IJSSCS
International Journal of Social Science and Community Service
https://ijsscs.com/index.php/journal
Online ISSN 3047-5406

Analysis of the Utilization of the Case Management System Model at the Intelligence Directorate of the Densus 88 Anti-Terror Unit, Indonesian National Police

Gilang Perdana Ramadhany[1], Riska Sri Handayani[2], Ahmad Ibrahim Badry[3]*

[1-3]Universitas Indonesia, Depok, Indonesia

E-mail: [1)] gilang.perdana@ui.ac.id

ARTICLE INFO

Article History
Received : 03.01.2026
Revised : 01.02.2026
Accepted : 06.02.2026
Article Type: Research Article

*Coresponding author:
Gilang Perdana Ramadhany
gilang.perdana@ui.ac.id

ABSTRACT

Integrated data management has become critical for intelligence analysis, particularly in terrorism-related crime handling. The Intelligence Directorate of Detachment 88 AT Polri faces significant challenges managing case data from multiple units and information sources. This study analyzes the utilization of a Case Management System (CMS) model in supporting intelligence analysis activities at Detachment 88. A qualitative approach was employed through in-depth interviews with key informants (Director of Intelligence, Head of Sub-Directorate of Analysis, and intelligence analysts) and document analysis of internal reports and national policies conducted during 2020-2023. Findings indicate that integrated CMS implementation positively impacts analysis speed, information accuracy, and cross-unit coordination. However, limitations persist including partial data integration due to format differences, reliance on manual verification processes, slow processing of large-volume data from social media and CCTV, and network infrastructure constraints in operational areas. System interoperability plays a crucial role in supporting timely and precise intelligence decision-making. The study identifies three critical pillars for CMS effectiveness: multi-source data integration, adaptation to evolving terrorism methods utilizing digital technology, and robust data security mechanisms including encryption and role-based access controls. CMS must evolve from a data repository to an AI-enabled analytical platform with automated data fusion, modular architecture, and layered security protocols to effectively counter dynamic terrorism threats while maintaining strict confidentiality standards.

Keywords: Case Management System, Data Integration, Densus 88, Intelligence Analysis

1. Introduction

Advances in information technology have meant that security agencies, including intelligence agencies, are faced with ever-increasing volumes of data. In such circumstances, the ability to manage information quickly and accurately is a non-negotiable requirement, especially when the data comes from multiple sources with varying degrees of accuracy. This challenge is also felt by Special Detachment 88 (Densus 88), which still faces limitations in its case management system. Some of the obstacles that often arise include slow data processing, lack of integration between platforms, and difficulties in adapting to ever-changing crime patterns, particularly terrorism, which makes extensive use of digital technology. These conditions can slow down the response in emergency situations. The need to improve these conditions has led to the development of a more integrated and responsive Case Management System (CMS). The new system is expected to combine various data elements into a single platform that is easily accessible in real time, thereby helping to speed up analysis and decision-making. With the support of such a system, Densus 88 can be more adaptive in facing dynamic terrorism threats and ensure that decisions are made based on accurate and up-to-date information. In

addition to supporting daily operations, the development of the CMS is also aimed at strengthening the organisation's resilience in facing future security challenges.

Ratcliffe (2005) through his work Integrated Intelligence and Crime Analysis, he shows that cross-source data integration can improve the effectiveness of law enforcement agencies in making strategic decisions. However, he also emphasises the importance of strengthening data security because the risk of leaks increases with the use of more complex technology. Without proper integration, case management systems tend to run separately and make comprehensive analysis difficult. Research by Ikhssani et al. (2024) entitled Cybersecurity and Intelligence Governance also emphasises that limited system integration in Indonesia remains an obstacle to intelligence work. He points out that platform differences and a lack of interoperability slow down the process of analysis and information exchange. In his study, Ikhssani recommends the development of an integrated CMS capable of consolidating field intelligence data, CCTV recordings, digital forensic findings, and analysis reports into a single interconnected system. This study is novel because it focuses on the context of the Indonesian National Police, particularly Densus 88. Unlike previous studies, which were more general in nature (Ratcliffe, 2005; Ikhssani et al., 2024), this research offers a CMS model that not only integrates data in real time but also supports inter-unit collaboration. With a more structured system, analysts, field operators, and leaders can access the same information when needed, resulting in faster decision-making and minimising miscommunication.

In addition to addressing data integration issues, this study also highlights the aspect of information security. The developed CMS offers stronger data protection mechanisms through the use of encryption, role-based access settings, and threat detection features tailored to ever-changing patterns of terrorism. With this approach, the system functions not only as a daily work tool but also as part of a long-term strategy to maintain information confidentiality and prevent data misuse. The CMS is designed to be able to keep up with changes in terrorist tactics. Every decision made through the system is expected to be based on valid and up-to-date data. In practice, the existence of an integrated CMS allows analysts, field operators, and leaders to access the same information without having to wait for manual distribution processes. This kind of shared access helps speed up analysis, reduces the potential for errors due to fragmented data, and accelerates case handling processes. The development of a more advanced CMS reflects the needs of modern organisations such as Densus 88 to manage data efficiently. This system not only collects information, but also acts as a strategic framework that helps organisations respond to threats more quickly and accurately. With these capabilities, CMS supports improved operational efficiency, strengthens data security, and assists in more accurate and evidence-based decision-making. Overall, this study seeks to develop a CMS model that suits the current operational needs of Densus 88. It is hoped that this system can become a strategic foundation for strengthening the effectiveness of case management in the Densus 88 Intelligence Directorate.

In formulating issues related to the development of an integrated case management system, there are several challenges that need to be considered. The system developed must not only support the operational needs of Densus 88 in terms of speed and effectiveness, but also be capable of maintaining the security and confidentiality of the data managed. This research aims to answer questions about how to design a system capable of combining and processing data from various sources to accelerate decision-making, adapt to developments in technology and methods of terrorism, and implement strategies to maintain the security and privacy of sensitive data. Theoretically, this research is expected to contribute to the development of data integration theory, information system security theory for highly confidential systems, and decision-making theory in dynamic environments. From a practical perspective, the benefits of this research include improving the operational effectiveness of Densus 88, adapting to changes in terrorist crime methods, and strengthening data security and protection to support national security.

The primary objective of this research is to develop and propose a comprehensive, secure, and adaptive model for an integrated case management system specifically tailored for Densus 88 AT Polri. This research is limited to the period 2020 to 2023, focusing on the process and use of the case management system at Densus 88 AT Polri. This period was chosen because it represents an important phase of digital transformation and the complexity of terrorism threats involving the physical and digital realms. The research subjects include the Director of Intelligence, the Head of the Sub-Directorate of Analysis and Products, and intelligence analysts, who were selected purposively due to their direct involvement in the implementation of the system.

This limitation is expected to provide a complete picture of the internal dynamics in developing an effective system, while also producing relevant recommendations for future improvements.

2. Literature Review

2.1. Case Management

Management is a key concept that regulates resources such as people, information, and time through the processes of planning, organising, directing, and controlling to achieve organisational goals effectively and efficiently. In its development, management is also understood as a form of knowledge management that transforms information into meaningful knowledge to support decision-making and organisational learning (Sridevi, 2021). According to Sridevi (2021), management is a combination of systematic science and art that requires intuition and creativity in its application. The modern environment demands adaptive and strategic management, capable of responding to technological changes, social dynamics, and global competition. Sorokina & Epishkin (2016) emphasises that management must maintain harmony between structure, strategy, and technology with the organisation's long-term goals, as well as function as a bridge between human needs and technological developments. In addition, effective management also considers social and ethical aspects, builds an adaptive work culture, and encourages integrity and innovation for organisational sustainability.

2.2. Operational Management

According to experts, operational management is a series of core organisational activities to efficiently transform inputs into quality outputs. Russell & Taylor (2009) defining it as an activity that manages resources such as raw materials, equipment, and labour to ensure that the production process runs consistently and efficiently, taking external factors into account. In modern practice, information technology is utilised to accelerate data flow and support decision-making. Porter (2011) emphasising its three main components: customer focus, efficient processes, and capacity in line with demand.

Heizer et al. (2020) emphasises the importance of operational management due to its role in connecting marketing, finance and production functions, as well as improving resource efficiency, cost control and profitability as the foundation for providing valuable products or services. Heizer et al. (2020) identify ten key decisions in operational management: product and service design, quality management, process and capacity design, location selection, layout design, human resource management and job design, supply chain management, inventory control, scheduling, and facility maintenance.

2.3. Warehouse (Cloud Base)

A warehouse, according to the Big Indonesian Dictionary (KBBI), is a place to store goods before they are used, sold, or distributed. Its function is very important in maintaining the availability of goods and the smooth flow of distribution. Porter (2011) emphasises that a warehouse is not just a static storage space, but an active part of the logistics system that manages and connects the production process with distribution, including activities such as sorting, consolidation, and packaging. In modern supply chains, warehouses serve as distribution centres that optimise the flow of goods, reduce costs, prevent damage, and improve operational efficiency through good governance and function as buffer stock to balance supply and demand.

Technological developments are increasingly changing the role of warehouses. The concept of Warehouse Management System (WMS) described by Hompel and Schmidt (2007) automates warehouse activities such as arrangement, stock monitoring, and recording to improve accuracy and speed. Integrated information systems, as described by Laudon et al. (2021) coordinate data and processes to support more transparent and effective decision-making. With the support of technologies such as sensors, IoT, and data analytics, modern warehouses can monitor conditions in real-time, predict stock requirements, and optimise goods rotation. Thus, warehouse management has evolved into a strategic component in businesses that emphasise efficiency, timeliness, and service quality.

2.4. Research Model

Case management at Densus 88, as an institution that deals with terrorism issues, is highly complex because it requires quick and accurate decisions. The use of a Case Management System (CMS) is crucial for setting priorities, managing information, and ensuring efficient analysis. The theoretical model underlying this study describes an integrated data management system consisting of three main stages for assessing CMS implementation.

The first stage is real-time data collection, which describes the process of continuously gathering information from various sources such as field reports, digital forensic data, CCTV recordings, social media, and internal databases to maintain an up-to-date picture of the situation. The second stage, process data as it flows, involves processing the collected data through cleaning, standardisation, transformation, and consolidation from various sources to produce accurate and analysable information. The third stage, explore and visualise, involves presenting the analysis results in visual forms such as dashboards or analytical reports to facilitate the identification of patterns, relationships, and potential threats.

Overall, this model emphasises that the effectiveness of CMS depends on three key aspects: speed of data collection, accuracy of information processing and integration, and the ability to present relevant and easy-to-understand analysis results. These three aspects are vital foundations for the development of CMS at Densus 88 so that it can respond effectively to the dynamics of terrorism threats in the digital age.

2.5. Previous Research

Several previous studies have examined the application of data and analytics technology in law enforcement institutions. Afzal and Panagiotopoulos (2025) found that data analytics can improve police effectiveness through structured data management and crime prediction, despite facing challenges in organisational culture and ethics. Similar findings regarding the potential and concerns were reported by Neiva et al. (2023), where police professionals saw the benefits of Big Data for prediction and investigation, but also expressed concerns about data bias, privacy, and misuse. The risks and opportunities of using advanced technology are further discussed by Kaufmann (2024), who highlight that AI can accelerate case analysis but carries the risk of bias and the need for a strong regulatory framework.

Specifically, the study by Afzal and Panagiotopoulos (2025) emphasises that integrated data management is at the heart of modern police innovation, influencing early detection and strategic decision-making. Meanwhile, Laufersweiler-Dwyer and Dwyer (2000) demonstrate that prescriptive analytics systems can improve resource allocation and case prioritisation. In the context of criminal intelligence, Murthy and Siddesh (2023) prove the effectiveness of AI-based systems for risk assessment and terrorist network modelling, while Bartlett and Reynolds (2015) emphasise the benefits of social media intelligence for counter-terrorism, noting the importance of integrated case management systems. Finally, Brayne (2021) reminds us that although data analytics makes investigations increasingly dependent on digital systems, control over the risks of algorithmic bias and over-policing is necessary through good governance.

2.6. Conceptual Framework and Hypothesis

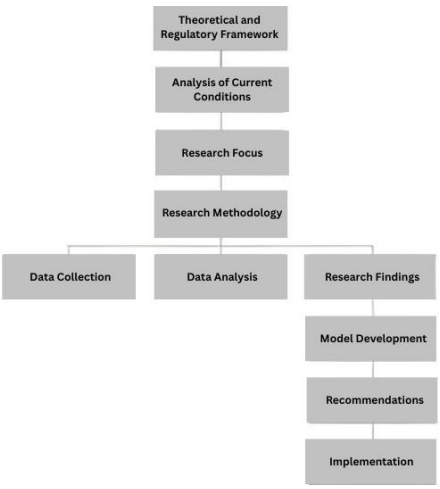

Figure 1. Conceptual Framework

Based on the framework illustrated in Figure 1, the hypothesis obtained for this study is:

H_1: The use of an integrated and efficiently run CMS at Densus 88 increases the effectiveness of terrorism case handling, particularly in the process of identification, case prioritisation, and coordination between units.

H_0: The use of CMS at Densus 88 does not have a significant impact on the effectiveness of terrorism case handling.

3. Methodology

3.1. Research Approach

This study uses a qualitative approach because the implementation and effectiveness of the Case Management System (CMS) in Densus 88 is complex and contextual, requiring a deep understanding of the experiences and views of direct users in a work environment that is highly confidential and demands quick decisions. Philosophically, this approach views social reality as pluralistic and constructed through the interpretation of actors' experiences, enabling comprehensive analysis not only of technical aspects but also of socio-cultural factors within the organisation, such as work culture and command structures that influence technology adoption (Lincoln & Guba, 1985). The flexibility of the qualitative approach allows the research focus to be adjusted according to findings in the field, resulting in a holistic analytical foundation that provides conceptual contributions and practical recommendations for the development of a more adaptive system.

3.2. Research Type

This study uses a naturalistic qualitative approach with a case study design to gain an in-depth understanding of the implementation and effectiveness of the Case Management System (CMS) at the Densus 88 Intelligence Directorate, focusing on interpreting patterns and meanings from empirical data in the field. This case study was chosen because the boundaries between the phenomenon and the sensitive organisational context cannot be clearly separated (Yin, 2018), with the aim of comprehensively describing the interaction between the technical aspects of the system, actors, and organisational culture. Data collection was carried out through triangulation of direct observation techniques, in-depth interviews with key informants, and documentation studies, so as to provide a complete picture of the utilisation, challenges, and contributions of CMS, as well as recommendations for system development and literature in the field of security.

3.3. Data Sources and Data Collection Techniques

The data sources for this study consist of primary and secondary data. Primary data was collected directly from primary sources through in-depth interviews with key informants (such as the Director of Intelligence and Densus 88 analysts) and direct observation at Densus 88 headquarters to understand the actual implementation and dynamics of the Case Management System (CMS). Meanwhile, secondary data was obtained from internal documents such as telegrams and activity reports, as well as external documents such as national policies, to provide a broader context for the research.

Data collection was carried out using triangulation by combining observation techniques, in-depth interviews, and documentation studies. This approach enabled the research to not only describe the technical aspects of the CMS, but also to analyse the social and cultural dimensions of the organisation that influence its implementation. Thus, the research is expected to provide a comprehensive picture of the CMS's function in supporting Densus 88's operational performance, as well as to produce theoretical contributions and practical recommendations for the development of a more effective system.

3.4. Research Process

In this qualitative study, the main instrument was the researcher himself as a living instrument who conducted direct observation, listening and interpretation in the field to understand the social context and meaning behind the implementation of the Case Management System (CMS) at Densus 88. Supporting instruments in the form of interview guidelines, observation sheets and documentation formats were used to ensure systematic data collection. The data analysis process follows an interactive model. Miles & Huberman (1994), which includes data reduction to focus on themes, presentation of data in narrative or matrix form to identify patterns, and drawing conclusions that are continuously verified. Data validity is tested through

triangulation techniques, both source triangulation by comparing data from various informants and documents, and method triangulation by comparing findings from observations, interviews, and documentation studies, to ensure the consistency and validity of research findings.

4. Results and Discussion

4.1. Description of Research Objects

The object of this study is the utilisation of the Case Management System (CMS) at the Directorate of Intelligence of Densus 88 AT Polri, which functions as the backbone of intelligence operations to integrate various stages from data collection to threat analysis in handling terrorism cases. In the face of rapidly evolving and increasingly asymmetrical threats, including the use of digital space, CMS plays an important role in processing large amounts of data from various sources such as field reports, wiretaps, and digital forensics into fast, accurate, and structured information. This enables faster analysis of threat patterns through automatic classification and relationship mapping features, while also supporting the analysis of terrorist networks by visualising the structure, communication patterns, and roles of individuals within a network.

Furthermore, the CMS serves as the basis for strategic decision-making by presenting threat trends and the dynamics of the digital space, such as the spread of radical content through Social Media Intelligence (SMI), in order to formulate appropriate preventive measures. This system also facilitates coordination between relevant agencies, such as BIN and BNPT, by ensuring fast and secure information exchange, so that operational responses can be more integrated and bureaucratic obstacles minimised. Overall, the CMS is positioned as a key component in building adaptive and collaborative intelligence capabilities, where evaluation of its utilisation is expected to identify its real contribution to work effectiveness and aspects that need to be refined to address future threats.

4.2. Multi-Source Data Integration for Analysis and Decision-Making Efficiency

Multi-source data integration is a fundamental element in the development of the CMS at the Densus 88 AT Polri Intelligence Directorate because the nature of modern terrorism threats demands speed, accuracy, and collaboration across information sources. The complexity of threats that combine physical and digital dimensions requires a system that is not only capable of collecting data, but also connecting, interpreting, and presenting the results of analysis in an integrated manner. The findings of Afzal and Panagiotopoulos (2025) show that the effectiveness of law enforcement is highly dependent on the system's ability to manage and integrate data in a structured manner to support timely crime prediction and detection. These findings are in line with the context of Densus 88, where various types of data, such as field intelligence reports, digital forensics, CCTV, OSINT, and social media data, must be processed in a single analytical platform capable of producing a comprehensive situational overview.

However, this study found that the CMS currently in use still functions partially; data from various units is not yet fully integrated due to differences in format, metadata limitations, and the dominance of manual verification. This situation causes delays in analysis and a lack of real-time information. This is reinforced by a statement from the Director of Intelligence at D88 BP. TAP, who said: *"We usually receive field data through standardised internal channels, while digital and social media data is processed first by the analysis unit before being combined at the central level. This process is ongoing, but it is not yet fully efficient because there are still manual verification stages."* This phenomenon is consistent with the results of the scoping review by Neiva et al. (2023), which revealed that Big Data in policing will only yield maximum benefits if cross-source integration is carried out systematically and supported by adequate technical infrastructure. Without such integration, most data becomes noise, redundant, or unusable in emergency situations.

Interviews with key informants revealed that although Densus 88 has SOPs for data integration, their implementation still faces technical obstacles. Narrative reports of field operations often require manual conversion to be compatible with digital data, while social media data requires a process of filtering for relevance and validity. The Deputy Director of Analysis at D88 IMW confirmed these challenges, stating: *"Specifically for social media data, we must first perform manual filtering to ensure that the information entered is truly relevant. There is a lot of manipulative content or hoaxes circulating, so it cannot be directly entered into the system."*

Bartlett and Reynolds (2015) explained something similar, stating that Social Media Intelligence (SOCMINT) will only be effective if it is supported by a case management system capable of automatically validating public and digital-based information.

Given these conditions, the Densus 88 CMS still resembles a data repository rather than an intelligence analytics system. According to Kaufmann (2024), AI-based systems in law enforcement should be capable of cross-format integration, automatic analysis, and pattern detection to support the speed of investigations. The lack of automation in the CMS means that the knowledge transformation process is not optimal because analysts still rely on manual input. Another technical constraint was revealed by the KP monitoring unit head, DCG: *"The system cannot yet read all data formats automatically. Sometimes we have to convert or change the data first before it can be entered into the CMS."*

From an operational decision-making perspective, research by Laufersweiler-Dwyer and Dwyer (2000) shows that prescriptive analytics can recommend task allocation, case prioritisation, and resource distribution more efficiently when the system has a good data integration structure. This is relevant in the context of Densus 88, which requires quick recommendations for threat mitigation. Meanwhile, AI-based criminal intelligence systems, as described by Murthy and Siddesh (2023), have been proven to strengthen terrorist network analysis and risk assessment when the data used is standardised.

In addition, limitations in network infrastructure in some of Densus 88's operational areas also hinder data synchronisation. Field Operator Dit Intel D88 BK. HS emphasised this constraint: *"The internet network in several operational areas is limited, so the data we send does not always go directly to the central system. This often causes delays."* When connectivity is slow, data updates are delayed, disrupting pattern detection and analysis of relationships between incidents. This is reinforced by the findings of Afzal and Panagiotopoulos (2025), which confirm that the quality of data integration in policing directly affects the speed of analysis and accuracy of early detection.

Efficient data integration is also the basis for establishing accurate situational awareness. In this case, Brayne (2021) emphasises that modern investigations are highly dependent on data analytics-based case management systems, as only such systems are capable of simultaneously connecting patterns of events, actors, locations, and times. If data integration does not work well, the risk of bias, misidentification, and over-policing increases.

The findings of this study are in line with the global research consensus that the main value of a CMS lies in its ability to perform data fusion, which is combining various types of data into new knowledge that supports strategic decisions. When a CMS is able to combine field data, digital forensics, visual recordings, OSINT, and SOCMINT data in a single platform, the system functions as an intelligence hub that strengthens cross-unit coordination and rapid response to terrorist threats. Thus, multi-source data integration is not only a technical necessity, but also a strategic foundation for a modern intelligence-based national security system.

4.3. Adapting the System to the Dynamics of Technology and Methods of Terrorism

The changing global security landscape over the past two decades shows that terrorist groups are becoming increasingly adept at using technology to support their operations. Whereas in the past, communication and coordination of terrorist acts were carried out through physical meetings, couriers, or conventional methods of communication, radical groups now use various digital platforms to hide their tracks and expand their reach. Social media is used for propaganda, recruitment, and the dissemination of extremist narratives, while encrypted messaging applications have become a means of planning attacks and sharing sensitive information securely. Fake digital identities, the use of VPNs, end-to-end encryption, and the dark web have become part of operational strategies that make it difficult for authorities to track the patterns of perpetrators' activities in a short period of time. This situation is entirely in line with the findings of Bartlett and Reynolds (2015), which show that global radical groups are increasingly relying on digital traces to move in a decentralised manner. The Head of Sub-Directorate D88 IMW added that 'Terrorists are now increasingly adept at using encrypted messaging applications and fake social media accounts to disguise their activities, making it difficult to distinguish radical communication from normal communication.' In other words, digital transformation not only makes it easier for terrorists to operate, but also changes the nature of the threat to be faster, more adaptive, and more difficult to predict using traditional investigation methods.

In this situation, the CMS at the Densus 88 AT Polri Intelligence Directorate is required to evolve from a mere data repository into an analytical platform capable of integrating cross-format data in real time. The complexity of modern threats requires the CMS to be able to read the relationships between events, recognise suspicious patterns, and provide a comprehensive situational overview with the support of artificial intelligence (AI) technology. Research by Partridge and Zaghloul (2025) provides a strong foundation that the effectiveness of modern investigations is highly dependent on the ability of information systems to manage heterogeneous data, make pattern-based predictions, and optimise resource allocation in case handling. With the integration of CDR, OSINT from social media, CCTV recordings, and data from field operations, CMS has the potential to become a comprehensive and responsive intelligence workspace for evolving threats.

However, research shows that the CMS currently in use still faces significant obstacles, particularly in terms of processing speed and threat detection accuracy. Large amounts of data from social media, CCTV, and open sources require long processing times, while information noise often masks the actual threat signals. Director of Intelligence D88 BP. TAP highlighted this weakness: *"The weakness of the current system lies mainly in the speed and accuracy of threat detection. Large amounts of data, particularly from social media and CCTV, still take a long time to process, while information noise often slips through because the system does not yet have an effective automatic filtering mechanism."* This situation is exacerbated by the lack of automatic filtering mechanisms and the limitations of algorithms in distinguishing important information from routine digital activity. These findings are reinforced by a scoping review by Neiva et al. (2023), which states that the quality of Big Data analysis in policing is highly dependent on the system's ability to filter data and integrate cross-format information structures. Without these capabilities, the system will remain reactive and unable to meet the rapid analysis needs required in counter-terrorism.

Furthermore, the development of terrorist groups' ability to manipulate digital platforms significantly increases the technical challenges for law enforcement agencies. Perpetrators now use digital impersonation techniques, burner accounts, and layered encryption to obscure their identities and locations. Kaufmann (2024) assert that the use of AI in policing can help overcome some of these problems, but only if the system is able to reduce algorithmic bias, improve threat classification accuracy, and comply with strict governance standards. Weak AI or AI trained with non-standardised data risks producing false positives and false negatives that can jeopardise field operations.

The integration of CMS with AI visual analytics-based CCTV networks is one of the most promising forms of adaptation. Through this integration, the system can automatically perform facial recognition, object tracking, and detection of suspicious behaviour, without waiting for manual analysis. Findings by Murthy and Siddesh (2023) show that AI-based criminal intelligence systems are capable of identifying terrorist network patterns, mapping relationships between entities, and detecting abnormal activities based on movement parameters and spatial interactions. When CCTV recordings are combined with geotagging, the system can provide spatial-temporal information that helps speed up the analysis of the chronology of events and narrow down the perpetrator's movements in a short time.

However, for all the potential of this technology to work optimally, the CMS architecture design must be modular, scalable, and flexible. The Head of Sub-Directorate D88 IMW emphasised the importance of modularity: *"The CMS must be designed to be modular, meaning that if there is new technology such as biometric analysis or encrypted communication pattern detection, the module can be added immediately without having to rebuild the entire system."* Modularity facilitates the integration of new features such as biometric analysis, encrypted communication detection, or OSINT modules without disrupting the entire system. Afzal and Panagiotopoulos (2025) emphasise that the sustainability of innovation in modern policing requires a system architecture that is capable of keeping up with changes in the environment and types of threats. Non-modular systems will quickly become obsolete, difficult to update, and incompatible with new technologies that continue to emerge in the world of intelligence and security. Director of Intelligence D88 BP. TAP emphasises this flexibility: *"The system must not be rigid; it must be continuously updated in line with the dynamics of threats, so that any new data that comes in can be processed immediately to support quick decisions."*

Technological adaptation must also be accompanied by an increase in human resource capacity. Brayne's (2021) research shows that the success of police information systems depends on the ability of personnel to understand how algorithms work, read automated analysis results, and apply critical logic in assessing system

output. In the Densus 88 environment, the technical competence of analysts and operators is crucial in determining whether the CMS is capable of producing accurate and timely intelligence. Without adequate digital literacy, sophisticated systems remain at risk of not being utilised to their full potential.

The next challenge is inter-agency interoperability. The information received by Densus 88 comes from BIN, BNPT, Polda, immigration, and various other agencies that use different data formats and protocols. Manual conversion processes are still often necessary, which causes delays in the flow of information and increases the risk of technical errors. The Head of the D88 IMW Analysis Sub-Directorate confirmed: *"Often, the data we receive from other agencies is not in a uniform format, so it takes additional time to convert it before it can be analysed in the CMS."* Findings by Laufersweiler-Dwyer and Dwyer (2000) show that prescriptive analytics can only work optimally if data between units has a uniform structure and can be exchanged without barriers. The implementation of a shared encryption protocol, standard APIs, and uniform metadata tags are mandatory requirements for efficient and secure cross-agency integration. This interoperability challenge was also emphasised by the Director of Intelligence D88 BP. TAP: *"The biggest challenge in CMS development today is not only the technological aspect, but also the system's ability to be integrated across agencies while maintaining data confidentiality."*

Strategically, an adaptive CMS is not just an operational tool, but also an intelligence decision support system platform capable of providing comprehensive overviews of threats to leadership. With cross-source data integration, AI analytics capabilities, and cross-agency interoperability, CMS can become a key node in the national intelligence ecosystem. This system can strengthen collaboration, increase response speed, and encourage more accurate strategic decisions in the face of increasingly dynamic terrorist threats. Based on previous research, the direction of modern CMS development must shift from an administrative paradigm to a data-driven and AI-enabled model that is capable of responding to the evolution of threats in the digital era more quickly, adaptively, and precisely.

4.4. Data Security and Privacy Strategy in the Integrated Case Management System

Data security and privacy are key foundations in CMS management, especially for the Indonesian National Police's Densus 88 AT Intelligence Directorate, which handles sensitive information related to terrorist networks on a daily basis. The data managed includes not only operational records, but also field intelligence reports, communication recordings, digital forensics results, perpetrator identities, and digital activities obtained from OSINT and SOCMINT. Leaks or misuse of such data can disrupt investigations, endanger personnel safety, and weaken counter-terrorism strategies. Therefore, CMS security and privacy strategies must be designed comprehensively and consistently with the dynamics of modern threats. Director of Intelligence D88 BP. TAP emphasised this urgency: *"The level of data confidentiality at Densus 88 must be maintained with the highest security standards, because even the smallest leak can be exploited by terrorist networks to paralyse operations."*

In the context of large-scale intelligence data processing, the findings of this study indicate potential risks to data protection. Therefore, the DPIA concept is relevant as a conceptual approach to assessing and mitigating data protection risks in the development and utilisation of CMS. DPIA serves as an evaluative mechanism to identify potential impacts on data rights and security, particularly in the collection, processing, and analysis of sensitive and massive intelligence data.

From a technical perspective, CMS needs to implement layered protection principles to maintain data security. Research by Partridge and Zaghloul (2025) emphasises that digital policing systems that handle sensitive data require strong security infrastructure, including end-to-end encryption, layered authentication, and real-time threat monitoring. In an interview regarding measures to protect confidential data, the Director of Intelligence at D88 BP. TAP emphasised: *"Data protection must begin at the technical level with the use of end-to-end encryption, multi-layered authentication, and regularly updated firewalls, so that data remains secure even in the event of a hacking attempt."* In addition, distributed backup and disaster recovery mechanisms must be implemented to ensure data availability in the event of disruptions, sabotage, or cyber attacks. The findings of Afzal and Panagiotopoulos (2025) also show that the integrity of police systems is highly dependent on the quality of technical architecture that is capable of protecting data while maintaining information consistency across units.

However, technical protection alone is not enough. Procedural aspects play an important role in preventing internal data misuse. Audit trails that record all user activities help ensure accountability and detect behavioural anomalies. The Head of Sub-Directorate D88 IMW emphasised the importance of this mechanism: "*Audit trails in CMS are very important because through user activity logs, we can ascertain who accessed the data, when, and for what purpose. Without this mechanism, the risk of misuse would be difficult to track."* The need-to-know principle or role-based access restrictions are important mechanisms for reducing the risk of internal leaks. The Deputy Director of Analysis D88 IMW also added a procedural aspect: *"Access procedures must be strictly regulated based on the need-to-know principle, meaning that not all personnel can access all data, but only according to operational needs and their authority."* This is reinforced by the findings of Neiva et al. (2023), which confirm that the risk of Big Data misuse in policing often occurs not because of the technology, but because of weak procedural controls and access governance at the user level.

From a managerial perspective, data security requires strong and consistent organisational policies. Digital security literacy training, incident handling simulations, and regular audits are necessary to ensure personnel readiness. Head of Monitoring Unit D88 KP. DCG emphasised this human resource aspect: "*Regular training for personnel is very important, because weaknesses often arise from human error. Without adequate cyber security literacy, even the most sophisticated systems can remain vulnerable."* Kaufmann (2024) show that the use of AI and digital systems in policing carries the risk of misidentification and algorithmic bias, requiring clear internal regulations on data governance, correction mechanisms, and oversight of technology use. In other words, data protection is not just about software, but also about how organisations prepare their human resources to manage these technologies safely.

Inter-agency coordination is a strategic component in maintaining CMS data security. The information managed by Densus 88 comes from various institutions such as BIN, BNPT, and Polda. Without a secure and standardised data sharing protocol, the risk of data inconsistency and potential leaks increases. Director of Intelligence D88 BP. TAP explained the existing coordination mechanism: "*Coordination is carried out through standardised data sharing protocols and is always supervised by leadership, so that all incoming and outgoing information is recorded and protected."* Deputy Director of Analysis at D88 IMW added: *"We use regular coordination forums with BIN, BNPT, and regional police to standardise encryption procedures and ensure that shared data complies with national security standards."* Bartlett and Reynolds (2015) emphasise that SOCMINT and digital intelligence are only effective if there is a consistent, protected, and verifiable data exchange mechanism. The implementation of shared encryption protocols, metadata standards, and integrated APIs is necessary to maintain cross-agency data security.

At the operational level, CMS needs to implement a tiered access system to ensure that sensitive information can only be accessed by certain personnel. This is important because Brayne's (2021) research shows that data analytics-based investigation systems are highly vulnerable to abuse when access is not properly mapped. Senior analyst D88 BK. HS emphasises this principle from a field perspective: *"The system must be equipped with tiered access, so that the field data we send is not immediately fully accessible to all levels, but is filtered according to need and authority. This is important to maintain the confidentiality of operations."* Restricting access not only prevents leaks, but also improves the accuracy of the information received by analysts in the field, as each piece of data is filtered according to the level of authority. On the other hand, data security is also related to the effectiveness of analytics. Research by Murthy and Siddesh (2023) found that AI-based criminal intelligence systems will only be optimal if the data received is clean, standardised, and secure. Unprotected or unverified data can corrupt AI models and produce erroneous conclusions. In the context of CMS, data security plays a dual role which are protecting sensitive information and maintaining the quality of artificial intelligence-based analysis.

Laufersweiler-Dwyer and Dwyer (2000) emphasise that prescriptive analytics in policing requires secure and consistent data to produce valid recommendations. Thus, security and privacy are not only technical issues, but directly affect the quality of decision-making in counter-terrorism operations. Strong data security creates trust between units and institutions. Afzal and Panagiotopoulos (2025) show that the success of police information systems is highly dependent on trust within the organisation, as trust influences the smooth flow of data and collaboration. In the context of Densus 88, this trust is the foundation of effective operational cooperation, especially in the face of fast-moving and complex terrorist threats. This operational coordination is also emphasised by Senior Analyst D88 BK. HS: *"Whenever there is a joint operation, data access is regulated in*

stages according to each team's tasks, so that not all parties can see all the information, only the parts relevant to their responsibilities."

5. Conclusion

Based on the results of the study, the effectiveness of the modern intelligence system at Densus 88 AT Polri is determined by three main pillars that are interrelated: data integration, technology adaptation, and information security. Currently, the case management system (CMS) is still in the transition phase from mere data storage to an integrated analytical platform. Major obstacles such as differences in data formats between agencies, reliance on manual conversion, and limited network infrastructure slow down the integration of multi-source data ranging from field reports, social media, to CCTV recordings, resulting in delays in analysis and strategic decision-making. Therefore, CMS development needs to focus on automating data merging and validation to create real-time and accurate situational awareness.

Furthermore, CMS must be able to adapt to the dynamics of terrorism threats that increasingly utilise digital technology, such as encrypted messages and false identities. This adaptation requires the integration of advanced technologies such as artificial intelligence for CCTV visual analysis and threat pattern detection, as well as a modular system design that is easy to update. On the other hand, sensitive data security is an absolute foundation that requires a layered approach ranging from encryption, audit trails, to access restrictions based on needs, and must be supported by personnel training and standard coordination between agencies. By strengthening these three pillars in a balanced manner, CMS can transform into a reliable, fast, and secure intelligence decision support system, thereby becoming an effective national intelligence hub in the face of complex terrorist threats.

6. References

Afzal, M., & Panagiotopoulos, P. (2025). Data in policing: An integrative review. *International Journal of Public Administration*, *48*(7), 411–430.

Bartlett, J., & Reynolds, L. (2015). *The State of the Art 2015: a literature review of social media intelligence capabilities for counter-terrorism*. Demos London.

Brayne, S. (2021). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press.

Heizer, J., Render, B., & Munson, C. (2020). *Operations management: Sustainability and supply chain management*. Pearson.

Hompel, M. Ten, & Schmidt, T. (2007). *Warehouse management: Automation and organisation of warehouse and order picking systems*. Springer.

Ikhssani, A., Mudra, C., & Prasidya, F. G. (2024). Cybersecurity dan Tata Kelola Intelijen. *Jurnal Kajian Stratejik Ketahanan Nasional*, *7*(1), 1–10. https://doi.org/10.7454/jkskn.v7i1.10086

Kaufmann, M. (2024). AI in policing and law enforcement. In *Handbook on Public Policy and Artificial Intelligence* (pp. 295–306). Edward Elgar Publishing.

Laudon, K. C., Laudon, J. P., & Traver, C. G. (2021). *Essentials of Management Information Systems Fouteenth Edition Global Edition*. Pearson.

Laufersweiler-Dwyer, D. L., & Dwyer, R. G. (2000). Profiling those impacted by organizational stressors at the macro, intermediate and micro levels of several police agencies. *Criminal Justice Studies*, *12*(4), 443–469.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry. Newberry Park*.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

Murthy, J. S., & Siddesh, G. M. (2023). AI Based Criminal Detection and Recognition System for Public Safety and Security using novel CriminalNet-228. *International Conference on Frontiers in Computing and Systems*, 3–20.

Neiva, L., Machado, H., & Silva, S. (2023). The views about Big Data among professionals of police forces: A scoping review of empirical studies. *International Journal of Police Science & Management*, *25*(2), 208–220. https://doi.org/10.1177/14613557231166225

Partridge, J., & Zaghloul, F. (2025). Policing the data: Can data analytics help law enforcement? *Journal of Information Technology Teaching Cases*, *15*(1), 90–94. https://doi.org/10.1177/20438869231212214

Porter, M. E. (2011). *Competitive advantage of nations: creating and sustaining superior performance*. simon and schuster.

Ratcliffe, J. (2005). The Effectiveness of Police Intelligence Management: A New Zealand Case Study. *Police Practice and Research*, *6*(5), 435–451. https://doi.org/10.1080/15614260500433038

Russell, R. S., & Taylor, B. W. (2009). *Operations Management: Along the Supply Chain*. Wiley.

Sorokina, A. V, & Epishkin, I. A. (2016). Management by Objectives and Motivation for Strategy Implementation. *World of Transport and Transportation*, *14*(3), 262–269.

Sridevi, K. B. (2021). Filling the quality gaps for a futuristic management education. *Journal of Economic and Administrative Sciences*, *37*(4), 393–400. https://doi.org/10.1108/JEAS-09-2018-0097

Yin, R. K. (2018). *Case study research and applications*. Sage Thousand Oaks, CA.