Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

ORGANIZATIONAL READINESS OF THE DIRECTORATE OF CYBER INVESTIGATION OF THE METRO JAYA POLICE IN IMPLEMENTING THE SECI MODEL IN HANDLING CYBERCRIME

Sopian Rahmadyanto[1a*], Lina Miftahul Jannah[2b]

[12] Universitas Indonesia, Jakarta, Indonesia

[a]*E-mail: hominem.fortinatum@gmail.com*
[b]*E-mail: linamjannah@gmail.com*

(*) Corresponding Author
hominem.fortinatum@gmail.com

ARTICLE HISTORY
Received : 20-04-2026
Revised : 07-05-2026
Accepted : 15-06-2026

KEYWORDS
Organizational Readiness;
Knowledge Sharing;
SECI Model;
Cybercrime;

ABSTRACT
The development of globalization and digital transformation has increased the complexity of cybercrime which demands that law enforcement organizations have adaptive and sustainable knowledge capacity. However, the acceleration of the development of cybercrime modes is often not balanced by the readiness of organizations to manage and transform knowledge as a strategic resource. This study aims to analyze the readiness of the Directorate of Cyber Investigation of the Metro Jaya Police in implementing the SECI Model (*Socialization, Externalization, Combination,* and *Internalization*) in handling cybercrime. The research uses a qualitative approach with a literature study method sourced from scientific journals, books, regulations, institutional documents, and various relevant publications that are analyzed descriptively. The results of the study show that the Directorate of Cyber Investigation of the Metro Jaya Police has been ready for every dimension of the SECI Model through the practice of knowledge sharing, documentation of case handling experience, integration of investigative information, and work experience-based learning. However, this readiness still faces challenges in the form of budget limitations, competency gaps and knowledge sharing culture in human resources, and the lack of formal institutionalization of knowledge management policies. This research implies the importance of strengthening policies, human resource capacity building, and sustainable organizational support to build knowledge-based law enforcement organizations that are adaptive to cybercrime dynamics.

INTRODUCTION

Global developments marked by the intensification of globalization and the acceleration of digital technology have formed new configurations in various aspects of life, including in the security dimension. Globalization is no longer just understood as a process of economic and political integration between countries, but has developed into a

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

multidimensional phenomenon that encourages the formation of *a borderless world*, where the flow of information, communication, and social interaction takes place quickly and simultaneously. Technological advances such as the internet, artificial intelligence, cloud computing, and big data analytics have accelerated this transformation, creating a digital space that is becoming a new arena for human activity. However, behind the opportunities generated, this development also gives birth to significant challenges, especially in the form of the emergence (Abdillah et al., 2024; Khaldun et al., 2020) *of cybercrime* that is increasingly complex, adaptive, and transnational.

Cybercrime is evolving as a logical consequence of society's increasing dependence on digital technology. Various forms of crime such as system hacking, data theft, online fraud, and ransomware attacks show that cyberspace has become a new medium for criminal activities with different characteristics from conventional crimes. These crimes are not only difficult to detect, but they also involve cross-border networks with a high level of technological sophistication. In this context, the challenges faced by law enforcement institutions are no longer linear, but complex, dynamic, and require an adaptive and knowledge-based approach. (Arsawan et al., 2022)

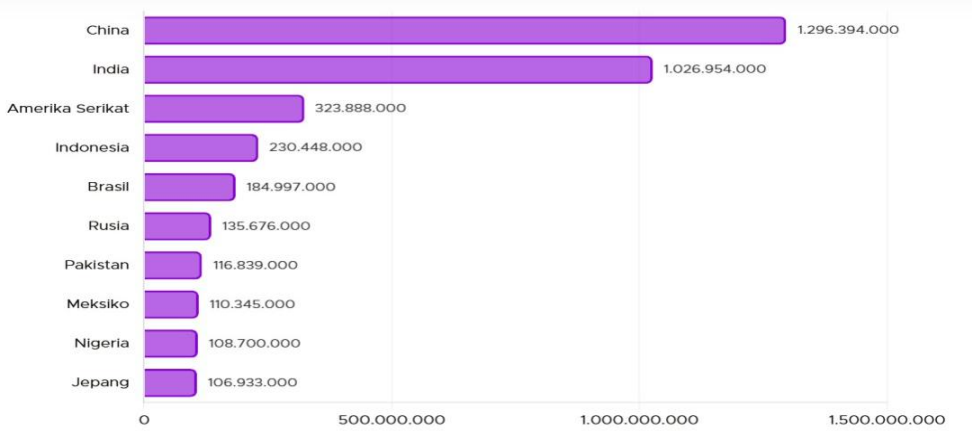

Figure 1. Statistics of the 10 Countries with the Largest Internet-Connected Population
Source: https://data.goodstats.id

In the Indonesian context, the increase in people's digital activities in line with national digital transformation has also encouraged the escalation of cybercrime threats. Indonesia is one of the countries with the fourth largest internet users in the world. From this perspective, Indonesia faces opportunities as well as challenges with the development of digital technology and the internet. Both in the social, political and economic dimensions, such as political provocations, hoaxes, SARA, hate speech, radical ideology, terrorism, hacking, data theft, online fraud, and other crimes in cyberspace. In Ginanjar's research in 2022, based on a survey conducted by the Indonesian Internet Service Providers Association (APJII) in 2022, more than 77.02% of Indonesians use the internet. This means that there are 210,026,769 people out of a total of 272,682,600 Indonesians who use internet connections. This has increased its users during the COVID-19 pandemic, which focuses on the use of internet technology to replace face-to-face activities. (Arnell & Faturoti , 2023) (Ginanjar, 2022)

As a metropolitan area with a high level of economic and digital activity, the jurisdiction of Polda Metro Jaya is one of the centers of vulnerability as well as the *main locus* for handling cybercrime. The Directorate of Cyber Investigation of the Metro Jaya Police has a strategic role as the front line in law enforcement in the digital space. However, the dynamics of the increasingly massive development of cybercrime require the development of human resources in organizations that not only focus on technological aspects, but also on awareness rather than human resources (HR) as the main actors in the investigation and case handling process that are aware of the importance of knowledge. It is in this context that human resource development becomes the main focus as awareness of the importance of knowledge. Related to this, the development of human resources at the Directorate of Investigation of

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

the Metro Jaya Police, which is the main focus, requires organizational readiness to be able to open awareness of the importance of knowledge. Knowledge as an asset is an important paradigm for the adaptability of an organization to the dynamic environment in today's era. (Dinda, 2024) (Omar & Desa, 2024) (Mak & Hong, 2020)

Organizational readiness to increase human resource capacity in this context cannot be narrowly interpreted as improving technical skills alone, but rather includes adaptive, analytical, and continuous learning capabilities in the face of the evolution of cybercrime. Effective human resources in handling cybercrime must be able to understand changing crime patterns, master digital investigation technology, and integrate various sources of information in the law enforcement process. Therefore, a conventional approach based on formal training alone is no longer adequate. A mechanism is needed that allows knowledge transfer or (Rimone et al., 2024) *knowledge sharing* dynamically and continuously within the organization. (Omar & Desa, 2024)

Efforts to build an organization in its readiness to become a knowledge-based organization basically do not only depend on the existence of information technology or organizational documentation alone. A more important factor is the readiness of the organization to adopt and implement mechanisms of knowledge creation and transfer in a systematic manner. The public administration and knowledge management literature shows that many knowledge management programs fail not because of weaknesses in the concepts used, but rather because organizations do not have adequate readiness to implement them. Organizational readiness reflects the organization's ability to provide resources, build a work culture that supports learning, prepare adaptive leadership, and develop policies that are able to encourage organizational behavior change. Thus, the success of the implementation of a knowledge management model is largely determined by the level of readiness of the organization itself. (Dirani et al., 2021) (Miller et al., 2023) (Makbul et al., 2023)

Within this framework, *knowledge sharing* emerged as a strategic approach in developing human resources. *Knowledge sharing* allows for the exchange of knowledge, experience, and expertise between individuals and units in the organization, thus forming an adaptive collective learning system. The concept of *knowledge creation* put forward by Nonaka and Takeuchi through the SECI Model (*Socialization, Externalization, Combination, Internalization*) provides a strong theoretical foundation in understanding how knowledge is created, developed, and distributed in organizations. Through this process, knowledge that is *tacit* can be transformed into *explicit* and vice versa, thus strengthening the capacity of the organization in responding to changes in the external environment. (Zheyu et al., 2021)

In the context of the Directorate of Cyber Investigation of the Metro Jaya Police, the implementation *of knowledge sharing* with the SECI Model not only functions as a managerial tool, but also as a means of strengthening development-oriented organizational functions in the Human Resources of the Metro Jaya Regional Police. This human resource development emphasizes the importance of making the organization a *knowledge-based institution*, in this context that learning, collaboration, and knowledge exchange are integral parts of the work process. Thus, the development of the human resources of the Metro Jaya Regional Police has an impact not only on improving individual competence, but also on improving overall institutional capabilities, including in terms of response speed, investigation accuracy, and adaptability to evolving cybercrime modes. (Woods et al., 2025) (Tobing et al., 2024)

However, in practice, there are still various challenges in developing knowledge sharing-based human resources , especially in the SECI Model. One of the main problems is the lack of optimal knowledge sharing mechanisms within the organization, which is often hampered by organizational culture factors, limitations of knowledge management systems, and the phenomenon of information system silos between units. In addition, the dynamics of cybercrime, which develops faster than the organizational learning process, are also a challenge in itself. This condition creates a gap between the needs of human resource capacity and the actual capabilities they have, thus having an impact on the effectiveness of handling cybercrime.

The implementation of the SECI Model requires adequate organizational readiness at every stage of knowledge conversion. The *socialization stage* requires a culture of knowledge sharing and intensive interaction between members of the organization. The *externalization* stage requires the organization's ability to document individual experiences and knowledge into a widely accessible form. The *combination* stage requires a system that is able to

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

integrate various available information and knowledge. Meanwhile, the *internalization* stage requires a learning mechanism that allows explicit knowledge to be transformed back into individual competencies. In other words, the implementation of the SECI Model is not only related to the existence of knowledge sharing activities, but also concerns the readiness of the organization in providing conditions that allow the entire process to take place effectively. (Russia et al., 2020)

Based on these conditions, the main issue that needs attention is not solely whether the practice of knowledge sharing has been carried out by the Directorate of Cyber Investigation of the Metro Jaya Police, but the extent to which the organization has the readiness to implement the SECI Model systematically and sustainably. Focusing on the readiness aspect is important because readiness is a prerequisite for the successful implementation of organizational change. Organizations that are not yet ready are likely to experience gaps between policies and practices, while organizations that have a high level of readiness will be better able to internalize changes into the day-to-day work system. Therefore, research on the readiness of the Cyber Investigation Directorate of the Metro Jaya Police in implementing the SECI Model is relevant to provide an overview of the actual condition of the organization, identify challenges to readiness for the implementation of the SECI model, and focus on organizational readiness to face increasingly complex cybercrime challenges in the digital era.

METHOD

This study uses a qualitative approach with a literature study, which aims to analyze Knowledge Management in the Directorate of Polda Metro Jaya with the SECI Model in handling cybercrime. In this case, data is obtained, classified and associated with a *knowledge sharing* theoretical framework approach that focuses on the SECI Model. Research writing uses descriptive writing, with the aim of describing the problem being researched in depth. Data from this study came from secondary sources in the form of scientific journals, publications from the National Police institution, and other relevant data sources. The theoretical framework in this study is used as a tool for readers in understanding the analysis presented by the researcher. (Ilhami et al., 2024)

RESULT AND DISCUSSIONS

The Existing Directorate of Cyber Investigation of the Metro Jaya Police on its Readiness to Implement the SECI Model

From the perspective of modern public administration, the existence of the Directorate of Cyber Investigation (Dissip) is not only interpreted as a work unit of the National Police that functions for law enforcement alone, but more holistically as a knowledge-based public organization. In its demands to accompany the rapid development of technology, Ditsiber is required to have an adaptive capacity in dealing with rapid changes in the strategic environment. Thus, the meaning of the duties, functions, roles and strategic positions of the Directorate of Cyber Investigation is important as a basis for analyzing knowledge management and organizational readiness in dealing with various developments in cybercrime.

The function of the Directorate from the perspective of public administration has three main dimensions, namely the dimension of the law enforcement function, which is oriented to the organization to ensure that every violation of the law in the digital space can be processed in accordance with the provisions of the law. The intelligence and cyber analysis function, which is oriented that Ditsiber is not only reactive, but also carries out the functions of monitoring threat development, identifying crime trends, mapping actors, and risk analysis. In the organizational learning function, the learning context is important in the digital era, because the rapid development of technology causes organizations to continue to update their knowledge and competencies, so that Dissipber is not only a law enforcement organization, but also a learning organization that is able to create, manage and utilize knowledge in a sustainable manner. (Irawan, 2025)

In contrast to conventional investigation units which mostly rely on field investigation capabilities, the Cyber Investigation Directorate operates in a work environment that is heavily influenced by the development of knowledge and technology. The success of handling a cyber case is not only determined by the legal authority of the organization,

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

but also by the ability of personnel to understand the development of digital technology, cyber investigation methods, digital forensic techniques, electronic data analysis, and understanding of changing threat patterns. In other words, the main strategic resource in this organization is not just the technological devices used, but the knowledge possessed by its personnel. (Tabiu et al., 2023)

In the perspective of modern public administration, an organization that operates in a highly dynamic environment assumes that its operational success depends heavily on the ability to create, manage, and utilize knowledge. These characteristics are very relevant to the Directorate of Cyber Investigation of the Metro Jaya Police. Every investigation and investigation process that is carried out is actually a knowledge-based activity. Investigators must be able to identify patterns of digital attacks, understand the techniques used by the perpetrators, interpret electronic evidence, and connect various information scattered in cyberspace to produce accountable legal constructions. (Budhiraja et al., 2024) (Srivastava et al., 2020)

Based on the findings of the study, one of the important characteristics found in the Cyber Investigation Directorate of the Metro Jaya Police is the high dependence of the organization on the knowledge possessed by individuals. The various investigative skills used in handling cases often develop through the direct experience of personnel in handling certain cases. This knowledge is not entirely obtained through formal education, but is formed through a continuous learning process that takes place during the implementation of tasks. As a result, most of the organization's strategic competencies are stored in the form of *tacit knowledge*, which is knowledge inherent in the individual experience, intuition, skills, and understanding of personnel.

This condition shows that the Directorate of Cyber Investigation faces a challenge commonly found in knowledge-based organizations, namely how to ensure that the knowledge possessed by individuals can be converted into organizational assets. In many public organizations, including law enforcement institutions, knowledge is often concentrated in specific personnel who have more experience in the performance of their duties. If the organization does not have an adequate knowledge management mechanism, then this knowledge has the potential to be lost when there is rotation, mutation, promotion, or personnel change. From an organizational perspective, these conditions can cause capacity gaps that have an impact on decreasing organizational effectiveness in facing increasingly complex challenges.

The study shows that the Cyber Investigation Directorate of the Metro Jaya Police has developed various mechanisms to reduce these risks. Briefing activities, leadership direction (AAP), technical discussions, case analysis, case titles and routine evaluations, as well as post-case handling evaluations are forms of activities that allow for the exchange of knowledge between personnel. In addition, the existence of mentoring relationships between senior and junior personnel indicates the organization's awareness that knowledge must be transferred on an ongoing basis to maintain the sustainability of institutional capacity. These findings suggest that organizations have moved toward learning organizational characteristics that place learning as an integral part of operational activities.

From the perspective of knowledge management, this condition has a very important meaning. Nonaka and Takeuchi, explain that the excellence of an organization in the age of knowledge is determined by its ability to create new knowledge through the interaction between *tacit* and explicit knowledge. Organizations that are able to manage these processes effectively will have a higher adaptability than organizations that rely solely on formal procedures and bureaucratic structures. In the context of the Directorate of Cyber Research, adaptability is a very urgent need considering that the development of cybercrime modes takes place much faster than the process of bureaucratic change in general. (Rizki, 2022)

In a more essential context, research shows that the main challenge facing organizations does not lie in the availability of technology alone, but in the ability to manage the knowledge generated from the use of that technology. Many organizations tend to focus on the procurement of digital devices and information systems, but neglect the aspects of knowledge management that are actually at the heart of the organizational learning process. In the context of the Directorate of Cyber Investigation, forensic technology tools, data analysis tools, and digital investigation systems will only provide optimal benefits if they are supported by personnel who are able to understand, develop, and share knowledge obtained through their use. (Oliveira, 2020)

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

The Directorate of Cyber Investigation of the Metro Jaya Police is currently in a very important phase in the process of adapting its organization to the existing dynamics. This organization can no longer be seen solely as an authority-based law enforcement unit, but must be understood as a knowledge-based organization whose success is determined by the ability to manage intellectual assets (knowledge as an asset). In a highly dynamic digital security environment, an organization's ability to learn faster than changes in the external environment will be the most strategic source of institutional excellence. (Endo, 2024)

In this context, the implementation of knowledge management is no longer an option, but an organizational need. The Directorate of Cyber Investigation needs a system that is able to capture investigative experience, convert these experiences into organizational knowledge, integrate various sources of information, and ensure that the knowledge that has been generated can be reused to improve the quality of handling the next case. In other words, organizations must move from an individual-oriented work pattern to an organization that is able to institutionalize knowledge as a collective asset.

The Directorate of Cyber Investigation of the Metro Jaya Police can be seen as a representation of modern public organizations that face the challenge of transformation towards a knowledge-based organization. The ability of organizations to manage knowledge will greatly determine the effectiveness of handling cybercrime in the future. The higher the organization's ability to create, share, integrate, and utilize knowledge, the greater the organization's capacity to respond to increasingly complex cyber threat developments. It is within this framework that knowledge management based on the SECI Model becomes relevant to be studied, as it provides a conceptual framework that enables organizations to build sustainable learning systems while strengthening institutional readiness in the face of evolving digital security challenges.

Readiness of the Directorate of Cyber Investigation in Implementing the SECI Model

The Directorate of Cyber Investigation of the Metro Jaya Police has various knowledge management practices that support the implementation of the SECI knowledge sharing model in handling cybercrime. In the context of Diversity, it is indicated that the organization has shown readiness in social, structural, and operational aspects to support the process of creation and knowledge exchange between personnel. This readiness can be seen from the existence of a mechanism for sharing investigative experience, case handling, documentation of operational knowledge, integration of information in investigations and investigations, and continuous learning processes carried out in support of increasingly complex handling of cybercrime.

Readiness on the *socialization side*

In the *socialization* dimension, the Directorate of Cyber Investigation of the Metro Jaya Police has a mechanism that allows the exchange of *tacit knowledge* between personnel. The process of sharing experiences is carried out through *briefing* activities before the implementation of tasks, post-case handling evaluations, technical discussions between investigators, and cross-unit coordination which is carried out periodically. In addition, personnel who have longer experience in handling cyber cases actively provide direction, mentoring, and consultation to newer personnel. These interactions not only take place in formal forums of the organization, but also develop through informal communication that occurs in the implementation of daily tasks.

In the context of *socialization*, it is oriented that handling cybercrime cases is often the main means of transferring experience between personnel. Personnel gain new knowledge through direct involvement in case handling, observation of the work methods of more experienced colleagues, and participation in investigative and investigative teams involving various specialties. This condition shows that the organization already has a work environment that allows for direct exchange of experiences. However, the intensity of *knowledge sharing* is still strongly influenced by the level of individual openness and the characteristics of the cases handled. Therefore, the readiness for the implementation (Omar & Desa, 2024; Zheyu et al., 2021) *of socialization* can be categorized as at a fairly good level because it has been supported by the collaborative work culture that has developed within the Directorate of Cyber Research.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Readiness on the *outsourcing side*

In the *externalization* dimension, that organization has made various efforts to convert the knowledge that individuals have into documented organizational knowledge. Various investigative experiences gained from handling cases have been poured into the form of investigation reports, investigation report results, technical guidelines, evaluation materials, and various other operational documents. In addition, there is a practice of compiling lesson *learned* notes from several cases that are considered to have a high level of complexity or contain new crime patterns that have not been handled before.

It is in this context that the Directorate of Cyber Investigation already has operational procedures that allow knowledge documentation to be carried out systematically. Various documents from the investigation are stored in the organization's administrative system and can be used as a reference in handling the next case. However, the findings of the study show that not all the knowledge possessed by personnel is optimally documented. Much of the knowledge gained through field experience is still stored as individual knowledge that is *tacit* in nature and has not been fully converted into explicit knowledge. This condition is mainly found in certain aspects of investigative techniques, perpetrator identification strategies, and analytical approaches that develop from the personal experience of investigators. Nonetheless, the existence of a documentation mechanism that has been in place indicates that the organization has sufficient readiness to implement the (Oliveira, 2020) *outsourcing process* within the framework of the SECI Model.

Readiness on *the combination side*

In the *combination* dimension, the Directorate of Cyber Investigation of the Metro Jaya Police has developed various knowledge integration mechanisms sourced from various documents, data, and investigation and investigation information. The integration is carried out through case data collection, digital archive management, use of investigation databases, and the use of various sources of information derived from investigations and cooperation with other agencies. In the process of handling cybercrime, personnel do not rely only on one source of information, but combine various information derived from public reports, digital data, forensic results, intelligence information, and relevant regulatory references. (Basten & Haamann, 2018)

In the context *of combination*, the organization's ability to integrate various sources of information has supported a more comprehensive investigative decision-making process. The various work units involved in handling cases have access to the information needed according to their respective authorities. In addition, the development of information technology used by organizations has helped the process of storing and distributing knowledge more effectively. In this case, it shows that there are efforts to update organizational information and knowledge on an ongoing basis along with the emergence of new modes of cybercrime. This condition externalizes the readiness of *combination* implementation to be in a relatively good category because organizations already have the capacity to integrate explicit knowledge from various sources.

Readiness on the *internalization side*

In the *internalization* dimension, the Directorate of Cyber Investigation of the Metro Jaya Police has carried out various activities that support the individual and organizational learning process. Knowledge that has been documented in the form of guidelines, case reports, and operational procedures is used as learning material for personnel. The organization has also informally carried out mentoring systems, from seniors to juniors on (Zheyu et al., 2021) sharing experiences aimed at strengthening the competence of personnel in dealing with the development of cybercrime.

It is in this context that the process of internalizing knowledge takes place through a combination of informal learning and hands-on experience in the execution of tasks. Personnel not only study existing training documents and materials, but also apply this knowledge in handling real cases. The practical experience then forms new knowledge that enriches the individual's ability to carry out cyber investigations. In addition, the periodic evaluation of case

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

handling provides an opportunity for personnel to reflect on the experience gained and develop a new understanding of emerging crime patterns.

The Directorate of Cyber Investigation of the Metro Jaya Police has a sufficient level of readiness in implementing the SECI knowledge sharing model. This readiness is reflected in the existence *of socialization* practices that support the exchange of experiences between personnel, *externalization mechanisms* that allow documentation of organizational knowledge, the ability *to combine* in integrating various information sources, and the *internalization* process which encourages learning and improvement of personnel competencies. However, the study also found that there was a variation in the level of readiness in each dimension. *Socialization* and *internalization* show a relatively stronger level of readiness because it has become part of daily operational activities. Meanwhile, *externalization* and *combination* still need strengthening, especially in the aspect of systematically *documenting tacit* knowledge and developing a more integrated knowledge management system.

The Directorate of Cyber Investigation of the Metro Jaya Police has an organizational foundation that supports the implementation of the SECI model in knowledge management. The existence of a collaborative culture, an ever-evolving investigative experience, an organizational documentation mechanism, and a continuous learning system are important indicators that demonstrate the organization's readiness to manage knowledge to support the increasingly complex and dynamic handling of cybercrime.

Challenges of the Directorate of Cyber Investigation in Implementing the SECI Model

In the context of the readiness for the implementation of the SECI Model at the Directorate of Cyber Investigation of the Metro Jaya Police, the success of knowledge management cannot be separated from various organizational challenges that have the potential to hinder the knowledge conversion process. In Nonaka's perspective, the creation of organizational knowledge is a process that takes place dynamically and continuously through the interaction between *tacit knowledge* and explicit knowledge. Therefore, various organizational factors such as budget, human resources, and institutional policies are important variables that determine the effectiveness of the implementation of the SECI Model. (Nonaka, 1994)

Budget Side

One of the main challenges in the implementation of the SECI Model is the limited budget support for the development of knowledge management systems. Handling cybercrime is a field that is highly dependent on technological developments, so it requires large investments in personnel competency development, digital investigation technology updates, knowledge database development, and the development of an integrated information management system. (Budhiraja et al., 2024)

In the context of *socialization* and *internalization* stages, budget constraints have the potential to reduce the frequency of training, further education, professional certification, and experiential learning activities that are indispensable in the development of personnel competencies. At the *externalization* and *combination* stages, budget limitations can hinder the development of an integrated and modern knowledge documentation system. As a result, knowledge generated from investigative experiences risks remaining stored in individuals and not developing into an organizational asset. From the perspective of organizational readiness, these conditions indicate that the successful implementation of the SECI Model requires sustained investment support. Without adequate budget resource allocation, the process of creating organizational knowledge will run partially and it will be difficult to achieve the optimal level of maturity.

Human Resources Side

The second very significant challenge has to do with the quality and quantity of human resources. Cybercrime is a phenomenon that develops much faster than the organization's ability to produce personnel who have specialist competence. The development of artificial intelligence technology, *blockchain, cryptocurrencies, the dark web, malware, ransomware*, and various forms of new digital threats demand constantly updated competencies.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

In the perspective of the SECI Model, human resources are the main actors who carry out the entire knowledge conversion process. In the *socialization stage*, individuals become the main source of tacit knowledge that is shared with other members of the organization. At *the externalization* stage, the individual is responsible for articulating his or her experience and knowledge into a documented form. In the *combination* stage, individuals play a role in integrating various sources of information into new knowledge. Meanwhile, at the *internalization stage*, the individual becomes the main subject who absorbs and implements organizational knowledge. (Dirani et al., 2021)

In the context of human resources, most of the strategic knowledge is still stored in certain personnel who have long experience in handling cyber cases. This condition indicates the risk of *knowledge concentration*, which is a situation when organizational knowledge is too concentrated on certain individuals. In the event of mutation, promotion, or personnel transfer, the organization has the potential to lose some of its intellectual capacity. Therefore, the readiness of the SECI Model implementation is highly dependent on the organization's ability to build a sustainable knowledge regeneration mechanism.

Policy Side

The next challenge is related to the policy and governance aspects of the organization. From a knowledge management perspective, the success of the SECI Model requires policy support that is able to encourage the formation of a culture of knowledge sharing in a sustainable manner. It is in this context that various *knowledge sharing* practices have taken place through *briefings*, case evaluations, technical discussions, and personnel assistance. Nevertheless, most of these practices are still evolving organically based on operational needs. This condition shows that knowledge management has not been fully institutionalized in the organizational system.

From the perspective of the readiness of the SECI Model implementation, the existence of formal policies is very important because it functions as an instrument to ensure the sustainability of the knowledge creation process. These policies can be in the form of knowledge management standards, investigative experience documentation mechanisms, the development of organizational knowledge repositories, and reward systems for personnel who actively share *knowledge*.

Through *socialization*, organizations can maintain the sustainability of experience transfer between personnel. Through *outsourcing*, investigative experience can be converted into documented organizational assets. Through *combination*, various scattered information can be integrated into new and more comprehensive knowledge. While through *internalization*, organizational knowledge can be transformed into competencies inherent in individuals and increase institutional capacity. (Ginanjar, 2022; Makbul et al., 2023)

In the context of evolving cybercrime response, an organization's ability to learn faster than changing threats is the most important source of strategic advantage. Therefore, the readiness of the Directorate of Cyber Investigation in implementing the SECI Model is actually not only related to knowledge management, but also related to the organization's ability to maintain its relevance, effectiveness, and adaptability in facing the dynamics of cybercrime in the future. In other words, the successful implementation of the SECI Model will determine the extent to which the Directorate of Cyber Investigation is able to develop from an organization that simply manages information to a knowledge-based organization that continuously creates, integrates, and utilizes knowledge as a source of institutional excellence.

CONCLUSION

The readiness of the Cyber Investigation Directorate of the Metro Jaya Police in implementing the SECI Model still faces major challenges in terms of budget, human resources, and policies. Budget constraints hinder capacity development, knowledge infrastructure, and the sustainability of knowledge management programs. In the aspect of human resources, there is still a gap in competence, experience, and knowledge sharing awareness that affects the effectiveness of the knowledge conversion process at each stage of SECI. Meanwhile, the lack of strong policy institutionalization has caused the practice of knowledge sharing to still depend on individual initiatives and

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 15 No. 2. June 2026 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

leadership. These three factors are strategic challenges that determine the success of the implementation of knowledge management in a systematic, sustainable, and integrated manner in supporting the handling of cybercrime.

The Directorate of Cyber Investigation of the Metro Jaya Police needs to strengthen *socialization* through the formation of learning communities and formal mentoring programs; strengthen *externalization* through the obligation to document *best practices* and the development of digital knowledge repositories, optimizing *the combination* by integrating data, archives, and investigative information in an integrated knowledge management system accompanied by a regulatory base, as well as strengthening *internalization* through training-based continuous learning, case simulation, and operational experience. In terms of challenges, special budgeting is needed for knowledge management, the development of *a culture of knowledge sharing* and human resource competence, as well as the preparation of knowledge management policies that are institutionalized in SOPs, performance indicators, and *long-term knowledge management roadmaps* to ensure the sustainability of the implementation of the SECI Model in a systematic, measurable, and adaptive manner in handling cybercrime.

REFERENCES

Abdillah, A., Widianingsih, I., Buchari, R. A., & Nurasa, H. (2024). The Knowledge-Creating Company: How Japanese Companies Create The Dynamics of Innovation. *Learning: Research and Practice*, *10*(1), 121–123. https://doi.org/10.1080/23735082.2023.2272611

Arnell, P., & Faturoti, B. (2023). The Prosecution of Cybercrime – Why Transnational and Extraterritorial Jurisdiction should be Resisted. *International Review of Law, Computers & Technology*, *37*(1), 29–51. https://doi.org/10.1080/13600869.2022.2061888

Arsawan, I. W. E., Hariyanti, N. K. ssy De, Atmaja, I. M. A. D. S., Suhartanto, D., & Koval, V. (2022). Developing Organizational Agility in SMEs: An Investigation of Innovation's Roles and Strategic Flexibility. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(3), 149. https://doi.org/10.3390/joitmc8030149

Basten, D., & Haamann, T. (2018). Approaches for Organizational Learning: A Literature Review. *Sage Open*, *8*(3). https://doi.org/10.1177/2158244018794224

Budhiraja, S., Yadav, M., & Rathi, N. (2024). Multi-Level Outcomes of Learning Organisation: A Bibliometric Analysis and Future Research Agenda. *Journal of Organizational Effectiveness: People and Performance*, *11*(2), 282–306. https://doi.org/10.1108/JOEPP-02-2023-0039

Cerchione, R., Centobelli, P., Borin, E., Usai, A., & Oropallo, E. (2024). The WISED Knowledge-Creating Company: Rethinking SECI Model in Light of The Digital Transition. *Journal of Knowledge Management*, *28*(10), 2997–3022. https://doi.org/10.1108/JKM-02-2024-0133

Dinda, A. L. S. (2024). The Effectiveness of Law Enforcement against Cybercrime in Indonesia. *Al-Dalil: Journal of Social, Political, and Legal Sciences*, *2*(2), 69–77. https://doi.org/10.58707/aldalil.v2i2.777

Dirani, K., Baldauf, J., Medina-Cetina, Z., Wowk, K., Herzka, S., Bello Bolio, R., Gutierrez Martinez, V., & Munoz Ubando, L. A. (2021). Learning Organization as a Framework for Networks' Learning and Collaboration. *The Learning Organization*, *28*(4), 428–443. https://doi.org/10.1108/TLO-05-2020-0089

Endo, T. (2024). Adaptive Governance and Evolution of a Groundwater-Based Resilient City: A Case Study of Kure City, Japan. *Water International*, *49*(8), 956–975. https://doi.org/10.1080/02508060.2024.2423451

Ginanjar, Y. (2022). Indonesia's Strategy to Establish Cyber Security in Facing the Threat of Cyber Crime Through the State Cyber and Cryptography Agency. *Journal of Global Dynamics*, *7*(02), 291–312. https://doi.org/10.36859/jdg.v7i02.1187

Ilhami, M. W., Nurfajriani, W. V., Mahendra, A., Sirodj, R. A., & Afgani, M. W. (2024). Application of the Case Study Method in Qualitative Research . *Scientific Journal of Educational Vehicles*, *10*(9), 462–469. http://jurnal.peneliti.net/index.php/JIWP/article/view/6872

Irawan, D. (2025). Strategy, Strategy for Cyber Police Human Resources Development in Regional Units in the Context of Realizing the National Police 4.0. *Journal of Research and Development of the National Police*, *28*(1), 73–78. https://doi.org/10.46976/litbangpolri.v28i1.299

Khaldun, R. I., Fita, G. A., Utami, A. N. F., & Tahawa, T. H. B. (2020). Globalization, Threats and Efforts to Increase the Competitiveness of Domestic Workers against Foreign Labor Attacks in Indonesia. *LINO Journal of International Relations*, *1*(1), 27–36. https://doi.org/10.31605/LINO.V1I1.827

Mak, C., & Hong, J. (2020). Creating Learning Organization 2.0: A Contextualized and Multi-Stakeholder Approach. *The Learning Organization*, *27*(3), 235–248. https://doi.org/10.1108/TLO-01-2020-0020

Makbul, S., Nugroho, A. S., & Zulkifli, Z. (2023). Efforts to Improve the Performance of Members of the National Police Human Resources Section at the Magelang City Police. *Indonesian Journal of Accounting Management Research*, *1*(1), 81–98. https://doi.org/10.32477/jrima.v1i1.662

Miller, A. N., Kordova, S., Grinshpoun, T., & Shoval, S. (2023). To Be or Not To Be a Systems Thinker: Do Professional Characteristics Influence How Students Acquire Systems-Thinking Skills? *Frontiers in Education*, *8*. https://doi.org/10.3389/feduc.2023.1026488

Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. *Organizational Science*, *5*(1). https://doi.org/10.1515/znb-1961-1011

Oliveira, M. J. S. P. (2020). For Organizational Communication that Promotes the Sharing of Tacit Knowledge. *Risk and Financial Management*, *2*(2), p37. https://doi.org/10.30560/rfm.v2n2p37

Omar, A. S., & Desa, Z. Mohd. (2024). A Conceptual Review of Trust and Knowledge-Sharing Behavior Among Academics in Public Universities. *Malaysian Journal of Social Sciences and Humanities (MJSSH)*, *9*(9), e002981. https://doi.org/10.47405/mjssh.v9i9.2981

Rizki, M. (2022). Development of Indonesia's Defense/Cyber Security System in Facing the Challenges of Technology and Information Development. *Polytheia: Journal of Political Science*, *14*(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Rusland, S. L., Jaafar, N. I., & Sumintono, B. (2020). Evaluating Knowledge Creation Processes in The Royal Malaysian Navy (RMN) Fleet: Personnel Conceptualization, Participation and Differences. *Cogent Business & Management*, *7*(1). https://doi.org/10.1080/23311975.2020.1785106

Srivastava, S. K., Das, S., Udo, G. J., & Bagchi, K. (2020). Determinants of Cybercrime Originating within a Nation: A Cross-country Study. *Journal of Global Information Technology Management*, *23*(2), 112–137. https://doi.org/10.1080/1097198X.2020.1752084

Tabiu, R., Heryanti, Intan, N., & Safiuddin, S. (2023). Globalization and Transnational Organized Crime. *Halu Oleo Law Review*, *7*(1), 99–110. https://doi.org/10.33561/holrev.v7i1.11

Tobing, C. I., Surya, T. M., Selvias, L. R., Girsang, S. R., Azzahra, P. B., Purba, L. Y., Putera, M. A., & Rusmana, N. (2024). Digital Globalization and Cybercrime: Legal Challenges in Dealing with Cross-Border Cybercrime. *Journal of Swan Law*, *10*(2), 105–123. https://doi.org/10.31599/sasana.v10i2.3170

Woods, C., Fitzpatrick, S., Lukersmith, S., Coulter, L., O'Neill, S., Savage, J. A., Moll, S., Bosanquet, K., Galdas, P., West, S., Bergeron, M., Shelton, J., Blume, A., Ditton-Phare, P., Nixon, R. D. V., Elizabeth, M., Hollerbach, B., Grillo, C., Heisel, M., … Darby, J. (2025). Sharing Knowledge on Implementing Mental Health and Wellbeing Projects for Veterans and First Responders. *Comprehensive Psychiatry*, *138*, 152579. https://doi.org/10.1016/j.comppsych.2025.152579

Zheyu, L., Weijin, C., Jihui, Z., Yuan, W., Ghani, U., & Zhai, X. (2021). Investigating the Influence of Tacit Knowledge Transformation Approach on Students' Learning Ability. *Frontiers in Psychology*, *12*. https://doi.org/10.3389/fpsyg.2021.647729