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.

The Security Intelligence Gathering Debate between Human Intelligence (Humint) versus Technological Intelligence (Techint)

Ade Mulya[1], Semiarto Aji Purwanto[2], Angel Damayanti[3], Hizkia Yosias Polimpung[4], Yogha Restu Pramadi[5], Prasetyo Adi Wibowo Putro[6]
[1]Sekolah Tinggi Ilmu Kepolisian, Jakarta, Indonesia, ade.mulya@polri.go.id
[2]Universitas Indonesia, Jawa Barat, Indonesia
[3]Universitas Kristen Indonesia, Jakarta, Indonesia
[4]Universitas Monash Malaysia, Subang Jaya, Malaysia
[5]Cardiff University United Kingdom, Wales, United Kingdom
[6]Politeknik Siber dan Sandi Negara, Jawa Barat, Indonesia

Corresponding Author: ade.mulya@polri.go.id[1]

Abstract: This article aims to compare security intelligence collection with humint and techint approaches to obtain intelligence information for security and public order purposes. The research on intelligence collection emphasizes the elements of intelligence focus, strengths, and challenges as well as prospective trends in intelligence application, by examining it from micro, meso and macro perspectives. The approach was adopted with interviews of security intelligence officers and literature review based on secondary sources, combined with an analysis of the challenges of intelligence collection faced in dealing with security threats and the evolving intelligence technology landscape and the role of humans in the future. The findings reveal that intelligence collection has made great strides due to the impact of information, communication and computer technology. However, human intelligence remains indispensable and continues to coexist with technological advancements due to the unique and irreplaceable qualities of humans compared to devices and machines.

Keywords: Intelligence Gathering, Security Intelligence, Technological Intelligence, Human Intelligence

INTRODUCTION

Security intelligence focuses on supporting the function of the state police, with the main aim of maintaining social stability and order as well as preventing and enforcing laws against crime (Telep et al., 2018) Given this crucial role, this article will discuss intelligence gathering in several countries to provide a more comprehensive picture.

Based on various academic studies, there is a significant focus on changes and dynamics in the collection of security intelligence between countries. In the last decade, there have been major changes in the operations of security and intelligence agencies across Europe, affecting all agencies (Brodeur, 2007). The increasing threat of transnational terrorism, such as

that posed by the Islamic State, has had a transformational impact on national intelligence missions and structures, as well as changing the way intelligence cooperation between European countries (Gill et al., 2008; Leigh & Wegge, 2018). Reemerging great power competition, especially between the United States, China, and Russia, has presented new challenges and opportunities for intelligence cooperation, influencing national security policy (Juneau et al., 2023). The importance of intelligence collaboration is increasing, with greater emphasis on full cooperation in intelligence within the European Union (Bilgi, 2016).

However, while this abstract provides insight into changes and dynamics in security intelligence gathering, there has been no specific measurement or quantitative assessment of the extent of such changes between countries. First, in Australia, criminal intelligence gathering and analysis is carried out by the police with the aim of crime prevention. The implementation of intelligence-led policing is supported by the national criminal intelligence system, which involves various law enforcement or criminal intelligence agencies. Police intelligence in Australia focuses on the collection, analysis and sharing of intelligence data for national security purposes. Australian Security Intelligence the Organization (ASIO) is tasked with gathering intelligence to warn the government about threats to national security, such as terrorism, with powers set out in the ASIO Act 1979 (Deery, 2010). ASIO can interrogate and detain suspects with warrants coordinated with the Australian Federal Police and state and territory police forces. In addition, ASIO officers have special investigative powers which include telecommunication interceptions, searches of premises and the use of covert surveillance devices. Overseas, Australian intelligence activities are carried out by the Australian Secret Intelligence Service (ASIS).

In Singapore, the approach to intelligence gathering has seen considerable advancements through the unification of three core components: Intelligence, Investigation, and Operations, which form the foundation of law enforcement practices. The Police Intelligence Department's (PID) mandate is to deliver actionable intelligence that aids in the prevention, deterrence, and investigation of criminal activities. PID's responsibilities encompass the processing and analysis of intelligence, enhancement of criminal databases and information, along with the aggregation and distribution of national crime figures. Additionally, PID plays a crucial role in evaluating crime patterns, pinpointing organized crime networks, and keeping track of environmental shifts that could influence security.

Security intelligence in Indonesia aims to support law enforcement and preventive approaches to maintain security and order. Intelligence organizations in Indonesia consist of several institutions that have intelligence units according to their respective duties and functions, with the State Intelligence Agency (BIN-Badan Intelijen Negara) as the main coordinator. Security intelligence in Indonesia tends to focus on police and law enforcement functions.

In some countries, this government agency is also known as the secret service or information service. Although the use of spies and specialized informants dates to ancient times in areas as widespread as Chennai, the Near East, and the Roman Empire, intelligence activities have acquired a new operational scale as a social, professional, and permanent occupation of the modern state of Europe. Even so, intelligence agencies, as we know them today, only began to be institutionalized in the 20th century. After the end of the Cold War, in many countries the need and role of these intelligence services was debated, which may suggest that their growing institutional weight was just a passing phenomenon, a product of the two world wars and the Cold War itself. During the first half of the 1990s, intelligence services had reduced their budgets significantly while the new international context became more unstable and, as a result, demands for information became more demanding and diverse. The rapid growth of new information and communications technologies (ICT) allows private companies to offer information about security issues on a global scale.

From the intelligence collection process both in government and other sectors, we can describe and find new perspectives in gathering security intelligence in crime control and law enforcement. Technology has played a dominant role in intelligence gathering, but the role of human intelligence remains important. Technological support does not completely replace human intelligence, as human factors remain critical in every process and stage of the security intelligence cycle, as will be explained in this article.

In addition to human factors, they are referred to as non-human actors. Human actors and non-human actors are concepts put forward by Bruno Latour in the actor-network theory (ANT). This concept states that all entities, both human and non-human, play a role. The agency possessed by technology has also played a role in the process of reassembling various configurations of old social practices as well as their institutionalization as new social practices. In Latour, technology is a marker of the existence of agency outside of humans (Robert & R, 2023) The previous traditional view that viewed humans as separate from their technology, by Latour as something new because humans and their technology are equal as actants. Including humint and Techint in intelligence gathering.

This article identifies new perspectives in security intelligence gathering in crime control and law enforcement. Technology has played a dominant role in intelligence gathering, but the role of human intelligence remains important. Technological support does not completely replace human intelligence, as human factors remain critical in every process and stage of the security intelligence cycle. Previous research that collects security intelligence in the interests of the police shows the very strong influence of the use of intelligence technology by collecting all data and information that has a level of threat to crime prevention, state security, and more specifically to maintaining social order and ongoing development in the local country. This literature study provides an overview of intelligence collection activities as a common practice in the world by paying attention to (1) methods of intelligence collection including intelligence with humint, techint and osint, (2) Aspects of intelligence focus, strengths, challenges and trends in the use of intelligence for law enforcement. (3) Best practices from several countries are the study and focus on this article which begins with intelligence gathering.

LITERATURE REVIEW

The results of intelligence collection can be combined to create more complete intelligence, but this has advantages as well as challenges in its implementation, especially dealing with terrorist crimes. Attention to terrorism has strengthened due to attacks on the public, including security officers. This threat is real and causes casualties, so it is necessary to protect officers (Mulya et al., 2023).

It's widely acknowledged among scholars that the Federal Bureau of Investigation's (FBI) extensive use of domestic intelligence capabilities can potentially infringe on civil liberties. Following the events of 9/11, the FBI shifted its focus to not only investigating terrorist incidents but also proactively preventing them, necessitating widespread intelligence operations within the United States. This proactive approach, however, is often criticized for compromising essential freedoms and having a propensity to diminish civil liberties in the name of threat prevention. Adopting strategies rooted in administrative law could facilitate intelligence gathering while minimizing disruption to citizens' lives. Although traditional oversight mechanisms are in place, they lack the necessary judicial and political backing, and the FBI prioritizes preventing attacks, sometimes at the expense of rights protection (Berman, 2014). On another point, police intelligence recognizes the practical importance of intelligence work in crime prevention, security maintenance, and effective risk management to ensure public safety. The effectiveness and operational scope of police intelligence are heavily dependent on the credibility of its personnel and their efforts. However, this scope remains constrained, and the impact of police intelligence practitioners is limited unless there is

substantial organizational support and commitment to bolstering intelligence operations (Wirtz, 2016).

Work intelligence on the part collection on cycles intelligence is flexible compared to the previous model. During collection intelligence, agent intelligence can be with his own (humint) and techint, followed by activities confirmation in the field. Intelligence security becomes more dependent on technology (Wirtz, 2016). There is a trend towards equipment and technology at the moment and this is becoming a problem. Besides, there are risks that can happen if change starts to rule out intelligence alone in collection intelligence.

In the collection process intelligence on cycles intelligence experience changes in cycles basically only leads to processing at once accept return come back from stages previously namely direction. As seen in Figure 1, stages collection intelligence directly related to dissemination from intelligence. all stages in cycle intelligence by Davies et. al. (2013) can directly connect and give return feedback that is very thick with integration. Thus, Philips is more comprehensive. On the side there is basic intelligence previously as feedback and dialogue between every cycle process stages intelligence. The stages collection will be loading on work collection can into two large categories, namely by humint and techint which are details that go to section discussion.

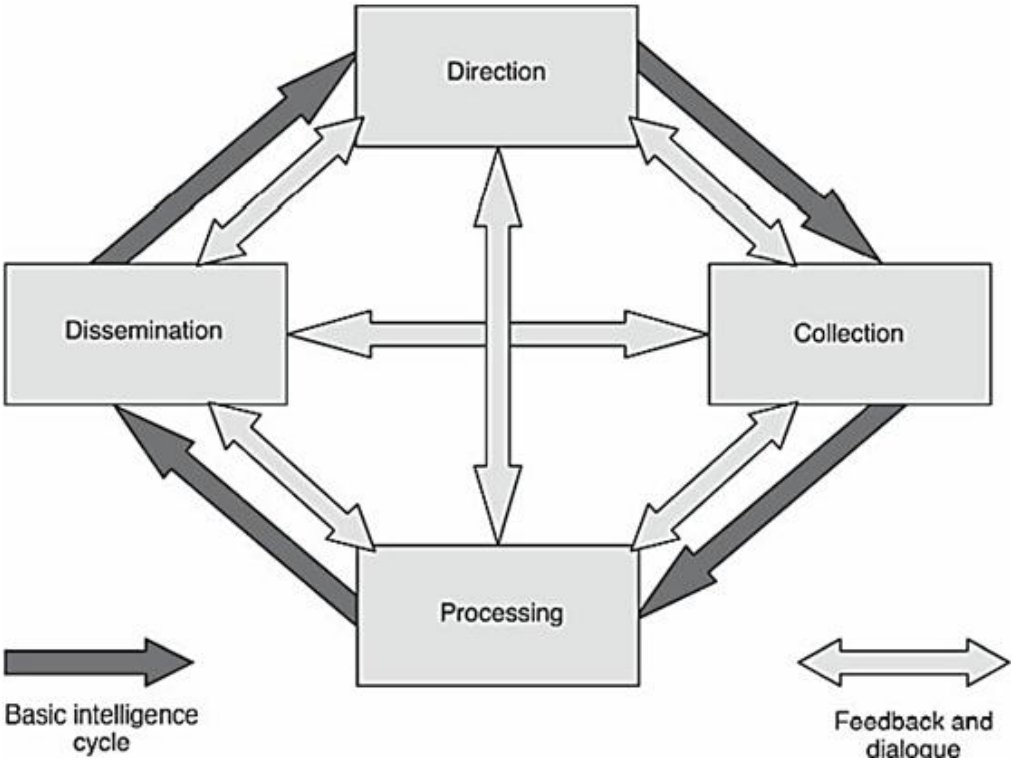

Figure 1. Intelligence Cycle (Davies, 2013)

In the realm of intelligence, there are inherent limitations that may arise. To mitigate the risk of intelligence asset failure, redundancy is employed using backup or alternative assets capable of fulfilling collection requirements. The deployment of diverse collection systems enhances this redundancy, with multiple units or sections often working on identical tasks or targets. While this may lead to some overlap and extra work, it also facilitates the gathering of varied types of intelligence, which can serve to verify the collected data. Collection operations rely on secure, swift, and dependable communication networks that support data sharing and enable coordination and alert-sharing among assets. After collecting, the correlated information is forwarded for further processing and compilation into reports for leadership.

Beyond NATO, the Five Eyes intelligence alliance, comprising the US, UK, Canada, Australia, and New Zealand, stands as the most enduring multilateral arrangement of its kind globally. From Five Eyes becomes The Fourteen Eyes. The alliance is a clandestine intelligence consortium tasked with monitoring and sharing internet user data and activity across multiple nations (Heimeriks et al., 2009). Comprising the United States, United Kingdom, Canada, New Zealand, Australia, Denmark, France, the Netherlands, Norway, Germany, Belgium, Italy, Sweden, and Spain, this alliance is often a stage for intense debates between proponents of Humint, who emphasize the value of human sources and traditional intelligence networks in gathering information, and advocates of Techint, who rely on mass surveillance technologies to acquire data on a large scale. These differing approaches frequently spark discussions regarding ethics, privacy, and the efficacy of each method within the modern intelligence landscape

Although not a formal security alliance in the traditional sense, Fourteen Eyes exhibits key characteristics of alliance operations, such as proactive burden sharing and internal negotiation. Many experts argue that the US exerts hierarchical control over the operational terms of the Fourteen Eyes network, leaving the lesser partners with little choice but to comply to continue receiving high-level intelligence from Washington. However, using Australia as an example, recent studies suggest that more dynamic interrelations are emerging, challenging the traditional views on asymmetric alliances and the roles of subordinate allies (O'Neil, 2017). Presently, intelligence cooperation within this alliance has expanded to include 14 countries. Nonetheless, figures like Snowden have criticized the alliance due to ethical and policy quandaries associated with the security of intelligence gathering by member nations. The structured framework for intelligence collection (encompassing methodology, context, and targets) is necessary to navigate the complex ethical and practical issues arising from various security intelligence collection activities. Additionally, it's crucial for politicians across the spectrum to dedicate ample time to thoroughly weighing the advantages against the drawbacks of any new security intelligence gathering initiatives.

Heads of intelligence agencies increasingly find themselves in the position (whether willingly or not) of having to justify and elucidate the public the necessity for new legislative or policy initiatives, while also preserving public trust. In late 2014, the chief of ASIO notably engaged with various media outlets to advocate for the advantages of new metadata retention laws in Australia from his viewpoint. Snowden has suggested that leaders of intelligence agencies should exhibit greater openness than has been customary when addressing the ethical and policy implications of security intelligence collection methods. Such transparency is crucial for conceptual and empirical scrutiny of security intelligence practices and alliance procedures (Walsh & Miller, 2016). Alliances play a pivotal role as corroborating intelligence through multiple sources diminishes the risk of incorrect judgments and susceptibility to deception. Until there is broader acknowledgment of policymakers' part in utilizing intelligence, flawed policies will persist, leading to what is perceived by the public as intelligence shortcomings or a general distrust in governmental intelligence.

METHOD

The method used is a qualitative approach with a literacy approach from various journal articles and unstructured interviews from selected sources. The approach is being taken by providing a general description and open interviews. Followed by coding by determining important keywords and constructive sentences by gathering intelligence in several countries. The nature of the interview gives freedom to the sources and the author himself as an instrument in this research.

Creswell & Poth (2018) stated that qualitative interviews occur when a researcher asks open-ended general questions to one or more participants. The interview results were coded and categorized using the keywords intelligence collection, human intelligence and techint.

Supporting references were obtained from reputable journals and on the website www.scholar.google.com.

Interviwee Code	Job Position	Job Experience (year)
T1	Intelligence Officer In Technology	7
T2	Field Intelligence Officer, Manager in Business Intelligence	33 (retired)
T3	Security Intelligence Analyst and Consultant (Returning to Private Sector)	35 (retired)
T4	Tactical Analysis Intelligence Officer	20
T5	Intelligence Officer in Intelligence Equipment	9

The framework begins by comparing intelligence gathering with law enforcement approach systems, the use of humint and techint as well as open source. As well as important aspects regarding the focus of intelligence activities, the strengths of each intelligence and tendencies in the use of intelligence. Apart from that, by exploring collaboration humint and techint in intelligence gathering in the intelligence cycle area which is practiced empirically in each country.

RESULT AND DISCUSSION

Human Intelligence (Humint) and Technological Intelligence (Techint)

Post-9/11, the field of intelligence has been shaped by evolving tactics and contemporary methods of information collection (Crosston & Valli, 2017). Aradau, as mentioned by Downing (2023), said that set against a backdrop of significant technological advancements such as social media, mobile communication, analytical processing, large-capacity solid-state data storage, and novel computing hardware and software. These developments have propelled the global intelligence community into an unfamiliar era characterized by multi-faceted intelligence dimensions. While both scientific and technological advancements and human expertise continue to be integral and intersecting components of intelligence, there is a noticeable divide with advocates fervently supporting one approach over the other. This article discusses how field operations and the processing and analysis of intelligence information can benefit from a synergy between Humint (human intelligence) and Techint (technical intelligence), advocating for an end to unnecessary rivalry and a shift towards the much-needed collaborative effort that is presently absent (Crosston & Valli, 2017).

Following the Cold War, Humint (human intelligence) experienced a decline, while policymakers have come to regard Techint (technical intelligence) as more dependable. Technical systems offer tangible proof of targets actions, and their lack of emotional bias renders them more credible. The reliance on technical systems also minimizes the risk to intelligence officers and soldiers by reducing the need for close-proximity intelligence gathering. However, Techint falls short in capturing and interpreting non-physical aspects such as emotions, judgments, or thought processes. The advent of new technology has brought about significant changes; these technologies are more accessible, and their significance more widely understood. They have altered the operational modes of various agencies, including those in intelligence. The sheer volume of information available today poses a daily challenge to process. Historically, data concerning specific security issues or strategic goals were centralized, then assessed and addressed using synthetic-analytic methods. The digital age demands that intelligence agencies swiftly collect, analyze, and process vast quantities of data, a feat made possible by new technologies. Nonetheless, this advancement prompts further questions regarding the necessity to adapt intelligence methodologies and the institutional capacities of states. A balanced integration of Humint with Techint is essential.

In the United States, the government agency that handles signals intelligence tasks is the NSA, an abbreviation for National Security Agency. The NSA is slightly different from the CIA, where the CIA focuses its duties and functions on Humint (Human Intelligence), while

the NSA focuses on Sigint as mentioned above. The two intelligence agencies do not overlap, instead they work together to cover each other's shortcomings. By the American Congress, the NSA received a much larger budget than the CIA because the NSA used more expensive equipment and technology supported by qualified personnel (National Crypto Agency - Indonesian Wikipedia, Free Encyclopedia, nd).

Within the context of Humint, Nunan et al., (2020) investigated the viewpoints and experiences of officers from a specialized counter-terrorism unit in England and Wales. The essence of collecting human intelligence lies in establishing and nurturing relationships, with effective communication, trust-building, commonality, reciprocity, and care as fundamental elements. Most participants agreed that relationships with informants could be developed through fostering connections. Such skills in human intelligence collection are honed through training and experience (Nunan, 2020). On another note, Sheptycki (2017b) highlighted that police intelligence divisions focus on four key intelligence activities: gathering intelligence; analyzing information to produce intelligence; tasking and coordination based on intelligence 'products'; or deployment in the field based on intelligence. The democratic oversight of police intelligence is crucial as they act as nodes within a broader security governance network (Sheptycki, 2017a). Furthermore, Jensen (2012) discussed how law enforcement can economize on crime management by recognizing the value of crime intelligence as part of future policing strategies. The Integrated Crime Intelligence Analysis Framework (The Diamond Matrix) aims to 'reduce the crime triangle' and lays the groundwork for programs targeting intelligence specialists/advanced specialists, decision-makers, and leaders an approach that leverages crime intelligence to meet professional policing needs (Jensen, 2012). Therefore, it is highly pertinent to direct research towards understanding intelligence gathering through both Humint and Techint.

There are at least three important changes to intelligence collection, (1) threats to technological progress, (2) collaboration of intelligence collection, (3) best practices in intelligence collection. The hybrid intelligence model combines the strengths of human intelligence (Humint) and technological intelligence (Techint) to overcome the limitations of both approaches. Humint's nuanced understanding of social and cultural contexts complements the precision, scalability, and speed of Techint. By leveraging their intersection, intelligence processes can enhance decision-making accuracy while minimizing risks associated with over-reliance on one method. This model operates on three levels:

1. Operational Level: Teams comprising human agents and advanced tools like AI-driven analytics collaborate in real-time intelligence missions, particularly in scenarios involving diverse and unpredictable socio-political factors. For example, Humint could validate or contextualize Techint findings such as signal interceptions.
2. Strategic Level: Data from Techint systems can highlight macro trends, guiding intelligence agencies where Humint operatives should focus their efforts.
3. Decision-Support Level: Intelligence output developed through the hybrid approach can support leadership decisions by offering balanced insight-objective data enriched with human judgment and situational awareness.

The hybrid model requires synchronized governance, training programs, and ethical oversight of advanced technologies. Key enablers include AI for data synthesis, IoT-based real-time monitoring, and algorithms designed to prioritize verified human inputs in sensitive situations.

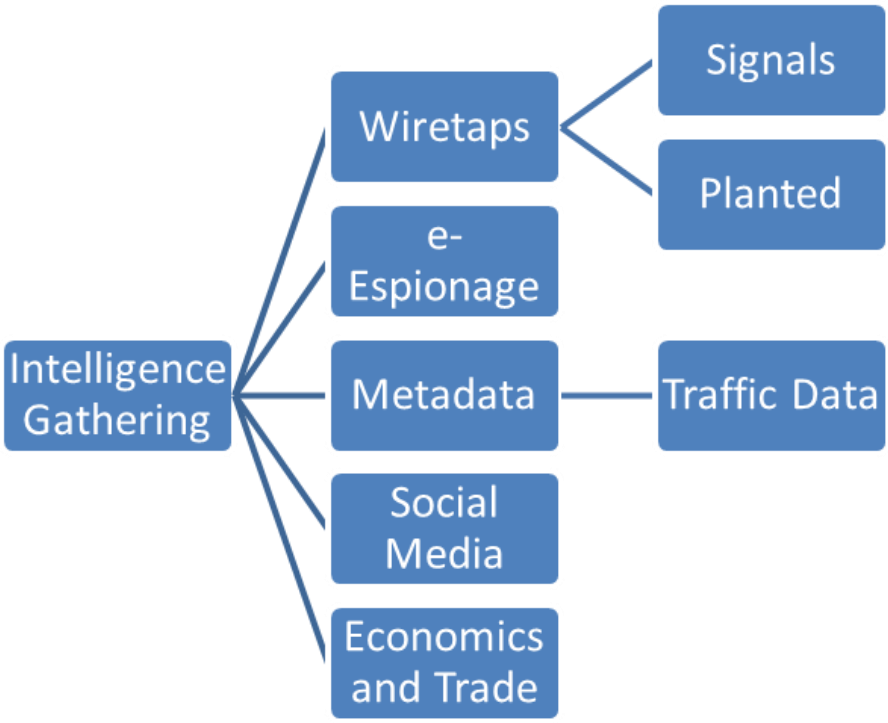

Figure 2. Techint's Intelligence Gathering Sources

First, advances in intelligence technology are in line with the threats that occur. In fact, Paul Virilio's perspective shows that new technology will be balanced with the risks and accidents that occur. The more advanced an intelligent technology is, the more it means creating accidents or failures in that technology. Even though it looks theoretical, it can be described that increasingly sophisticated intelligence technology also creates risk effects or even accidents that cause failure of the technology itself. Paul Virilio 's view can be illustrated simply by the invention of airplanes, which will be comparable or there will also be plane crashes as an effect of this technological discovery. In this way, new intelligence also creates risks or threats that can occur, just like the airplane illustration above. The following table describes the risk of accidents that occur from the development of security intelligence technology as follows:

Second, the most effective way of gathering intelligence using the internet network is Open-Source Intelligence (Osint), Cyber Intelligence (Cybint), and Human Intelligence (Humint). The collection of intelligence from publicly accessible sources and social activities of individuals and media organizations are an important source. Cybint is a method of intentionally gathering intelligence from various online sources, including social media. Cybint as a derivative and detail of Osint. Meanwhile, obtaining intelligent information from people or individuals through direct interaction and behavioral analysis is known as Humint (Sood & Enbody, 2014). The collection model shows two major parts and clustering between humans and non-humans in the act of collection. The position of the agent and structure merge with every element in the actant. All elements are only within the intelligence gathering group. In this way, collaboration with various techniques and approaches will produce comprehensive and strong intelligence in intelligence collection.

Third, on the use of techint in intelligence gathering in alliances with a technological approach that carries out intelligence collection by wiretapping through capturing signals or attaching them to the target device (Walsh & Miller, 2016).

The new term refers to e-espionage to describe intelligence gathering activities through intelligent electronic devices by working like field agents, but with an electronic and digital approach (see figure 2). Sensitive data can also be collected through metadata that can be

captured as well as data sent, and data received. The use of social media is also an important source of information because it is included in the Osint category. Its function is to obtain information and carry out in depth and confirmation. Various tools include trade economic reports that can be measured by market levels and threats to the market if there is a market downturn and supply disruptions chain can cause potential disruption.

Intelligence collection from human intelligence and techint as well as open-source intelligence as part of the development of information and communication technology. There is an assessment and there are important indicators both in terms of humint and techint. The process of gathering intelligence for law enforcement and at the same time maintaining social order, especially in the broad scope of state security. The table below describes these situations and conditions and summarizes all aspects. However, it emphasizes that there are two important things that play a role in intelligence gathering, namely human actors and non-human actors, both of which can be implemented in detail. Whatever is external to humans we call non-human actors, such as signals such as communications, intelligence equipment, laptop support tools or even radio signal receivers, forms of description or tools for intelligence analysis fall into the category of non-human actors. in the intelligence gathering process.

Meanwhile, the development of Osint is so strong that it is believed that the use of social media can form a large database as a function that is easy to access and must also be verified from the data collected. For those implementing intelligence collection who use Osint, the data must be verified and tested to determine whether what is obtained from open-source intelligence is valid and used as an intelligence report. The category of open source and its analysis by machines is a category of non-human actors. However, naturalistic analysis can also be carried out by humans using manual methods, but this cannot be done because the database is so large that adequate equipment is needed to analyze large, complex databases.

Table 1. Intelligence Gathering Humint and Techint

Collection Method	Procedure	Use in Law Enforcement
Human Intelligence (Humint)	- Intelligence agents are stationed in the country. - Recruitment informants and confidential sources. - Operation intelligence confidential. - Interrogation of detainees and suspects. - Use informants and agents confidential.	- Use informants and agents confidential for combat crime organized and terrorism. - Use interrogation to get information from suspects. - Use technology for tracking the movement of people and online activity.
Technical Intelligence (Techint)	- Interception of electronic communications. - Reconnaissance electronics. - Intelligence data collection signal (Sigint). - Use technology for tracking the movement of people. - Intelligence data analysis signal (Sigint). - Social media analysis. - Use technology for track movement of people and online activity. - Analysis document public.	- Use of Sigint for combat crime organized and terrorism. - Use social media analysis to identify threat potential. - Use technology for track movement of people and online activity. - Use of Osint to identify threat potential. - Use of Osint for investigating crime.

Source: Processed Author, June 2024

Based on the one-row table on humint shows that LO task placement is very important in intelligence gathering. He works not only with himself, but also with technological tools and intelligence devices.

As Human Actors, intelligence liaison increases exponentially during so-called terror threats including from abroad that enter the country. Nevertheless, intelligence liaisons assigned overseas remain largely understudied and substantially undertheorized awareness of intelligence gathering by humint and techint. LO is in the humint category. LO placement

abroad can be of relevance to international relations. The task of gathering intelligence is also assigned to the LO with input from international relations theory which is certainly not the same as the conceptual and theoretical approach to intelligence (Andrew, 2004). LO's contribution will be strong with training and utilization of intelligence equipment. LO serves openly and privately according to the interests of his duties.

The phenomenon of intelligence relations can only be theorized so far. Different approaches, even when adopted together, also have discernible limits. The greater complexity also emerges most clearly when examples of intelligence phenomena are to be analyzed at the level of the individual or more broadly across institutions or countries. The level of intelligence includes intelligence gathering at the micro, meso, and macro levels. Although abroad, the aim of gathering security intelligence is an integral and integral part of the important main tasks in the country which lead to protection, protection and police services. Apart from this explanation, it aims to maintain security and order or what is usually referred to as social order. Apart from that, the focus of security intelligence is on carrying out police duties by providing early warning, early detection and early action as an initial preventive effort or action. Intelligence is more about three things. The first is prevention efforts with a preemptive nature. Second, by participating in security activities and the final part is by returning it to its original safe condition. All these actions begin with intelligence collection planning as in the intelligence cycle. During the intelligence gathering process it cannot be detached from the techint. Technology has almost replaced human jobs. However, there is much that cannot be understood which says that all centers of action are in humans. At this time, it turns into part of a complex network. British intelligence said that gathering intelligence to build detailed knowledge about threats to the country was at the core of MI5's work. Assessment and investigation process (Gathering Intelligence MI5 - The Security Service, n.d.). Meanwhile, Ronald (2021) maps out domestic and foreign affairs. domestic policy and foreign policy meet, and the point where it connects with other states and territories. The focus of the discussion highlights the difficulty of distinguishing clearly between internal and external security, as well as national and human security (Crelinsten, 2021).

There are at least three levels of discussion collection intelligence: micro, meso and macro. It must have a parameter, namely focus intelligence, then from side strength his intelligence, his superiority strength, how? challenges that lie ahead, as well intelligence own tendencies towards its use for state interests. By details discussed and summarized in detailed table give description collection intelligence including activities that are not free from action collection intelligence by humint and techint on every level.

Table 2. Intelligence Collection at the Micro, Messo, and Macro Levels

Level	Focus	Strength	Future Challenges	Use Case
Micro	- Individual. - Small Group. - Local activity.	- Local information access. - Network information. - Knowledge of the local environment.	- Lack of power source. - Range limitations. - Infiltration difficulty.	- Crime prevention. - Law enforcement. - Local security protection.
Meso	- Organization. - Community. - Regional scope. - Industrial sector.	- Access regional information - Regional network intelligence - Data analysis ability.	- Problem complexity. - Fragmentation of information. - Political intervention.	- Maintain regional stability. - Economic security. - Critical infrastructure protection.
Macro	- Country. - Alliance. - Ideology. - Global trends.	- Global information access. - International intelligence network. - Geopolitics analysis ability.	- Complex global threats. - Political uncertainty. - Competition between countries.	- National Security - Foreign Policy - National Interest Protection.

Source: Synthesized By Author, June 2024

Use of Humint and Techint in Intelligence Gathering

Although intelligence technology continues to advance, respondents emphasized that technology cannot fully replace the role of humans in intelligence operations. As one respondent stated, "So technology cannot manage itself without human decision... the most sophisticated technology is still needed. That is the balance between humans and technology" (T1). This highlights that while technology serves as an essential tool, strategic decision-making remains a human responsibility. In the context of HUMINT, a human-centered approach is indispensable, as intelligence targets are individuals themselves. As another respondent noted, "Humans cannot be replaced by technology... the approach taken can only be done by humans, related to the assessment of behavior, feelings, desires, motives, etc." (T3). This aligns with Stottlemyre (2015), who asserts that crowdsourced intelligence relies on human contributions, making HUMINT and OSINT the most relevant disciplines for such an approach.

Nevertheless, technology plays a crucial role in enhancing the efficiency of intelligence collection and analysis. One respondent stressed that while One Man Operation (OMO) requires human expertise, intelligence equipment is still essential as marginal task support: "Humans cannot be replaced, there must still be intelligence gathering... but intelligence equipment is needed as marginal task support" (T2). A major challenge in HUMINT today lies not only in data collection but also in filtering and analyzing vast amounts of information. As another respondent explained, "The nature of technology in our opinion only helps in analyzing a lot of data. Mapping and describing in general" (T3). Thus, HUMINT practices require a synergy between human analytical skills and technological support to process the increasing volume of intelligence data in the digital era. While OSINT is categorized under the broader field of Techint, which encompasses intelligence technologies and equipment, the high costs associated with intelligence technology must also be considered. Aldrich (2015) discusses the substantial operational expenses of global intelligence collection, raising the question of whether the benefits justify the costs.

Furthermore, in SIGINT, technology still has limitations. As one respondent pointed out, "No matter how sophisticated the equipment is, I think there are things that cannot replace humans. For example, wiretapping is currently still limited to GSM, for data communication it cannot yet" (T5). This indicates that despite technological advancements, intelligence operations still necessitate manual methods, such as direct surveillance of targets. Even when using advanced intelligence equipment, human intervention is required for configuration and task customization, as another respondent stated: "Including equipment that seems to not require humans, it turns out that it requires settings by forming its needs or tasks" (T4). Law enforcement agencies rely on legal interception to monitor suspects' communications, in accordance with legal frameworks, to facilitate prosecution (Mulya et al., 2022).While practices such as wiretapping and the application of intelligence technology are crucial for national security, they must be balanced with democratic concerns regarding privacy and civil liberties (Berman, 2014).

In conclusion, while technology plays an essential role in various intelligence disciplines, it cannot fully replace human involvement. The balance between technological advancements and human decision-making is crucial in ensuring the effectiveness of HUMINT, OSINT, and even SIGINT in supporting national security efforts. Moreover, as the volume of intelligence data continues to grow, technological support is indispensable in structuring and categorizing information, allowing human analysts to make informed and strategic assessments. However, as Aldrich (2015) argues, intelligence operations must continuously assess whether the significant investment in technology-driven intelligence is justified by its effectiveness in achieving national security objectives.

Here, a suite of established intelligence disciplines is acknowledged, including human intelligence (Humint), open-source intelligence (Osint), signals intelligence (Sigint), measurement and signature intelligence (Masint), and geospatial intelligence (Geoint). Among these, Humint and Osint are predominantly derived from the analysis of data gathered by individuals and are therefore well-suited to crowdsourcing platforms, which rely solely on human contributions.

While certain crowdsourced data might resemble geospatial intelligence (Geoint), such as aggregating location metadata from various online activities, all crowdsourced information is deemed to be gathered, created, and/or disseminated by individuals in an open setting, thus aligning more closely with open-source intelligence (Osint). Signals intelligence (Sigint), which involves collecting intelligence via signal interception, is not essential for crowdsourced intelligence due to the inherently public aspect of crowdsourcing. Law enforcement agencies employ legal interception to monitor the communications of suspects in accordance with the law and to facilitate their prosecution. This procedure necessitates the use of intelligence technology and cooperation with telecommunications service providers (Mulya et al., 2022).

Masint involves the collection and analysis of data from technical devices like radar and is inherently not crowdsourced due to its lack of human involvement. Crowdsourced intelligence, which relies on information from a collective of individuals, is therefore limited to Humint and Osint (Stottlemyre, 2015). Conversely, Osint falls under the broader category of Techint, which encompasses the use of intelligence technologies and equipment. However, employing such technology comes at a significant cost. Aldrich, R.J. (2015) discusses the substantial operational expenses involved in global intelligence collection. While some advanced intelligence technologies are developed with regime interests in mind, others are created for the enhancement of analytical management. The debate continues whether the hefty price tag of robust intelligence justifies its benefits. The effectiveness of intelligence-led national security policy in achieving its goals may not always justify the expenditure (Aldrich, 2015). Threat assessments and policy considerations in intelligence must be backed by strong and credible reasons. Yet, domestic opposition to Humint and Techint collection methods has arisen due to democratic concerns. Nonetheless, practices such as wiretapping, and the application of intelligence technology play a crucial role in national safety. Government regulations aim to establish sound, evidence-based structural and procedural frameworks that include insights from outside the intelligence sector while also considering civil liberties (Berman, 2014).

Apart from regulations, Humint also faces problems in managing and analyzing the data it collects. In the digital era, the amount of data continues to increase is very large, and humint needs to be able to process and sort relevant information in limited time. Good analytical skills are important to be able to identify the truth of existing information as well as relate and understand this information in a wider context. If the amount of data is large or very large, machines are needed to provide categories that make it easier to read this large amount of data.

New Intelligence Perspective on Intelligence Gathering

Perspective new collection intelligence shows exists internal interests' collection intelligence with angles new view about exists humans and actor's humans inside collection intelligence. The emergence of technological advances, including artificial intelligence and big data analytics, has changed intelligence gathering practices. The philosophy of intelligence (Sims, 2006) grapples with the implications of relying on technology, weighing the benefits of increased efficiency and capability against concerns of privacy, bias, and the potential erosion of human judgment and intuition. Humint has advantages and limitations. Techint is the same. This means that in the context of intelligence gathering, both aspects must be considered in a balanced manner. The humint approach as human and non-human actors in intelligence

equipment will allow for a new understanding that intelligence collection is not only carried out by humans but also by objects in the form of intelligence equipment.

Adopting a socio-technical perspective (Pasmore, 1995) allows for insights into technology adoption that would be unattainable without considering both technological and socio-technical entities. This is particularly pertinent in the context of IoT-based intelligence tools, where technical entities can autonomously collect data and interact with one another, independently of human intervention, and even initiate actions on their own. Such advancements have the potential to forge new types of interactions and alter the dynamics of existing ones, not by influencing humans as socio-technical agents, but through their inherent capabilities (Tatnall & Davey, 2019) Consequently, this technology is poised to diminish the human role in intelligence collection. While technological capabilities must be bound by human-defined parameters, the benefits derived from these technologies are not solely predicated on their constraints. It's important to recognize that technology is ultimately a human creation.

Table 3: Human Actors and Non-Human Actors in Intelligence Gathering

Human Actor	Non-Human Actors
Intelligence agent	Intelligence Equipment
Informants and society	Analysis tools
Analyst group	Signals and communication networks
User or Leader	Databases intelligence
Stakes holders	Data records
Intelligence community	Techint Devices

Source: processed by author, June 2024

Human actors in intelligence collection and management include intelligence agents, informants from the public, as well as those working on intelligence, namely intelligence analysts, including leaders of intelligence organizations and related stakeholders who may be partners in an intelligence alliance. Lastly, groups from the intelligence community who are recognized and trusted in intelligence work. In the previous initial discussion, collection also involves intelligence equipment and various equipment used, including intelligence analysis applications, then the use of signals and communication networks, intelligence databases including records, communication data, and the existence of intelligence devices that support intelligence collection. Table 3 above illustrates that in collection activities there are not only humans, but it appears that human actors also play a role or take part in the intelligence collection itself. The role of non-human actors was mentioned by Alan Turing as the beginning of the belief that equipment works the way humans think (Turing, 2023). Intelligence collection from communication signals cannot be reached by five senses and must use special equipment. Machines think exactly like humans think as smart computer machines do. Thus, we must pay attention to the fact that intelligence tools have a value and importance that should be the same as what humans do. The term as a tool will increase or have a value that continues to approach equality of collecting activities carried out by humans. Another consideration is that work that does not use intelligence equipment as a non-human actor will have weaknesses in capacity and is also the least troublesome because it requires quite a lot of human power. The risk of intelligence work accidents such as leaks of confidential data, the very possible negative effects of using intelligence equipment due to radiation to the operator's body must be considered and considered in the use of intelligence equipment. The operators in question are intelligence officers who enter as human actors.

Apart from human actors there are non-human actors. Explanation of non-human actors in intelligence networks in the form of sensing or surveillance equipment to search for information, binocular equipment, server devices and workstations that function to process incoming information. A large database that makes it possible to collect relevant information

according to the purpose of searching for the information. This equipment works using electricity and requires human settings. However, the way humans work is not like computers. Repetitive work or processing large amounts of data in databases is carried out by machines, including categorization or analysis. Basically, humans cannot manage large amounts of data using their five senses, but they can make settings and settings on the device.

Techint's work is also on internet data flows. It is possible that internet traffic is digital data that can be read directly by a computer or by a database, but this traffic can show the activity of internet users including which nodes are passed through. All these activities require electricity. Electrical management is done by humans. Not everything can be done by machines, it requires settings and requires many things to be able to run the system. Thus, what is in techint cannot be separated from the collection work between humans and machines.

Humans have become an important part of intelligence collection. Technology has changed the nature of long-standing relationships in this process. Today, there are technologies that function as objects capable of "thinking," much like humans. These technologies can even limit or "regulate" human actions. Intelligent devices, things embedded with artificial intelligence, have formed networks of actors involved in gathering information. This represents a new model in intelligence collection: one that combines human and non-human agents. The shift began with a separation between human and technological actors, but over time, this distinction has blurred. Now, there is a hybrid model of intelligence gathering that integrates HUMINT (human intelligence) with TECHINT (technical intelligence).

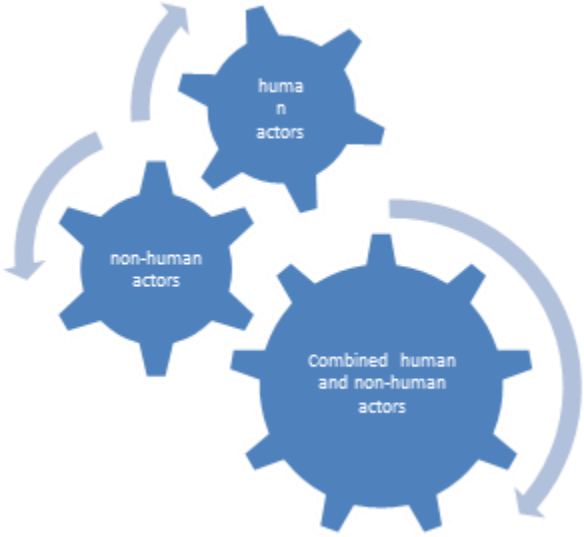

Figure 3. Synergy of Human and Non-Human Actors

Combination in collection intelligence between actor humans and non-human possible exists flexibility and more comprehensive because work actor human and non- human actors that will show exists strong understanding for collecting agents' intelligence bring up exists awareness inner see that equipment intelligence is a non-human actor whose position important even on-stage future and development furthermore own the value of "equality" with actors' man. Equipment intelligence enters in category things as non-human actors (see figure 3). Equipment the no can have feelings and attitudes like man, but they have a machine that is results design and creation man for make it easier work computing and methods think similar humans. machines on equipment intelligence given lesson or given parameter settings by humans. The writer believes that combination between actor humans and actors human inside collection intelligence for a combination of strength and will give awareness new about what is the collection process integrity done until produce to report accurate intelligence sharp for takers decisions and state leadership.

CONCLUSION

Intelligence collection activities as a common practice in the world pay attention to the method of intelligence collection including intelligence with humint, techint and osint. Apart from that, aspects of intelligence focus, strengths, challenges and trends in the use of intelligence for law enforcement. Best practices from several countries have focused on intelligence gathering activities. Intelligence gathering can use intelligence tools, but it does not completely replace the role of humans in sensing and decision making. Future debates will show that a form of autonomy is also created by humans themselves with all the procedures that must be included in the intelligence equipment. On the other hand, it must be acknowledged that the use of intelligence equipment is very powerful and makes human work easier, and in the future, there is even a possibility that the intelligence work area will be dominated by techint. In humint in certain areas that show the decision and involvement of feelings or soul and the conception of thought of a humint. The orientation of the center of gravity of intelligence technology coupled with human intelligence between strong intelligence technology with operators who use it, and the support of qualified analysts, human intelligence and intelligence technology cannot work alone. We call this combination of humint and techint a hybrid of intelligence collection by considering aspects of intelligence agents such as human actors and techint as non-human actors.

Human intelligence (Humint) and technical intelligence (Techint) are both expanding fields. Typically, the creation of intelligence products entails the amalgamation of data from diverse sources (Sunethpriya, nd). The integrated approach of Humint and Techint in intelligence gathering offers a fresh perspective, highlighting the significance of both human and non-human agents in the process. The limitations associated with this kind of raw intelligence - often preliminary and requiring corroboration from additional sources - stem from its incomplete nature and potential inaccuracies or ambiguities that necessitate further investigation and analysis. Within the intelligence cycle, there exists a vast and unsorted array of information that can be refined during the processing stage (Stottlemyre, 2015). The synergy between Humint's role in natural analysis and Techint's role in validation, which leverages large datasets and enhanced computational speed, can result in precise and effective collaboration. The final intelligence product comprises information that has been compared, scrutinized, and evaluated to facilitate the formulation of conclusions in a report for leadership.

Technology and intelligence tools have played a dominant role in intelligence gathering, but the role of human intelligence remains important. Technological support does not completely replace human intelligence, because human factors remain critical in every process in the security intelligence cycle stage. The author ventures with an important key sentence that "Humans will continue to exist in any technological era." Intelligence agents everywhere will continue to update their knowledge and skills and create intelligence equipment technology for prosperity and social order and to prevent threats to their country's security.

Further research focuses on intelligence gathering by Humint and Techint with the perspective of human actors and non-human actors in the use of intelligence in practice and the future capacity of Humint which is influenced by ways of acting Humint by intelligence equipment and Techint in the context of implementation and intelligence work. On the other hand, it is impossible to counter the development of technology and intelligence equipment with human capabilities and capacities but rather an approach that is beneficial to the interests of humanity by prioritizing human strengths and responding to developments in intelligence technology.

REFERENCES

Aldrich, R. J. (2015). The 100 billion dollar brain: Central intelligence machinery in the UK and the US. *International Affairs*, *91*(2), 393–403. https://doi.org/10.1111/1468-2346.12242

Andrew, C. (2004). Intelligence, International Relations and "Under-theorisation." *Intelligence and National Security*, *19*(2), 170–184. https://doi.org/10.1080/0268452042000302949

Berman, E. (2014). Regulating Domestic Intelligence Collection. *Washington and Lee Law Review*, *71*(1), 3–91. http://scholarlycommons.law.wlu.edu/wlulr/vol71/iss1/5/

Bilgi, Ş. (2016). Intelligence cooperation in the european union: An impossible dream? In *All Azimuth* (Vol. 5, Issue 1). https://doi.org/10.20991/allazimuth.167342

Brodeur, J.-P. (2007). High and Low Policing in Post-9/11 Times. *Policing*, *1*(1), 25–37. https://doi.org/10.1093/police/pam002

Crelinsten, R. (2021). *Terrorism, Democracy, and Human Security; A Communication Model; First Edition*. Routledge Taylor and Fr.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry Research Design: Choosing Among Five Approaches* (4th ed., Vol. 13, Issue 1). SAGE Publications.

Crosston, M., & Valli, F. (2017). An Intelligence Civil War: "HUMINT'" vs. "TECHINT", Cyber, Intelligence, and Security, Vol. 1, Issue 1, Spring 2017. *Intelligence, and Security* |, *1*(1), 67–82. http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/An Intelligence Civil War "HUMINT'" vs. "TECHINT".pdf

Davies, P. (2013). *MI6 and the Machinery of Spying: Structure and Process in Britain's Secret Intelligence*. http://books.google.co.uk/books?id=TTW2h5GHlWkC

Deery, P. (2010). Australian Security Intelligence Organisation. In *Spies, Wiretaps, and Secret Operations: an Encyclopedia of American Espionage: volumes 1-2* (Vols. 1–2, pp. 59–60).

Downing, J. (2023). Social Media, Digital Methods and Critical Security Studies. *New Security Challenges*, 71–108. https://doi.org/10.1007/978-3-031-20734-1_3

Gill, P., Marrin, S., & Phythian, M. (2008). Intelligence theory: Key questions and debates. In *Intelligence Theory: Key Questions and Debates* (Vol. 9780203892). https://doi.org/10.4324/9780203892992

Heimeriks, K. H., Klijn, E., & Reuer, J. J. (2009). Building Capabilities for Alliance Portfolios. *Long Range Planning*, *42*(1), 96–114. https://doi.org/10.1016/j.lrp.2008.10.005

Jensen, M. A. (2012). Intelligence failures: What are they really and what do we do about them? *Intelligence and National Security*, *27*(2), 261–282. https://doi.org/10.1080/02684527.2012.661646

Juneau, T., Massie, J., & Munier, M. (2023). Intelligence Cooperation under Multipolarity: Non-American Perspectives. In J. Massie & M. Munier (Eds.), *Intelligence Cooperation under Multipolarity: Non-American Perspectives*. University of Toronto Press.

Leigh, I., & Wegge, N. (2018). Intelligence and oversight at the outset of the twenty-first century. In *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World* (1st ed., pp. 7–24). Routledge. https://doi.org/10.4324/9781351188791-2

Mulya, A., Ismail, M., & Jumaeng, S. (2023). Perspective Of Security Intelligence in Law Enforcing Terrorism in Indonesia. *International Journal of Social Service and Research*, *3*(12), 3125–3136. https://doi.org/10.46799/ijssr.v3i12.620

Mulya, A., Marzuki Ismail, R. Bayu Yuliantoro, & Heriyanto Kandati. (2022). Dampak Implementasi Lawfull Interception pada Pemberantasan Tindak Pidana Terorisme. *Formosa Journal of Multidisciplinary Research*, *1*(2), 367–382. https://doi.org/10.55927/fjmr.v1i2.551

Nunan, J. (2020). *Developing an Evidenced-Based Approach to Enhance the Collection of Intelligence from Covert Human Intelligence Sources Declaration*. *December*.

O'Neil, A. (2017). Australia and the 'Five Eyes' intelligence network: the perils of an asymmetric alliance. *Australian Journal of International Affairs*, *71*(5), 529–543. https://doi.org/10.1080/10357718.2017.1342763

Pasmore, W. A. (1995). Social Science Transformed: The Socio-Technical Perspective. *Human Relations*, *48*(1), 1–21. https://doi.org/10.1177/001872679504800101

Robert, R., & R, U. A. R. (2023). Konstruktivisme Bruno Latour dan Implikasinya Terhadap Ide Keagenan Sosiologi. *Masyarakat: Jurnal Sosiologi*, *28*(2). https://doi.org/10.7454/MJS.v28i2.13565

Sheptycki, J. (2017a). Liquid modernity and the police métier; thinking about information flows in police organisation. *Global Crime*, *18*(3), 286–302. https://doi.org/10.1080/17440572.2017.1313734

Sheptycki, J. (2017b). The police intelligence division-of-labour. *Policing and Society*, *27*(6), 620–635. https://doi.org/10.1080/10439463.2017.1342645

Sims, J. E. (2006). Foreign Intelligence Liaison: Devils, Deals, and Details. *International Journal of Intelligence and CounterIntelligence*, *19*(2), 195–217. https://doi.org/10.1080/08850600500483657

Sood, A., & Enbody, R. (2014). Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware. *Targeted Cyber Attacks: Multi-Staged Attacks Driven by Exploits and Malware*, 1–142. https://doi.org/10.1016/C2013-0-14275-4

Stottlemyre, S. A. (2015). HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence. *International Journal of Intelligence and CounterIntelligence*, *28*(3), 578–589. https://doi.org/10.1080/08850607.2015.992760

Tatnall, A., & Davey, B. (2019). Rise of the Non-Human Actors: the Internet of Things. In *Analytical Frameworks, Applications, and Impacts of ICT and Actor-Network Theory*.

Telep, C. W., Ready, J., & Bottema, A. J. (2018). Working towards intelligence-led policing: The Phoenix Police Department intelligence officer program. *Policing (Oxford)*, *12*(3), 332–343. https://doi.org/10.1093/police/pax094

Turing, A. M. (2023). Computing Machinery and Intelligence. *Brain Physiology & Psychology*, *LIX*(236), 212–240.

Walsh, P. F., & Miller, S. (2016). Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden. *Intelligence and National Security*, *31*(3), 345–368. https://doi.org/10.1080/02684527.2014.998436

Wirtz, J. J. (2016). Understanding intelligence failure: Warning, response and deterrence. In *Understanding Intelligence Failure: Warning, Response and Deterrence*. https://doi.org/10.4324/9781315673295