GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v3i2.

Development of The Capacity of The North Kalimantan Police Sub-Division V Cyber Crime Unit in Handling Cyber Crime: A Qualitative Analysis

Oscar Fajar Rahadian[1], Joko Setiono[2], Ilham Prisgunanto[3]
[1]Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia, oscarfajarr@gmail.com
[2]Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia, joko_setiono@ymail.com
[3]Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia, prisgunanto@gmail.com

Corresponding Author: oscarfajarr@gmail.com[1]

Abstract: Enhancing the capacity of police organizations is crucial in the digital age, which is marked by increasingly complex cybercrime. This study analyzes capacity development within the Cyber Sub-Directorate V of the Special Criminal Investigation Directorate of the North Kalimantan Regional Police. Using a qualitative approach, this study explores the capacity enhancement mechanisms that have been implemented and the obstacles faced by the North Kalimantan Regional Police's cyber unit. The study results indicate that despite facing limitations in personnel and resources, various strategic efforts have improved the effectiveness of cybercrime case handling. The implementation of a technology-based case management system strengthened coordination among stakeholders, and ongoing human resource training programs have significantly contributed to enhancing personnel competencies and unit performance. The cyber case resolution rate increased from 60% to 80% within a year, accompanied by a decrease in the average handling time per case. On the other hand, challenges such as budget constraints, a shortage of IT-skilled personnel, rapid technological developments, regulatory constraints, and low public cyber awareness still hinder capacity optimization. This study provides in-depth insights into capacity development strategies in regional police cyber units and compares them with findings from similar research. The findings are expected to serve as a reference in formulating policies to strengthen police organizational capacity in addressing cybercrime threats.

Keywords: Organizational Capacity Development, Police, Cybercrime, Human Resources, North Kalimantan Regional Police

INTRODUCTION

Advances in information technology have presented new challenges for law enforcement. Cybercrime continues to increase in both volume and complexity, posing a serious threat to public and national security. (Widianingrum, 2024) Police forces in various countries are required to improve their organizational capacity to respond to widespread cyber

threats. Organizational capacity in the context of law enforcement encompasses an institution's ability to effectively mobilize resources, technology, and trained personnel to prevent and address cybercrime. (Indrayanti, 2018)

The Indonesian National Police (Polri) has taken adaptive measures by establishing a cyber directorate at the central level and cyber units at the regional level. (Kasim, 2024) The North Kalimantan Regional Police, as one of the youngest regional police forces, faces the challenge of limited resources in handling increasingly complex cyber cases. The Cyber Sub-Directorate V of the Special Criminal Investigation Directorate of the North Kalimantan Regional Police (hereinafter referred to as Subdit V Siber) is tasked with handling cyber crimes in the North Kalimantan region, including crimes in cyberspace and electronic transactions. However, limited personnel and resources—only seven personnel in 2024, with two having a background in information technology—are major obstacles to optimizing the unit's performance. (Syamsul Arifin, 2024) This situation is similar to the phenomenon in various jurisdictions, where police cyber units often lack staff with adequate technical expertise. (Aini, 2024)

As a result of these limitations, efforts to uncover cyber cases are often hampered. External challenges such as knowledge gaps among investigators, the rapid evolution of cybercrime modus operandi, and regulatory limitations widen the gap between cyber threats and police response capacity. (Aditama, 2025) At the national level, legal frameworks such as the Electronic Information and Transactions Law (EIT Law) have been updated from (Law No. 19 of 2016) to (Law No. 1 of 2024) to strengthen investigative authority, including international cooperation in addressing cybercrime. (Budianto Pansariadi, 2024) However, policy implementation requires adequate institutional capacity at the regional level.

Based on this background, this study aims to: (1) examine the mechanisms or efforts used by Sub-Directorate V Cyber of the North Kalimantan Regional Police in improving its organizational capacity, and (2) analyze the obstacles faced by the unit in the process of developing its organizational capacity. Focusing on the case of the North Kalimantan Regional Police Cyber Crime Sub-Directorate V, this study aims to provide an empirical overview of the real challenges in the field and the strategies for development, which can serve as a model for other police units in improving their ability to deal with cybercrime.

LITERATURE REVIEW

The concept of organizational capacity building refers to the process of improving an organization's ability to perform its functions effectively and sustainably. (Irawan, 2016) According to public management literature, organizational capacity encompasses various dimensions, such as human resource capacity, structure and systems, leadership, and adaptability to change. (Fefta, 2014) Capacity building in law enforcement institutions emphasizes strengthening personnel competencies, updating technology and supporting infrastructure, improving work procedures, and improving internal and external coordination.

Previous research on police and cybercrime shows that many police organizations face capacity gaps in responding to cybercrime. (Yurizal, 2018) Lack of specialized training, minimal organizational support, and limited resources are common problems found in various countries. For example, Wilson & Cross in their study of the Australian police found that although officers felt confident individually in handling cyber incidents, they were less confident in their organizational capabilities and expressed the need for increased resource support and professional development programs in their institutions. Similar findings were reported by Nouh et al. (2019), who highlighted the socio-technical challenges faced by cyber investigators, such as limited tools, system interoperability issues, and the need for improved technical skills and domain knowledge.

In terms of cybercrime response, the literature also emphasizes the importance of partnerships and collaboration. Cross-sector collaboration, such as cooperation between the police, IT experts, industry, and the community, is considered effective in closing certain capacity gaps and addressing evolving cyber threats. (Djarawula, 2023) Public-private partnership models have been proposed in various studies to improve the efficiency of cybercrime detection and enforcement, especially in complex and cross-jurisdictional cases. In addition, digital literacy programs for the public are considered an integral part of cyber prevention strategies. Cyber security education among the public can reduce the number of victims and incident reports, thereby lightening the workload. (Loso Judijanto, 2025)

Referring to the above framework, this study places the capacity development of the Cyber Sub-Directorate V within the context of organizational capacity-building theory and recent empirical findings. The conceptual framework includes internal factors (human resources, technology, budget, organizational culture) and external factors (regulation, partnerships, public support) that influence the capacity of police organizations to deal with cybercrime.

METHOD

This study uses a qualitative approach with a case study design on Subdit V Siber Polda Kalimantan Utara. The qualitative approach was chosen to gain an in-depth understanding of the processes, experiences, and challenges of organizational capacity development in this unit. The unit of analysis for this study is the Subdit V Siber organization itself, while key informants include officials and personnel related to the Subdit V Siber structure as well as relevant external stakeholders.

Data was collected using several techniques: in-depth interviews, participatory observation, and document studies. In-depth interviews were conducted with key informants, including the Head of Sub-Directorate V Cyber Crime of the North Kalimantan Regional Police, investigators and operational staff of the cybercrime unit, as well as other parties such as officials from the Indonesian National Police's Directorate of Information Technology or external partners (e.g., digital forensics experts from universities). The interviews focused on capacity-building mechanisms (e.g., training programs, use of new technologies, collaboration patterns) and the challenges faced. Participatory observation was conducted to directly observe the unit's operations, including the use of systems or technological tools in handling cases, as well as internal coordination dynamics. Document studies included reviewing police performance reports, personnel data, budget documents, training modules, and Standard Operating Procedures (SOPs) related to cybercrime handling. Data triangulation was conducted by comparing information from various sources to enhance the validity of the findings.

The collected data was analyzed using thematic analysis techniques. The analysis stages included transcribing interview results, coding important information units, categorizing codes that emerged into specific themes, and drawing conclusions based on the thematic patterns found. Some of the main themes anticipated based on the conceptual framework include: human resource development strategies, technological innovation and information systems, patterns of cooperation/collaboration, resource constraints, regulatory constraints, and organizational cultural aspects. The researcher conducted member checks with several informants to ensure that the interpretation of the findings was consistent with the reality on the ground. Furthermore, the empirical findings were compared with the theoretical framework and other research results (cross-case analysis) to identify similarities and specificities of the Subdit V Siber case.

This study also considered ethical aspects. All informants provided informed consent before the interviews, and their identities were kept confidential in the reporting of results.

With this methodology, it is hoped that the analysis results will provide a comprehensive and in-depth picture of the efforts and challenges of organizational capacity development in Sub-Directorate V Cyber of the North Kalimantan Regional Police.

RESULT AND DISCUSSION

1) Brief Profile of Subdit V Siber Polda Kaltara

Subdit V Siber Polda Kalimantan Utara was formed to handle cases related to cybercrime, ITE (Information and Electronic Transactions), and other technology-based crimes in the jurisdiction of Polda Kalimantan Utara. As a relatively new police department (the North Kalimantan Police Department was officially established in 2018), the cybercrime unit's resource capacity is still under development. As of 2024, the unit is staffed by only 7 personnel, consisting of 1 officer and 6 non-commissioned officers, with most having backgrounds in general police work. Only 2 personnel have formal education in information technology, while the others acquired technical skills through short-term training within the National Police. In terms of infrastructure, Subdit V Siber has a cyber control room and some investigative tools for digital investigations, but the completeness and modernity of the equipment are deemed insufficient to address increasingly sophisticated cybercrimes.

Performance data shows that in 2023, Sub-Directorate V Cyber received 100 reports of cybercrime cases, ranging from online fraud, and account hacking, to cybersex cases and the dissemination of illegal content. Of these, approximately 60% of cases were successfully followed up to the completion stage (complete files), while the remaining 40% of cases were delayed or transferred to the National Police Criminal Investigation Agency (Bareskrim Polri) due to technical limitations at the Regional Police Headquarters. This capacity limitation reflects the real challenges faced by cyber units at the regional level: the high caseload is not balanced with the available human resources and equipment.

2) Capacity Development Mechanisms Implementation

Despite facing various limitations, Sub-Directorate V Cyber of the Kaltara Regional Police has undertaken several strategic efforts to develop its organizational capacity. The research findings identified several key initiatives as follows:

Modernization of Equipment and Technology

This unit proactively proposes and utilizes budgets for the procurement of modern digital investigation tools. During the 2023-2024 period, Sub-Directorate V Cyber acquired several new pieces of equipment, such as digital forensic imaging devices, malware analysis software, and IP tracking tools. This modernization of equipment is seen as a strategic step to enhance the unit's digital forensic capabilities. The implementation of new equipment is accompanied by technical guidance for personnel. Overall, the modernization of digital investigative equipment is a timely and strategic step; with careful planning and proper implementation, this investment is expected to significantly enhance Sub-Directorate V Cyber's capabilities in addressing cybercrime. Initial data supports this: for example, forensic analysis of mobile phones, which previously had to be sent to the central laboratory, can now be conducted independently by Sub-Directorate V Cyber for certain cases, saving investigative time.

Development of an Integrated Information System (SIBER)

Subdit V Siber has developed an integrated information system and database called SIBER (Evidence-Based and Real-Time Information System). This system was built in collaboration with the Indonesian National Police's ICT Directorate to support cyber investigation operations. The main features of SIBER include a case Management System to

track case progress from start to finish, Digital Evidence Management to securely store and manage digital evidence, a Threat Intelligence Database containing the latest cyber threat information, and an Analytics Dashboard to identify patterns and trends in cybercrime. The integration of SIBER with the work processes of Sub-Directorate V Cyber has resulted in several improvements: case status monitoring can now be done in real-time, case handling workflows are more standardized through workflow automation features, and task management for team members is more coordinated. The implementation of this IT-based case management system has proven to improve case handling efficiency; internal performance reports show that the average case resolution time has decreased from ~60 days to ~45 days, and the prosecution success rate has increased from around 65% to 80% following the system's adoption. Additionally, the system has improved accountability and transparency in case handling, which in turn strengthens public trust in the cyber unit's performance.

Human Resource Training and Development Program

Recognizing the technical limitations of its personnel, Subdit V Siber continuously sends its personnel to attend IT and cybercrime-related training and certification programs. This human resource development program includes digital forensics training, ethical hacking courses, cyber intelligence analysis workshops, and participation in technical guidance programs organized by the National Police Headquarters or other institutions. Every staff member has completed basic cybercrime training, and some have obtained international certifications (e.g., Certified Digital Forensic Examiner). In addition to formal training, Cyber Division V implements a knowledge-sharing model, where staff returning from training share their knowledge with their colleagues. As a result, despite the small number of staff, the team's skill set has relatively improved. The technological literacy and technical capabilities of each member are more evenly distributed compared to the early years of the unit's formation. The competence improvement is reflected in the unit's success in uncovering more complex cyber cases; some cross-regional hacking and cyber fraud cases that previously had to be transferred can now be handled independently by the Cyber Sub-Directorate V team thanks to personnel who have mastered advanced cyber investigation techniques.

Strengthening Coordination and Collaboration

Subdit V Cyber builds an effective coordination mechanism with other agencies, both internal and external to the National Police. Internally, this unit actively coordinates with Ditreskrimsus of other Regional Police and Bareskrim Polri, especially in handling cross-regional or high-profile cyber cases. The formation of a joint task force is carried out for cases that require additional personnel or equipment support. A real-time information exchange system with intelligence units and related units in the Regional Police is also developed to ensure a quick response in the event of a cyber incident. Externally, Subdit V Cyber collaborates with various stakeholders: including universities (such as universities that have IT experts and cyber study centers) for scientific consultations and recruitment of temporary experts; the technology industry to obtain the latest threat information updates and technology solutions (several cybersecurity companies provide short training or threat detection software licenses as part of CSR); and financial institutions such as PPATK in order to track the flow of funds in online fraud cases. International collaboration is also being explored, considering that cybercrime is often cross-border. The support of the Indonesian National Police's Hubinter Division facilitates Subdit V Cyber to connect to the Interpol and ASEAN Cyber Police networks for the exchange of information. Strengthening this coordination is in line with the mandate of Article 43 paragraph (6) of the ITE Law which allows cooperation between Indonesian investigators and other countries in uncovering cyber crimes. The real impact is

that several cross-country scamming cases involving victims in North Kalimantan can be handled more quickly through sharing information with law enforcement in other countries..

The above efforts show that the North Kalimantan Police Cyber Sub-Directorate V has made important innovations and initiatives in improving its organizational capacity. The implementation of new technologies and continuous improvement of human resource competencies have strengthened the unit's ability to face cybercrime challenges. Improved internal performance indicators (case resolution increased to ~80%, shorter response time) are evidence of the initial success of capacity development. However, several structural and contextual constraints still limit the optimization of these efforts, as discussed in the following subsections.

3) Barriers and Challenges to Capacity Development

The results of the qualitative analysis revealed various obstacles faced in the capacity development process at the Subdit V Cyber Polda Kaltara. These challenges stem from internal organizational factors and the external environment, including:

Operational Budget Limitations

Limited funding is a major obstacle in accelerating the development of unit capacity. The budget allocation for cyber operations at the North Kalimantan Regional Police is relatively small, considering that this regional police is still new and has a lower scale of cyber cases compared to large regional police. Although there is a trend of increasing budgets every year, the amount is still insufficient to meet all needs - especially related to the procurement of sophisticated equipment, increasing the number of personnel, and advanced training. (Heri, 2019) Interviews with regional police officials revealed that requests for additional budgets often run up against other priorities and limitations of the state budget. As a result, several initiatives have had to be carried out in stages or seek alternative sources. For example, for advanced HR training, Sub-Directorate V Cyber has been forced to be selective in sending personnel due to limited funds, and seek training programs sponsored by third parties when possible. Temporary solutions such as borrowing equipment from Bareskrim or collaborating with universities have been carried out, but have not yet answered funding needs comprehensively. Without adequate budget support, capacity development tends to be slow and ad-hoc. This indicates the need for a strategic approach in Polri budget planning, for example by refocusing the budget for cyber priorities or seeking grants.

Lack of Human Resources with Special Skills

Limited human resources and lack of specific competencies are crucial challenges. As explained previously, only 2 out of 7 personnel in Subdit V Cyber have an IT education background, the rest have a general police background with little technical training. This shortage of experts causes a high workload on a handful of personnel who are technically proficient. The impact is seen in case handling: several cybercrime reports cannot be followed up optimally due to limited personnel capabilities, so complex cases have to be transferred to the central level. The internal recruitment process of the National Police which has not been able to quickly meet the need for specialists (for example recruiting computer graduates as investigators) makes the situation worse. Interviews with members of the Subdit revealed a feeling of being overwhelmed when faced with complex cases, because they have to learn new technologies on their own. (Winata, 2023) Efforts to strengthen human resources through training are hampered by personnel rotation; sometimes trained personnel are transferred to other units, so that the unit must re-adjust to new personnel who are not yet experienced in the cyber field. The moratorium on ASN recruitment in recent years has also been an external factor that has hampered the addition of new personnel to the Regional Police. Overall, these

HR challenges require long-term solutions in the form of more structured career planning and capacity building for Polri HR, including incentives for technology experts to join and stay in the cyber unit.

Technological Developments and Crime Modus Operandi

The speed of information technology evolution is a challenge in itself. Cybercriminals continue to adopt new technologies and modes that require the police to constantly update their knowledge and technical capabilities. For example, the trend of using cryptocurrency and the dark web in cybercrime is increasingly rampant, while the capacity of Subdit V Cyber in this area is still very limited. Personnel admit that it is difficult to keep up with the latest hacking techniques or new malware variants that emerge. The police's equipment procurement cycle, which tends to be slow, also makes some devices obsolete before they can be optimally utilized. (Afianto, 2021) Organizational adaptability is an issue: how quickly internal procedures and skills can adapt to the changing threat landscape. The study findings show that the proactive attitude of Subdit leaders plays a major role in this. With limited resources, the unit tries to build resilience through a culture of self-learning - for example, members voluntarily learn new trends via online cyber communities, share articles and threat updates in internal groups, etc. However, without systematic support (such as regular training curriculum updates, technology testing laboratories, etc.), these adaptation efforts are less than optimal. (Aditya, 2023) The challenges of technological development have a wide impact: if not anticipated, the gap in capabilities between perpetrators and officers will widen. Therefore, institutional commitment is needed to ensure that regional cyber units have continuous access to the latest information and training.

Limitations of Regulation and Legal Procedures

In terms of regulation, although Indonesia already has the ITE Law, several derivative regulations and technical guidelines for cyber law enforcement are still lagging behind. Cyber Sub-Directorate V investigators face obstacles when they have to preserve cross-border data, or when dealing with new types of crimes that have not been explicitly accommodated in law (for example, cases of personal data violations before the PDP Law was passed). Procedures such as digital evidence chain of custody have also not been regulated in detail in the Perkap (Chief of Police Regulation), so investigators rely on international best practices so that digital findings are recognized in court. This regulatory vacuum makes several law enforcement efforts less effective; for example, forcing foreign platforms to hand over data requires a long process because there is no strong cooperation agreement. (Raslin, 2021) In addition, internal bureaucratic processes such as permits for data confiscation or cross-directorate coordination sometimes hinder a quick response. The Sub-Directorate admits that these regulatory challenges are not within their control, but have a direct impact on performance in the field. Advocacy is needed from the police to policy makers to immediately improve regulations related to cybercrime, including international agreements (Mutual Legal Assistance) that facilitate the collection of electronic evidence across countries. In the short term, Subdit V Cyber has overcome this by coordinating a lot with the public prosecutor from the start of the investigation so that the evidence strategy is in accordance with existing legal corridors.

Low Public Awareness and Participation

Another external factor is the low level of digital literacy and cybersecurity awareness of the community. Many cases of online fraud in North Kalimantan are not reported by victims due to a lack of understanding of the reporting process or the shame (stigma) of being a victim. Low reporting results in underestimating the scale of the problem, so that the allocation of police resources for cyber units may be considered a non-priority. In addition, the lack of

awareness often makes the community ignore basic preventive measures, so that similar cases recur. (Gigantara, 2021) Sub-Directorate V Cyber has conducted socialization and education through the Regional Police's social media and seminars at schools/campuses, but its reach is limited. Then, collaboration is needed with other agencies such as the Communication and Information Service and local IT activist communities to increase cyber awareness. Increasing community participation is also important: for example, encouraging the involvement of cyber volunteers (such as cyber patrol volunteers) or Cyber Education programs in schools. These socio-cultural barriers require a long-term approach, but if not addressed, they will continue to be a weak point in the cybercrime handling ecosystem. (Aldriano, 2022)

Organizational Culture and Internal Resistance

Another interesting finding is the resistance to change within the organization. Several senior personnel at the Regional Police have shown reluctance or are slow to adapt to new technology-based procedures. For example, the implementation of the SIBER system initially faced passive resistance, where some investigators were reluctant to switch from manual to digital recording, because they were used to the old pattern. It took time and a persuasive approach from the leadership for this new work culture to be accepted. In addition, the high workload with limited personnel sometimes makes staff reluctant to get involved in extra initiatives (such as additional training or system development projects) because they are considered to add to the work. A hierarchical bureaucratic culture also has the potential to hinder the communication of ideas from the bottom up. (Muhdiyati, 2024) For example, innovative ideas from junior staff may be stifled if superiors are not open. However, in the Sub-Directorate V Cyber Polda Kaltara itself, researchers observed the leadership of the Sub-Directorate Head who was relatively visionary and participatory, so that resistance could be minimized. The leadership actively encouraged a change in mindset that digital transformation was inevitable. Organizational learning began to grow, where every challenge was seen as an opportunity to learn and improve. However, maintaining the momentum of this cultural change requires consistency and ongoing support from the Polda and Mabes Polri levels.

Analysis and Implications

The above results indicate that organizational capacity development in regional cyber police units is a multidimensional process that faces complex challenges. Subdit V Cyber Polda Kaltara has shown significant initiatives within its limitations, which have a positive impact on short-term performance. The application of technology (case information systems, forensic tools) and increasing HR competencies have been shown to improve several performance indicators (outputs). This confirms the resource-based view theory that better utilization of internal resources (technology and human capital) will improve organizational capabilities and performance. (Hidayah Endang, 2021)

However, there is a gap between internal achievements and greater external challenges. The dynamic nature of cybercrime demands an agile and adaptive organizational response. Regulatory gaps and low public awareness are issues that are beyond the direct control of the unit, but greatly affect the success of cyber law enforcement. (Irfan, 2024) This shows the importance of a holistic approach: capacity development is not enough at the operational unit level, but requires support from the meso level (Regional Police, National Police Headquarters) to the macro level (regulators, government, community).

This case study also confirms that limited HR is a critical problem in cyber law enforcement. Even with sophisticated technology, without competent personnel, the results are not optimal. (Midarwanto, 2015) The National Police can consider a special recruitment policy for cyber investigator positions with IT expertise backgrounds, as well as a special retention scheme so that these experts are willing to be placed in areas such as North Kalimantan. In

addition, it is also important to build a knowledge network between cyber units in various regional police. For example, the Kaltara Cyber Sub-Directorate V can be mentored by a more advanced cyber unit in the Regional Police (a kind of sister unit), in order to transfer knowledge and provide technical assistance if necessary. This kind of horizontal collaboration can be a solution to overcome capacity disparities between regions.

Comparison with Similar Research

To understand the position of this study's findings in a broader context, it is important to compare them with the results of similar research in the field of police organizational capacity development and handling cybercrime.

The previously mentioned study by Wilson & Cross (2022) in Australia provides a perspective that capacity issues are not only experienced by developing countries, but also in police forces in developed countries. Wilson et al. found a gap between individual capacity and organizational capacity; officers may be well-trained, but if the organization does not provide adequate resources and support, the response to cybercrime remains suboptimal. This finding is in line with the conditions in the Subdit V Cyber Polda Kaltara, where personnel who are actively training are still hampered by limited institutional support (additional human resources, budget, etc.).

The implications of Wilson & Cross's results emphasize the importance of continuous investment in resourcing and professional development as organizational policies, not just individual-level initiatives. For the National Police, this means that the cyber unit's capacity development program must be institutionalized - for example, making advanced cyber training part of the routine curriculum, and ensuring that the unit is given sufficient authority and funding for innovation.

Research by Nouh et al. (2019) in an international forum underlines the socio-technical challenges in cyber investigations. They found that investigators are often hampered by less user-friendly interfaces and tools, limited interoperability between systems, and a lack of training support to keep up with the rapid development of technology. The case of Subdit V Cyber also reflects several similar things: for example, obstacles to cross-agency system integration and the need for continuous training. The difference is, in the Indonesian context the problem is exacerbated by the limited number of personnel. Nouh et al. recommend a user-centered design approach in designing an investigation system for the police, as well as increasing technical support and involvement of the IT expert community to assist law enforcement. The North Kalimantan Police can learn from this by continuing to involve local academics/experts in developing the SIBER system to suit the needs of users (investigators) in the field.

In general, a comparison with these studies confirms several common threads: (a) The need for capacity building is universal in handling cybercrime, covering aspects of human resources, technology, and cooperation; (b) Obstacles in the form of limited resources and regulations often arise, both in developed and developing countries, only the scale is different; (c) The importance of institutional and policy support that accommodates the uniqueness of cyber threats (structural flexibility, continuous learning, regulatory updates) as a key factor in the success of capacity building. By comparing local findings (Subdit V Cyber Kaltara) and global/regional trends, it can be concluded that efforts to develop the capacity of police organizations must be carried out comprehensively and in stages.

Initiatives at the unit level need to be supported by comparative studies and benchmarking with best practices from research and the experiences of other police forces. For example, the case management system that is implemented can be compared with similar systems used by police forces in other countries, so that it can continue to be improved. Likewise, the training model, the Police can adopt international modules (Interpol Cyber

Training, Europol) to improve quality. Ultimately, by learning from research and practice in various places, Subdit V Cyber Polda Kalimantan Utara and similar units can accelerate the process of increasing their capacity towards ideal standards.

CONCLUSION

This study concludes that the North Kalimantan Police Cyber Sub-Directorate V faces complex organizational capacity challenges in carrying out law enforcement duties in the cyber realm. The main challenges include budget constraints, the minimal number and competence of IT personnel, and the rapid development of technology and cybercrime modes. Nevertheless, this unit has made various significant capacity development efforts: starting from modernizing digital investigation equipment, developing an integrated information system (SIBER), improving HR competency through ongoing training, to strengthening coordination with internal-external stakeholders. These efforts have succeeded in significantly improving the performance of the Cyber Sub-Directorate V, as demonstrated by, among others, an increase in the level of case resolution and the ability to handle more complex cyber cases than before.

On the other hand, existing obstacles have not been fully resolved. Limited support for resources and regulations requires attention from higher levels of leadership. Organizational capacity development is an ongoing process that requires long-term commitment and support from various parties. To achieve optimal results, synergy is needed between Polri's strategic policies (such as adding formations and special budgets for cyber units, adaptive training curricula) and operational-level initiatives (technological innovation, partnerships, and a learning culture in the unit). In addition, ecosystem support in the form of improving regulations and increasing public awareness must run in parallel so that police efforts are more effective in the long term.

This case study of the Subdit V Cyber Polda Kaltara provides a lesson that even units with limited resources can make leaps forward through innovation, collaboration, and visionary leadership. Every challenge faced can be an opportunity to learn and transform, forming a more resilient and adaptive police organization in the digital era. In the future, this transformation journey needs to continue as new challenges emerge, with the foundation of experience that has been gained as valuable capital. The spirit to continue learning, adapting, and developing must always be a core value held by all elements of the police organization in facing the dynamics of cybercrime.

As a recommendation, the North Kalimantan Police and the National Police in general should: (1) prepare a strategic plan to strengthen cyber capacity at the regional level, including a roadmap for increasing the number and competence of personnel and IT infrastructure; (2) adopt best practices from other police forces (national and international) through knowledge exchange programs; (3) involve the community (academics, companies, society) in supporting cyber police tasks, both in prevention through education and expertise assistance; and (4) encourage the acceleration of regulations and cross-border cooperation needed to close legal loopholes in cyber law enforcement. With these comprehensive steps, the capacity of the police organization is expected to be able to keep up with the pace of technological development and the complexity of cyber threats, so that security and order in the digital space can be maintained.

REFERENCES

Aditama, P. (2025). Perbandingan Hukum Pidana Cyber Crime dan Pengaruhnya terhadap Sistem Hukum Indonesia. *Jurnal Kajian Hukum, 10*(2), 100–115.

Aditya, L. (2023). Analisa Pelatihan dan Pengembangan Sumber Daya Manusia di Polri. *Jurnal Nusa Karya, 1*(1), 1–10.

Afianto, M. (2021). Analisis Strategi Pembinaan Sumber Daya Manusia Polri dalam Meningkatkan Profesionalisme. *Syntax Literate: Jurnal Ilmiah Indonesia, 6*(3), 1–10.

Aini, N. (2024). Tantangan Pembuktian dalam Kasus Kejahatan Siber. *Judge: Jurnal Ilmu Hukum, 8*(1), 50–65.

Aldriano, M. (2022). Cyber Crime dalam Sudut Pandang Hukum Pidana. *Pembangunan Hukum, 7*(2), 1–15.

Budianto Pansariadi, R. S. (2024). Tindak Pidana Cyber Crime dan Penegakan Hukumnya. *Binamulia Hukum, 12*(2), 14.

Djarawula, M. A. (2023). Tinjauan Yuridis Tindak Pidana Kejahatan Teknologi Informasi (Cybercrime) Di Indonesia Ditinjau Dari Perspektif Undang-undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Cakrawala Ilmiah, 2*(10), 3799–3806.

Fefta, A. &. (2014). *Manajemen Publik: Teori dan Praktik.* Malang: UB PRESS.

Gigantara, L. (2021). Kesiapan Sumber Daya Manusia Kepolisian Republik Indonesia Menghadapi Revolusi Industri 4.0. *Jurnal Ilmu Kepolisian, 13*(2), 1–10.

Heri, E. I. (2019). Tantangan Pengembangan SDM Polri di Era Revolusi Industri 4.0. *Jurnal Ilmu Kepolisian, 13*(2), 1–13.

Hidayah Endang, E. e. (2021). Tantangan Pengembangan Kompetensi Aparatur Sipil Negara Menuju 'Low Cost Training' dalam Mewujudkan Reformasi Birokrasi. *Jurnal Manajemen Sumber Daya Aparatur, 9*(2), 117–127.

Indrayanti, K. W. (2018). Police's Needs for Capacity Building in Its Efforts to Prevent Cybercrime in Indonesia. *Asian Journal of Research in Social Sciences and Humanities, 9*(4), 4–14.

Irawan, B. (2016). *Kapasitas Organisasi dan Pelayanan Publik.* Jakarta: Publica Press.

Irfan, M. (2024). Optimalisasi Pengembangan Sumber Daya Manusia untuk Meningkatkan Kualitas Kinerja Polri melalui Strategi Pendekatan Talent Scouting. *Triwikrama: Jurnal Ilmu Sosial, 6*(5), 51–60.

Kasim, Z. (2024). Kebijakan Hukum Pidana untuk Penanggulangan Cyber Crime di Indonesia. *Indragiri Law Review, 2*(1), 18–24.

Loso Judijanto, B. N. (2025). Regulasi Keamanan Siber dan Penegakan Hukum terhadap Cybercrimedi Indonesia. *Sanskara Hukum dan HAM, 3*(3), 118-124.

Midarwanto, D. (2015). Pengembangan Sumber Daya Manusia Polri dalam Rangka Penegakan Hukum. *Jurnal Ilmu Kepolisian, 4*(1), 56.

Muhdiyati, S. (2024). Knowledge Management dalam Kerangka Pengembangan SDM Polri. *Jurnal Academia Praja, 1*(1), 45.

Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019). Cybercrime investigators ae users too! Understanding the socio-technical challenges faced by law enforcement. Dalam Workshop on Usable Security (USEC) 2019, San Diego

Raslin, H. e. (2021). Implementasi Penanganan dan Pembinaan SDM Polri yang Terlibat Masalah Guna Meningkatkan Kinerja. *Jurnal Ilmu Kepolisian, 13*(2), 1–10.

Syamsul Arifin, M. S. (2024). PERAN PENYIDIK KEPOLISIAN NEGARA REPUBLIK INDONESIA DALAM PENEGAKAN HUKUM CYBERCRIME. *COURT REVIEW: Jurnal Penelitian Hukum, 4*(2), 40.

Widianingrum, A. R. (2024). ANALISIS IMPLEMENTASI KEBIJAKAN HUKUM TERHADAP PENANGANAN KEJAHATAN SIBER DI ERA DIGITAL. *JOURNAL IURIS SCIENTIA, 2*(2), 90–102.

Wilson, M. T., & Cross, C. (2022). Police preparedness to respond to cybercrime in Australia: An analysis of individual and organizational capabilities. Australian & New Zealand Journal of Criminology, 55(4), 468–494researchgate.netresearchgate.net.

Winata, F. H. (2023). Kajian Manajemen dan Standar Pembinaan Sumber Daya Manusia Polri. *Justitia: Jurnal Ilmu Hukum, 1*(1), 1-12.

Yurizal. (2018). *Penegakan Hukum Tindak Pidana Cyber Crime di Indonesia,.* Malang: Media Nusa Creative.