evaluations and feedback regarding organizational performance;

f. "Human-machine collaboration," positioned at the center of the framework as an integration between human analytical intelligence and the computational power and speed of machines capable of automating processes and enhancing capabilities through artificial intelligence (AI).

Referring to the framework above, the SEI version of cyber intelligence shares similarities with the conceptual framework proposed by Bonfanti (2018), particularly in the understanding that analytical practices in cyber intelligence rely on data and information collected from various intelligence disciplines. In this context, analytical practices in cyber intelligence are divided into two major functions, namely threat analysis and strategic analysis. These functions illustrate that cyber intelligence processes pursue both "narrow" objectives involving tactics, techniques, and procedures, as well as "broader" objectives encompassing all aspects related to the cyber domain. The interdependent and continuous relationships among the six variables may be explained as follows:

a. Data collection must be based on the identification of environmental conditions influenced by organizational decisions derived from the cyber intelligence received.

b. Strategic analysis and threat analysis mutually reinforce analytical practices in order to generate comprehensive intelligence products capable of providing recommendations for tactical and operational actions as well as strategic responses to cyber-related issues.

c. Reporting and feedback function as mechanisms of control and evaluation for decision-makers to ensure that analytical practices align with organizational objectives, directions, and environmental conditions.

d. The combination of human performance and machine capabilities in data collection and analysis processes may produce timely, accurate, and actionable intelligence relevant to ongoing cyber issues.

In other literature, the Forum of Incident Response and Security Teams (FIRST) introduced a cyber intelligence framework that combines the traditional intelligence cycle (Direction, Collection, Processing, Analysis, Dissemination, and Feedback) with the F3EAD cycle (Find, Fix, Finish, Exploit, Analyze, and Disseminate) as an alternative model for understanding cyber intelligence processes. The relationship between the two cycles is illustrated as follows:

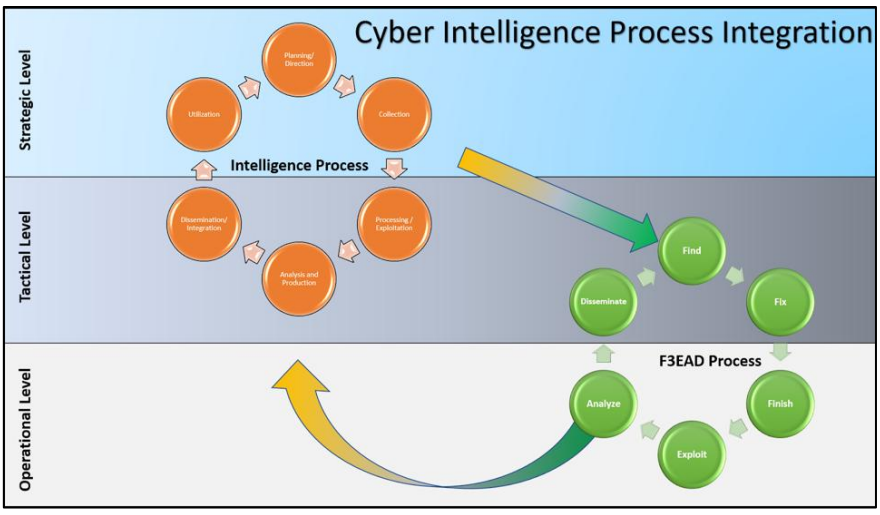

Figure 4. Cyber Intelligence Process according to FIRST Cyber Threat Intelligence SIG

Based on this model, the traditional intelligence cycle and the F3EAD cycle are utilized simultaneously within cyber intelligence processes to fulfill both tactical and strategic organizational requirements. The model is visualized as interconnected gears rotating together within the cyber intelligence process, particularly at the intersection between the "collection" phase of the traditional intelligence cycle and the "find" phase of the F3EAD cycle. Although this model provides an alternative understanding of cyber intelligence practices, it does not comprehensively explain how such practices are implemented in relation to the broader body of knowledge within the cyber domain.

4.2. Developing a Competency Framework for Cyber Intelligence Professionals in Indonesia

Cyber intelligence plays a highly important role in efforts related to the early detection and prevention of cyber threats originating from various sources or threat actors. In addition to the importance of understanding cyber intelligence as a new dimension within the discipline of intelligence studies, it is also necessary to develop a clear cyber intelligence framework by taking into account the issues and challenges faced by the state. Such efforts must also be accompanied by strategies to prepare qualified human resources, institutional infrastructure, budgetary support, and technological capabilities in order to strengthen the role of cyber intelligence in national defense and security (Astarini & Rofii, 2021). The enhancement of cyber intelligence capabilities is not limited solely to intelligence agencies, military institutions, law enforcement bodies, or national security instruments, but also extends to quasi-public entities such as public service companies, financial institutions, and other strategic organizations (INSA Cyber Intelligence Task Force, 2015). Therefore, a mechanism for developing human resource competencies within cyber intelligence institutions is required, based on a competency model or framework specifically designed for cyber intelligence.

In Indonesia, there are currently no adequate academic manuscripts or government regulations capable of providing a comprehensive explanation regarding cyber intelligence competencies, particularly those supporting cyber threat detection tasks in the context of national security. Although the Badan Siber dan Sandi Negara (BSSN) has established regulations concerning technical competencies in cyber intelligence through BSSN Regulation No. 11 of 2020, the implementation of this regulation is limited to the internal environment of BSSN and does not apply to other institutions. This condition indicates that cyber intelligence governance in Indonesia remains insufficiently integrated. Furthermore, the absence of comprehensive regulations concerning cyber intelligence competencies may affect both the processes and outcomes of cyber intelligence practices themselves, considering that each stage of cyber intelligence operations requires specific expertise and capabilities in order to function optimally.

In order to develop a competency framework for cyber intelligence in Indonesia, references from academics and practitioners in other countries are required. The United States, for example, has extensively developed frameworks related to cyber intelligence, including conceptual models, operational practices, and competency standards required to support cyber intelligence activities. As an example, the National Institute of Standards and Technology (NIST), together with other United States government institutions, has collaborated with scientific and professional communities to establish workforce requirements and standards within the cybersecurity domain. This initiative provides the foundation for the establishment of specific competency domains for cyber intelligence, namely: (1) "identification," referring to activities related to managing cybersecurity risks; (2) "protection," referring to security measures for critical infrastructure services; (3) "detection," referring to activities aimed at accurately identifying cybersecurity-related incidents; (4) "response," referring to appropriate actions taken against detected cybersecurity incidents; and (5) "recovery," referring to activities intended to restore capabilities following cybersecurity-related incidents (INSA Cyber Intelligence Task Force, 2015).

Subsequently, NIST formulated the National Cybersecurity Workforce (NCW) Framework, which offers significant guidance for developing cyber intelligence training and educational requirements. The NCW Framework includes 31 specialization areas for cybersecurity personnel organized into seven categories, one of which is the "analysis" category that serves as a reference for classifying cyber intelligence functions. Within the "analysis" category, four specialization areas are identified: threat analysis, all-source intelligence analysis, exploitation analysis, and target analysis we can see in Figure 5.

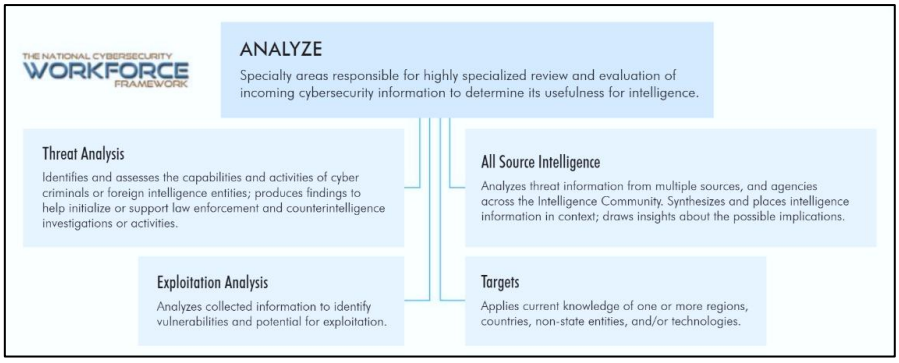

Figure 5. "Analysis" Category in the NCW Framework

In addition to the two cyber intelligence competency frameworks discussed above, researchers at the Software Engineering Institute (SEI) of Carnegie Mellon University have also conducted a research initiative entitled Cyber Intelligence Tradecraft Project (CITP) since 2012. The project aims to define the core competencies and skills that characterize a professional cyber intelligence analyst. Unlike the NCW Framework, the CITP conceptualizes cyber intelligence as a discipline composed of core competencies—namely skills that can be learned and developed. These competencies include the categories of "critical thinking," "data collection and examination," "communication and collaboration," "computing fundamentals," "information security," and "technical exploitation."

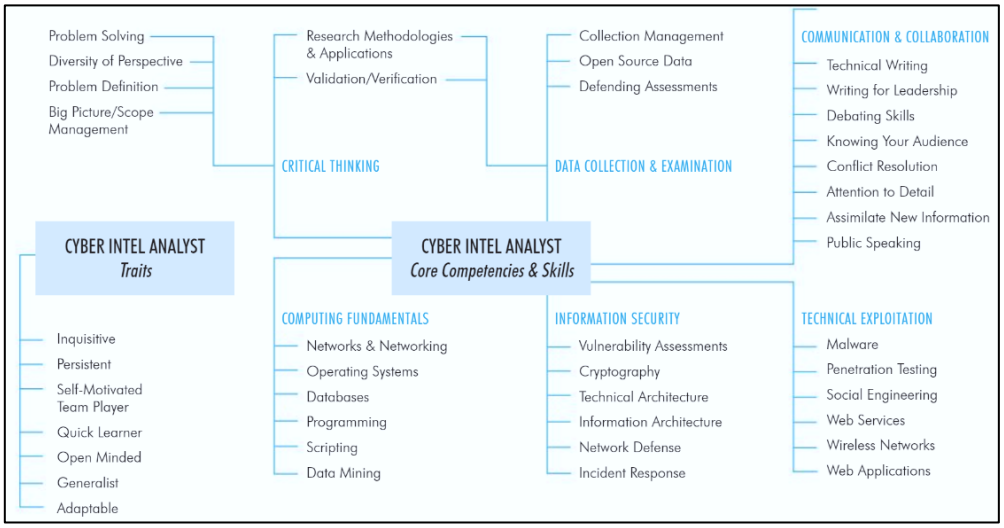

Figure 6. Core Competencies and Cyber Intelligence Capabilities

The findings of the Cyber Intelligence Tradecraft Project (CITP) clearly classify both analytical and technical domains, commonly referred to as "soft skills" and "hard skills," which are required for cyber intelligence professionals to perform effectively and efficiently. In contrast, the NCW Framework primarily refers to several relevant cyber intelligence functions but does not specifically distinguish the foundational categories of analytical skills. Since cyber intelligence is predominantly considered a technical discipline, professionals in this field are required to conduct research, develop hypotheses, manage new knowledge, formulate and solve complex problems, provide rational and logical judgments, and communicate effectively through written reports, oral presentations, and visual representations.

Based on the three cyber intelligence competency frameworks discussed above—namely the National Institute of Standards and Technology (NIST), the National Cybersecurity Workforce (NCW) Framework, and the Cyber Intelligence Tradecraft Project (CITP)—the Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force formulated an integrated competency-based framework in 2015. This framework encompasses technical competencies, analytical competencies, knowledge and information management competencies, contextual domain competencies, as well as communication and organizational competencies as we can see at Figure 7.

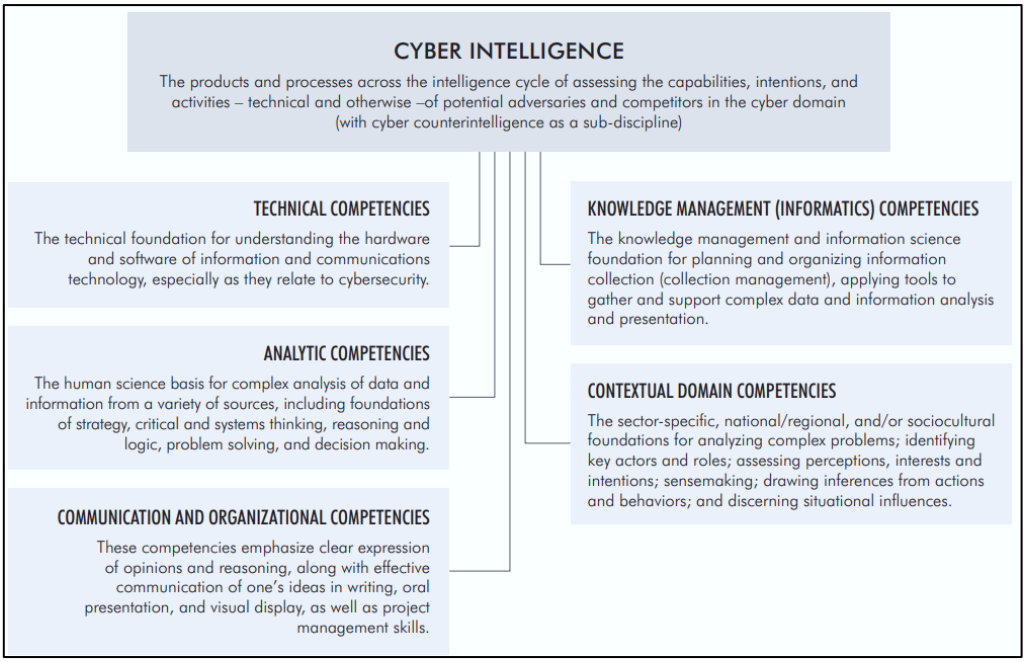

Figure 7. Cyber Intelligence Competencies

Referring to the five cyber intelligence competencies formulated by the Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force (2015), the Indonesian government may formulate specific regulations or academic studies related to these competencies by considering domestic cybersecurity dynamics as well as broader geopolitical conditions. The following cyber intelligence competencies are considered relevant for developing highly capable human resources in addressing cyber threats in Indonesia:

a. Technical Competency

Fundamental technical understanding of information and communication technology hardware and software is essential, particularly in relation to cybersecurity. This includes knowledge of the operational mechanisms of workstations, networks, and operating systems, as well as vulnerabilities and exploitations involving both technical and human factors. Furthermore, it is important to understand the principles of information security and the tools used in cybersecurity practices, such as risk assessment, intrusion detection, cryptography, and incident response mechanisms. The implementation of these competencies may assist the Indonesian government in strengthening cyber resilience and responding to cyber threats effectively and efficiently.

b. Analytical Competency

A comprehensive understanding of the social sciences constitutes an important foundation for conducting complex analyses of data and information derived from multiple sources. This competency includes knowledge related to strategy, systems thinking, logic, and decision-making processes. The primary focus lies in the formulation and testing of hypotheses, as well as the application of appropriate analytical methodologies, both qualitative and quantitative. It also involves adherence to ethical and professional standards in selecting and utilizing analytical methods. Within the context of cyber intelligence, analysts must consider cultural, leadership, behavioral, and background aspects of the actors involved. By incorporating these social and scientific dimensions, the Indonesian government may improve its understanding of cyber threats and formulate more appropriate responses to address them.

c. Knowledge and Information Management Competency

The application of knowledge management and information science principles constitutes a key element in planning and collecting information. This competency includes the development and utilization of tools capable of gathering complex data from multiple sources while supporting information analysis processes. The visualization of information is also important in facilitating

data comprehension. In addition, understanding, utilizing, and evaluating various information storage and retrieval systems are essential components of this process. By strengthening competencies in knowledge management and information science, the Indonesian government may improve the efficiency and effectiveness of managing cyber intelligence information, thereby enhancing its capability to address cyber threats.

d. Contextual Domain Competency

The application of competencies in analyzing complex problems is not limited to sector-specific or national and regional understanding, but also includes psychosocial and sociocultural foundations. Understanding these dimensions is important for identifying key actors and stakeholders, evaluating perceptions, interests, and objectives, and interpreting observed actions and behaviors. Foreign language proficiency and regional or cultural understanding are also required within strategic, operational, and tactical contexts. By improving understanding of these aspects, cyber intelligence analysts in Indonesia may produce deeper and more accurate analyses that support efforts to address complex challenges within the cyber intelligence domain.

e. Communication and Organizational Competency

The application of communication and organizational skills is highly important in managing and implementing projects related to cyber intelligence activities. The ability to present arguments and reasoning clearly, as well as communicate effectively through written reports, oral presentations, and visual representations, is essential to ensure that cyber intelligence information and ideas are properly understood by all relevant stakeholders. In addition, project management capabilities are required to plan, organize, evaluate, motivate, coordinate, and control resources, processes, and outputs in order to achieve specific objectives related to cyber intelligence. By recognizing and developing these competencies, the implementation of cyber intelligence in Indonesia may become more effective and efficient, thereby contributing more significantly to overall cybersecurity resilience

5. Conclusion

The intelligence approach in addressing cyber threats has become an essential strategic instrument in safeguarding national interests and national security. In the Indonesian context, cyber intelligence governance remains insufficiently integrated due to the absence of comprehensive academic frameworks and government regulations that may serve as fundamental references for the implementation of cyber intelligence practices. Based on existing literature, various cyber intelligence frameworks may be adopted as references for developing an integrated and effective cyber intelligence governance system in Indonesia. In particular, the SEI framework developed by the Software Engineering Institute of Carnegie Mellon University, as well as the FIRST Cyber Threat Intelligence SIG model, provide valuable conceptual and operational approaches for strengthening cyber intelligence practices through comprehensive analytical processes and the integration of traditional intelligence cycles with the F3EAD model.

Furthermore, the absence of standardized cyber intelligence competency guidelines in Indonesia may negatively affect the effectiveness of cyber intelligence processes and outcomes, considering that each stage requires specific expertise and professional capabilities in order to function optimally. By referring to the competency frameworks developed by the National Institute of Standards and Technology (NIST), the National Cybersecurity Workforce (NCW) Framework, the Cyber Intelligence Tradecraft Project (CITP), and the integrated framework formulated by the Intelligence and National Security Alliance (INSA) Cyber Intelligence Task Force, the Indonesian government may establish a comprehensive cyber intelligence competency framework to strengthen domestic cyber intelligence capabilities.

The proposed competency framework should encompass five core competencies, namely technical competency, analytical competency, knowledge and information management competency, contextual domain competency, and communication and organizational competency. These competencies need to be formulated clearly and specifically by considering domestic cybersecurity dynamics as well as broader international geopolitical developments. In addition, collaboration among government institutions, academics, cybersecurity experts, and practitioners is necessary to formulate conceptual frameworks, competency standards, regulations, and education and training mechanisms capable of strengthening professional cyber intelligence governance in Indonesia. Through these efforts, Indonesia is expected to

develop an integrated, adaptive, and professional cyber intelligence system capable of responding effectively to the increasingly complex challenges and threats within cyberspace.

References

Astarini, D. R. S., & Rofii, M. S. (2021). SIBER INTELIJEN UNTUK KEAMANAN NASIONAL. Jurnal Renaissance, 6(1). https://doi.org/10.53878/jr.v6i1.143

Badan Siber dan Sandi Negara. (2020). BSSN Regulation Number 11 of 2020 concerning the Dictionary of Technical Competencies in Cybersecurity and Cryptography. Government of Indonesia.

Bendassolli, P. F., Borges-Andrade, J. E., Gondim, S. M., & Makhamed, Y. M. (2016). Performance, self-regulation, and competencies of entrepreneurs in Brazilian creative industries1. Psicologia: Teoria e Pesquisa, 32(Special Issue). https://doi.org/10.1590/0102-3772e32ne221

Bonfanti M. (2017). Another -Int on the Horizon? Cyber-Intelligence is the New Black. National Institute for Intelligence Studies, 17–18, 127–156.

Bonfanti, M. E. (2018). Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice. Cyber, Intelligence, and Security, 2(1).

Borum R. (2014). Getting 'Left of the Hack': Honing Your Cyber Intelligence Can Thwart Intruders. InfoSecurity Professional, 26–29.

Borum R., Felker J., Kern S., Dennesen K., & Feyes T. (2015). Strategic Cyber Intelligence. Information and Computer Security, 23(3).

Boyatzis, E., & Richard. (1982). The competent manager : a model for effective performance / Richard E.Boyatzis. Review Hugh Gunz Source: Strategic Management Journal, 4(4).

Brantly, A. (2013). Defining the role of intelligence in cyber: A hybrid push and pull. In Understanding the Intelligence Cycle. https://doi.org/10.4324/9780203558478

Caplan, N. (2013). Cyber War: the Challenge to National Security. Global Security Studies, 4(1).

Daniali, S. M., Barykin, S. E., Khortabi, F. M., Kalinina, O. V., Tcukanova, O. A., Torosyan, E. K., Poliakova, S., Prosekov, S., Moiseev, N., & Senjyu, T. (2022). An Employee Competency Framework in a Welfare Organization. Sustainability (Switzerland), 14(4). https://doi.org/10.3390/su14042397

Djoyonegoro, N. (2018). Intelijen di Era Digital: Prospek dan Tantangan Membangun Ketahanan Nasional. CMB Press.

Ettinger, J., Galyardt, A., Gupta, R., DeCapria, D., Kanal, E., Klinedinst, D. J., Shick, D., Perl, S. J., Dobson, G. B., Sanders, G., Costa, D. L., Rogers, L., Barmer, H., Kane, J., Evans, H., Mellinger, A. O., & Brandon, E. (2019). Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States.

Graham, S. (2009). Disrupted cities: When infrastructure fails. In Disrupted Cities: When Infrastructure Fails. https://doi.org/10.4324/9780203894484

INSA Cyber Intelligence Task Force. (2015, September). Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats. Https://Issuu.Com/Insalliance/Docs/Insa_cyber_intel_preptalent/1?E=6126110/15292430.

Intelligence and National Security Alliance. (2015, December 16). Tactical Cyber Intelligence. Https://Issuu.Com/Insalliance/Docs/Insa_tacticalcyber.

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational Levels of Cyber Intelligence. International Journal of Intelligence and CounterIntelligence, 27(4). https://doi.org/10.1080/08850607.2014.924811

McClelland, D. C. (1973). Testing for competence rather than for "intelligence". The American Psychologist, 28(1). https://doi.org/10.1037/h0034092

Mooney, A. (2007). Core Competence, Distinctive Competence, and Competitive Advantage: What Is the Difference? Journal of Education for Business, 83(2). https://doi.org/10.3200/JOEB.83.2.110-115

Prunckun, H. (2015). Scientific Methods of Inquiry for Intelligence Analysis (J. Goldman, Ed.; 2nd ed.). Rowman & Littlefield.

Republic of Indonesia. (2011). Law Number 17 of 2011 concerning State Intelligence. Government of Indonesia.

Rahim, A. S., Widodo, P., Reksoprodjo, A. H. S., & Alsodiq, A. (2023). Identify Cyber Intelligence Threats in Indonesia. International Journal Of Humanities Education and Social Sciences (IJHESS), 3(1). https://doi.org/10.55227/ijhess.v3i1.426

Septasari, D. (2023). The Cyber Security and The Challenge of Society 5.0 Era in Indonesia. Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E), 5(2). https://doi.org/10.30604/jti.v5i2.231

Skorková, Z. (2016). Competency Models in Public Sector. Procedia - Social and Behavioral Sciences, 230. https://doi.org/10.1016/j.sbspro.2016.09.029

Staškeviča, A. (2019). The Importance of Competency Model Development. Acta Oeconomica Pragensia, 27(2). https://doi.org/10.18267/j.aop.622

Usman, A., Che-Ahmad, A., & Abdulmalik, S. O. (2023). The Role of Internal Auditors Characteristics in Cybersecurity Risk Assessment in Financial-Based Business Organisations: A Conceptual Review. International Journal of Professional Business Review, 8(8). https://doi.org/10.26668/businessreview/2023.v8i8.2922

Uthoff, C. (2015). Strategic Cyber Intelligence: An Examination of Practices across Industry, Government, and Military. In Current and Emerging Trends in Cyber Operations. https://doi.org/10.1057/9781137455550_13

Warner, M. (2007). Wanted: A Definition of Intelligence — Central Intelligence Agency. Studies in Intelligence.