SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 03 No. 02 (2026), pp. 151-158
Research Article
doi: https://doi.org/10.70710/sitj.v3i2.100

Cyber Open Source Intelligence in Counter-Terrorism: A Systematic Literature Review and Indonesian Case Study Analysis

Rizal Amrullah[1,a], Vedaniar Zahra Danardini Mulia[1,b,*]

[1]Politeknik Siber dan Sandi Negara, Bogor, Indonesia
[a]rizal.amrullah@student.poltekssn.ac.id; [b]vedaniar.zahra@student.poltekssn.ac.id
*Corresponding author

Article Info
Received: 29-May-2026
Revised: 15-June-2026
Accepted: 30-June-2026

Keywords
BNPT; Counter-Terrorism; Cyber Intelligence; Indonesia; Open Source Intelligence; Surabaya Bombing

Abstract
The burden on Indonesia's counterterrorism (CT) services has increased due to terrorist groups' exploitation of the internet. Between 2023 and 2025, the National Counter-Terrorism Agency (BNPT) recorded 137 actors who were actively abusing the internet for terrorism; in 2025 alone, 21,199 radical content pieces were reported on key platforms. In this setting, open source intelligence (OSINT), or intelligence drawn from publicly accessible material, has become a crucial strategic weapon; nevertheless, Indonesian scholarship is still dispersed and policy-disconnected. In accordance with PRISMA 2020 principles, a systematic literature review (SLR) of 47 peer-reviewed papers (2014–2025) is presented in this work together with a case study analysis of the 2018 Surabaya bombings and the 2024 disintegration of Jemaah Islamiyah (JI). The research reveals six theme clusters: the growth of OSINT, cyber tools and AI integration, terrorist cyberspace exploitation, OSINT applications in CT, ethical-legal frameworks, and the Indonesian institutional environment. As a result of inter-agency fragmentation across Densus 88, BNPT, BSSN, and BIN, the case studies show that pre-attack OSINT signals in 2018 were observable but not put together into actionable intelligence. The study makes the case that Indonesia needs a federated OSINT doctrine that is in line with Law No. 5/2018 and the Personal Data Protection Law (UU PDP 27/2022). It also suggests a five-part policy framework based on securitization theory, intelligence cycle theory, and second-generation OSINT.

1. Introduction

On May 13 and 14, 2018, three families associated with Jamaah Ansharut Daulah (JAD) detonated explosives at three churches and a police headquarters in Surabaya, resulting in 28 fatalities and 57 injuries (Schulze, 2018). According to forensic reconstruction, the Oepriarto family's Facebook activity had abruptly stopped in 2014 in a pattern consistent with radicalization; the families had spread propaganda from Inspire and Rumiyah magazines; and pro-IS Telegram channels had recently incited followers to violence (Schulze, 2018; IPAC, 2018). The signals may be seen. Prior to the attack, none were transformed into useful intelligence.

The incident brought to light an issue that Indonesian CT policy has yet to completely address: how can the government preserve democratic accountability while turning publicly accessible digital traces into preventative intelligence? The urgency has grown since then. Indonesia has 221.5 million internet users (79.5% penetration), according to APJII (2024). Kemp (2024) estimates that 185.3 million people use social media on a daily average of three hours and eleven minutes. Online radicalization, which used to take three

to six years, now takes three to six months, according to BNPT CEO Eddy Hartono's January 2026 observation (VOI, 2026). 21,199 radical content pieces were recorded by BNPT in 2025: 14,314 on Meta, 1,367 on TikTok, and 1,220 on X (ANTARA, 2025).

The U.S. Office of the Director of National Intelligence defines open source intelligence (OSINT) as intelligence that is obtained "exclusively from publicly or commercially available information that addresses specific intelligence priorities" (ODNI & CIA, 2024). OSINT has become a strategically important response. Although the exact empirical foundation for this number is disputed, Ghioni and colleagues (2023) estimate that OSINT accounts for 80–90% of intelligence operations carried out by Western law enforcement organizations. This work is motivated by three deficiencies in the literature: (1) no integrative review summarizes Indonesian and worldwide research on cyber OSINT for CT; (3) The policy implications of Indonesia's changing regulatory landscape, especially the relationship between Law No. 5/2018 on Counter-Terrorism and Law No. 27/2022 on Personal Data Protection (UU PDP), have not been thoroughly examined; (2) Indonesian academic work has remained primarily normative-juridical, with little engagement with technical tradecraft.

In order to fill these gaps, this study poses the following research question: How can Indonesia operationalize cyber OSINT as a strategic CT capacity while balancing it with UU PDP 27/2022 and democratic accountability? A systematic reanalysis of the Surabaya 2018 attack and the 2024 JI dissolution as paired OSINT instances, a federated OSINT philosophy adapted to Indonesia's legal and institutional framework, and the first SLR combining Indonesian and worldwide OSINT-CT literature are the three contributions.

2. Theoretical Framework

A three-layered structure is used in the article. The intelligence cycle, which organizes intelligence activities across planning, collecting, processing, analysis, dissemination, and assessment, is the first layer (Lowenthal, 2019; NATO, 2001). Despite criticism that it oversimplifies intelligence work (Hulnick, 2006), it is still the most often used framework for assessing how OSINT fits into a larger CT organization. The second layer is second-generation OSINT (Williams & Blum, 2018), which uses lexical, network, and geospatial techniques to conceptualize the qualitative transition from broadcast-era OSINT to internet-scale open-source analysis. Van Puyvelde and Tabarah (2025) qualify this model, arguing that although tooling changes, the core intelligence problems—reliability, overload, and ethics—remain the same. Securitization theory (Buzan, Waever & de Wilde, 1998), which Hara and Azizah (2022) modified for Indonesia, is the third layer. This theory explains how civil society's desecuritization of terrorism limits its growth, but rhetorical securitization of terrorism permits it. When taken as a whole, the framework enables the study to evaluate what OSINT may technically do as well as the political circumstances that make its growth politically viable.

3. Research Methods

3.1. Research Design

The study uses a qualitative design that combines comparative case study analysis with a systematic literature review (SLR) (Yin, 2018). The case studies anchor findings in two significant Indonesian events, while the SLR establishes the current status of the field. The combination offers depth—a concentrated analysis of how themes appear in Indonesia—as well as breadth—a worldwide synthesis.

3.2. SLR Protocol (PRISMA 2020)

The review was conducted in accordance with PRISMA 2020 guidelines (Page et al., 2021). Four databases were searched: Google Scholar, DOAJ, Semantic Scholar, and Garuda Kemdikbud (SINTA-indexed Indonesian journals). The search was carried out from January 2014 to December 2025. Boolean search strings were used to link three concept blocks: ("open source intelligence" OR "OSINT" OR "SOCMINT") AND ("counter-terrorism" OR "radicalization" OR "violent extremism") AND ("cyber" OR "online" OR "digital"). For Garuda, strings in Indonesian were added. Peer review, significant OSINT or SOCMINT focus,

CT/extremism relevance, English or Indonesian language, and full-text availability were all prerequisites for inclusion. Opinion pieces and commercial white papers were not included.

Table 1. PRISMA 2020 Record Selection Flow

Phase	n
Records identified (all databases)	268
Records after duplicates removed	227
Records screened (title/abstract)	227
Records excluded at screening	138
Full-text records assessed	89
Full-text records excluded	42
Studies included in synthesis	**47**

3.3. Case Study Methodology

Purposive sampling was used to choose two examples. The 2018 Surabaya bombings were selected as an illustration of an OSINT-failure-digital signals that were visible before an assault but were not converted into meaningful intelligence. Because Jemaah Islamiyah's official dissolution in 2024 was the outcome of ongoing interagency monitoring pressure, it was used as a contrasting example of intelligence success. Open-source court documents, security assessments, scholarly studies (Schulze, 2018; IPAC, 2018; Virgantara et al., 2024b), BNPT declarations, and reliable press coverage were among the data sources. Bias was accounted for by cross-source triangulation. This study's inability to acquire classified operational data is a significant constraint; interpretations are based solely on publicly accessible information.

4. Results and Discussion

Six topic clusters were generated by synthesizing the 47 included papers. The case study evidence and policy implications are discussed in conjunction with these conclusions.

4.1. OSINT Evolution and the Cyber Shift

From the Foreign Broadcast Monitoring Service (1941) to the DNI Open Source Center (2005) to the ODNI's present designation of OSINT as the "INT of first resort" (ODNI & CIA, 2024), the included material traces OSINT. According to Williams and Blum (2018), second-generation OSINT—which is distinguished by lexical, network, and geographic analysis techniques as opposed to straightforward broadcast monitoring—has been created by internet-scale data. Van Puyvelde and Tabarah (2025) describe this framing as evolutionary rather than revolutionary, pointing out that ethical constraints, information overload, and source reliability are persistent intelligence issues that new tools have made worse rather than better. The AI-integration literature is just now starting to address Hulnick's (2002) early criticism that "the greatest problem is the excess of OSINT now overwhelming the ability of analysts to sort through it" (Browne et al., 2024).

4.2. Cyber Tooling and AI Integration

The review details a toolchain that is developing quickly. Graph-based link analysis is made possible by Maltego, internet-connected devices are indexed by Shodan, and hundreds of types of specialized resources are cataloged by the OSINT Framework. Open-source geolocation, picture forensics, and social media analysis may generate intelligence-grade results without classified access, as shown by Bellingcat's investigation methods, which were most famously used in the MH17 attribution (Bellingcat, 2015). Four integration topics are identified by Browne and colleagues' (2024) comprehensive assessment of 163 AI–OSINT studies: automated danger alerts, picture and video forensics, natural-language processing for multilingual extremist content, and predictive network analysis. Yadav et al. (2023) provide a detailed account of machine learning applications in digital forensics and social network research. The identification of multilingual support and real-world integration as major needs by Browne and colleagues (2024) is an important result that is directly related to Indonesia's requirement for the detection of extremist content in Indonesian.

4.3. Terrorist Exploitation of Cyberspace

Four methods of terrorist cyber exploitation are identified by Wiil's (2011) foundational volume: fundraising, recruiting, operational planning, and propaganda distribution. In their assessment of OSINT extraction for information relevant to terrorism, Chaudhary and Bansal (2022) divide these operations into three phases: data-acquisition, enrichment, and knowledge inference. They highlight notable academic development in each of these phases. While Hidayat and colleagues (2025) identify encrypted messaging platforms as the main route for tactical coordination, Astuti (2024) and Safri and colleagues (2025) record the movement of recruiting from organized face-to-face networks to social media in the Indonesian setting.The financial aspect is highlighted by BNPT's discovery of Rp 5.09 billion in terrorism financing across 16 instances (2023–2025). While open platforms offer abundant SOCMINT signals, important operational material has moved to closed, end-to-end encrypted channels, restricting open-source visibility of the most harmful behavior, according to the Counter Extremism Project (2024) and Omand and colleagues (2012).

4.4. OSINT Applications in Counter-Terrorism

Four recurrent CT applications are found in the review. First, a long-term SOCMINT study of Salafi-jihadist communities and reports of overseas fighters is used to detect radicalization. Propaganda analysis, which includes categorization, attribution, and the creation of counternarratives, comes in second. The operational use of social media intelligence for counter-narrative activity by Densus 88 is documented in Virgantara and colleagues' (2024b) publication in this journal. The third method is network mapping, which is a graph study of impact links and organizational structures. Fourth, machine-learning techniques for sentiment shift and anomaly identification provide early warning. Lavinia and colleagues (2023) argue that OSINT "is still under-exploited as a source of intelligence information in Indonesia," citing closed agency postures and a lack of organized collaboration with practitioners in academia and civil society as the reasons for this deficiency in the most relevant Indonesian study. In a similar conceptual contribution, Prawira (2025) proposes a defensive–offensive OSINT architecture for Indonesian CT using Prunckun's intelligence strategy paradigm.

4.5 Ethical, Legal, and Privacy Dimensions

A structural tension is found in Ghioni and colleagues' (2023) thorough examination of 571 articles on the governance, ethical, legal, and societal consequences of AI-powered OSINT: existing privacy and oversight regimes become less effective as tools get more powerful. This conflict is documented in the Indonesian CT context by Masyhar and Emovwodo (2023), where techno-prevention methods run the danger of undermining due process. The legal framework in Indonesia is multilayered yet lacking. The mandate of BIN is governed by Law No. 17/2011 on State Intelligence; Law No. 5/2018 on Counter-Terrorism introduces preemptive-justice provisions (Articles 43A–43D) but does not specify OSINT tradecraft standards; and Law No. 27/2022 on Personal Data Protection (UU PDP), which is mandatory as of October 2024, limits the processing of personal data while leaving national security exceptions unclear. According to Situmeang (2026), "the absence of specific laws that explicitly regulate cyberterrorism crimes" leads to "enforcement challenges." Astuti (2024) investigates how the updated UU ITE (Law No. 1/2024) falls short of a complete cyber-CT legislation while addressing cyber-terror charges in part.

4.6 Indonesia's OSINT Institutional Landscape

BIN (strategic intelligence), Densus 88 (kinetic CT and counter-narrative), BNPT (prevention and deradicalization), BAIS-TNI (military intelligence), and BSSN (cyber and cryptography, parent agency of Poltek SSN) are the five state actors mapped by the review. Each agency has specialized—BIN in technology-based intelligence, BNPT in socio-psychological counter-radicalization, and Densus 88 in tactical-operational capabilities, which produces analytical depth but coordination friction, according to Prasetyo and colleagues (2025). The success and limitations of Densus 88's Counter-Narrative Subdirectorate's SOCMINT activities are documented by Virgantara and colleagues (2024a), who note platform-policy changes, data volume, and privacy issues as the main obstacles. Through interviews with Densus 88 employees in Java and Bali, Hidayat and colleagues (2025) support similar findings, adding regulatory loopholes and low digital literacy to the list of constraints.

The most institutionally advanced civilian OSINT capacity is provided by Drone Emprit, which was created by Ismail Fahmi and operationalized through Universitas Islam Indonesia's Drone Emprit Academic platform (Fahmi, 2018). The software analyzes Indonesian social media using NLP, sentiment analysis, and social network analysis. However, major terror communications have moved to closed Telegram channels outside of the platform's reach, as admitted by Fahmi. This conclusion is consistent with the encrypted-platform issue in the international literature.

4.7. Case Study Analysis: Surabaya 2018 and JI Dissolution 2024

4.7.1 The 2018 Surabaya Bombings: An OSINT Failure

Four discernible digital signals preceded the Surabaya attacks, according to Schulze's (2018) CTC Sentinel analysis and the IPAC (2018) Report No. 51: (1) the perpetrating families' use of propaganda from Inspire, Rumiyah, and Al-Fatihin; (2) the Oepriarto family's unusual Facebook activity cessation in 2014; (3) pro-IS Telegram channel calls for violence in Indonesian; and (4) interaction with AQAP and IS instructional materials on improvised explosives. These signals were distributed throughout several families and platforms. Pre-attack synthesis was not accomplished. Because there was no interagency OSINT synthesis process in place, the attack is a prime example of an OSINT-gap failure: observable signals that were not incorporated into actionable intelligence.

Crucially, post-attack OSINT efforts were more successful. According to BenarNews (2018), within weeks of Surabaya, Indonesian police employed Telegram monitoring to thwart a planned attack on a police district headquarters. The Surabaya failure was institutional and architectural, a result of fragmentation, rather than a fundamental inability, as this quick shift from failure to effectiveness highlights. The integration did not exist, although the capacity did.

4.7.2 The 2024 JI Dissolution: OSINT as Sustained Pressure

At a ceremony overseen by the BNPT in Bogor on June 30, 2024, sixteen top JI officials publicly announced the organization's demise. About 130 people from all throughout Indonesia signed the proclamation, which was signed by notable individuals including Para Wijayanto, Abu Rusdan, and Abu Fatih. OSINT was not the only factor in the breakup; JI's own strategic recalculations, BNPT's deradicalization initiatives, and Densus 88's kinetic operations also had a role. However, it took place within the framework of ongoing intelligence surveillance, which included financing routes, leadership communications, and open-source tracking of JI's pesantren network (BNPT reported 198 JI-affiliated schools). Thus, the breakup serves as an example of OSINT as one component of a comprehensive, institutionally cohesive CT campaign—exactly the kind of architecture that the Surabaya case lacked.

4.8 Policy Implications: A Federated OSINT Framework

The report suggests five elements for an Indonesian federated OSINT philosophy, which is a research-based foundation for institutional design rather than a comprehensive operational blueprint, by synthesizing the SLR findings and case study analysis.

An OSINT Coordination Cell comes first. A permanent interagency cell with seconded staff from Densus 88, BNPT, BIN, and BAIS-TNI that is perhaps located at BSSN and is controlled by tradecraft norms based on ODNI (2024) ICD-301 principles. The interagency fragmentation reported in Prasetyo and colleagues (2025) and the Surabaya case is immediately addressed by this.

Second, an NLP pipeline for Indonesian. A research-operational collaboration on dialect-aware extremist material identification and counter-narrative development involving Poltek SSN, BSSN, and university OSINT units. The Indonesian academic environment, which includes the institutional home of this study, is well-positioned to create multilingual support, which Browne and colleagues (2024) identified as a critical weakness in present AI-OSINT systems.

Statutory clarity comes in third. A separate cyber-CT modification to Law No. 5/2018 that outlines legal digital monitoring under court supervision, explicitly addressing the coordination issues noted by

Hidayat and colleagues (2025) and Situmeang's (2026) legal-gap study. Additionally, the revision should include accountability procedures and retention caps that are in line with UU PDP 27/2022.

Fourth, a code of practice that is consistent with the UU PDP. An Indonesian version of the ODNI's IC OSINT Strategy 2024–2026, which addresses Ghioni and colleagues' (2023) conclusion that AI-powered OSINT has surpassed governance frameworks worldwide and offers operational guidelines for OSINT practitioners as well as a point of reference for oversight organizations.

Fifth, collaboration with civic society. Drone Emprit Academic and similar platforms should be formally incorporated into a non-classified threat-information sharing forum with stringent UU PDP safeguards. This will directly address Lavinia and colleagues' (2023) finding that Indonesian-language capability is underutilized when civil-society OSINT practitioners are excluded from intelligence collaboration.

These elements depend on one another. Without a legal framework, the Coordination Cell runs the danger of failing to provide accountability; without operational doctrine, the legal framework results in formal compliance without analytical capacity; and without civil-society collaboration, both render Indonesian-language NLP inadequate. The JI dissolution instance illustrates the rewards to institutional coherence, whereas the Surabaya case illustrates the price of fragmentation

5. Conclusion

In order to address how Indonesia can operationalize cyber OSINT as a strategic CT capability while balancing it with democratic accountability and legal constraints, this paper has presented a systematic literature review of cyber OSINT for CT along with a case study analysis of the 2018 Surabaya bombings and the 2024 JI dissolution.

There are three main conclusions. First, despite significant changes in its tools, scope, and ethical implications, cyber OSINT has developed into a strategically important field whose fundamental logic—turning publically accessible information into actionable intelligence—remains consistent with traditional intelligence operations. Second, there is actual but dispersed institutional participation in Indonesia: Densus 88, BNPT, BIN, BAIS-TNI, and BSSN all bring unique capabilities that have not been unified under a common theory. Third, Law No. 5/2018, UU PDP 27/2022, and the updated UU ITE together provide a framework that falls short of an established cyber-CT legislation, leaving the legal superstructure necessary for sustained OSINT expansion unfinished.

The case studies provide specific examples of these conclusions. An architectural flaw in the Surabaya 2018 assault featured detectable but disjointed OSINT signals. Open-source monitoring played a major role in the persistent, institutionally cohesive intelligence pressure that led to JI's demise in 2024. It is useful to note that the strategic value of OSINT is found in its organization, governance, and integration rather than in the capacity itself.

There are three directions for further study. First, Poltek SSN has a natural institutional advantage in an empirical research of radical content identification in Indonesian utilizing publicly available data. Second, a comparison of Indonesia's OSINT stance with those of its ASEAN counterparts. Third, a long-term assessment of JI-dissolution online network activity beyond 2024 to determine if the organization has completely demobilized or reconstituted—a issue that cyber OSINT techniques are ideally suited to address.

References

ANTARA News. (2025, December 30). *BNPT ungkap 27 rencana serangan terorisme berhasil digagalkan*. ANTARA. https://www.antaranews.com

APJII. (2024). *Survei penetrasi internet Indonesia 2024*. Asosiasi Penyelenggara Jasa Internet Indonesia.

Astuti, S. A. (2024). Literasi kemanfaatan teknologi terhadap cyber terrorism di era disrupsi dengan AI (Artificial Intelligence). *Indonesian Journal of Criminal Law and Criminology*, 5(2), 88–102.

Bellingcat Investigation Team. (2015). *MH17: The open source evidence*. Bellingcat. https://www.bellingcat.com

BenarNews. (2018, June 20). Indonesian authorities uncover plot to attack police district HQ. *BenarNews*. https://www.benarnews.org

Browne, T. O., Abedin, M., & Chowdhury, M. J. M. (2024). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. *International Journal of Information Security*, 23(4), 2911–2938.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Chaudhary, M., & Bansal, D. (2022). Open source intelligence extraction for terrorism-related information: A review. *WIREs Data Mining and Knowledge Discovery*, 12(5), e1473. https://doi.org/10.1002/widm.1473

Counter Extremism Project. (2024). *Extremist content online: Telegram used by ISIS to spread propaganda globally*. CEP. https://www.counterextremism.com

Fahmi, I. (2018). *Drone Emprit Academic: Software for social media monitoring and analytics*. Universitas Islam Indonesia. https://dea.uii.ac.id

Ghioni, R., Taddeo, M., & Floridi, L. (2023). Open source intelligence and AI: A systematic review of the GELSI literature. *AI & Society*, 39(4), 1827–1842. https://doi.org/10.1007/s00146-023-01628-x

Hara, A. E., & Azizah, N. (2022). Securitization of terrorism and human rights protection in Indonesia. *KnE Social Sciences*, 7(11), 83-95.

Hidayat, F., Hermawan, A., & Setyawan, B. (2025). From threat assessment to action: Counterterrorism Special Detachment 88's perspective on combating cyber terrorism in Indonesia. *Journal of Lifestyle and SDGs Review*, 5(2), 1–18.

Hulnick, A. S. (2002). The downside of open source intelligence. *International Journal of Intelligence and CounterIntelligence*, 15(4), 565–579.

Hulnick, A. S. (2006). What's wrong with the intelligence cycle. *Intelligence and National Security*, 21(6), 959–979.

Institute for Policy Analysis of Conflict. (2018). *The Surabaya bombings and the future of ISIS in Indonesia* (IPAC Report No. 51). IPAC.

Kemp, S. (2024). *Digital 2024: Indonesia*. We Are Social & Meltwater.

Lavinia, N., Pamungkas, B. A., & Yusuf, M. (2023). Urgensi pemanfaatan Open Source Intelligent (OSINT) dalam upaya pencegahan aksi terorisme di Indonesia. *Jurnal Sosial Humaniora Terapan*, 5(2), 88–101.

Lowenthal, M. M. (2019). *Intelligence: From secrets to policy* (8th ed.). CQ Press.

Masyhar, A., & Emovwodo, O. (2023). *Techno-Prevention in Counterterrorism : Between Countering Crime and Human Rights Protection* (Vol. 3, Issue 3).

NATO. (2001). *NATO open source intelligence handbook*. North Atlantic Treaty Organization.

Office of the Director of National Intelligence & Central Intelligence Agency. (2024). *The IC OSINT strategy 2024–2026*. ODNI.

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, 27(6), 801–823.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71.

Prasetyo, D., & Wilantara, M. (2025). The change management of human resource development in terrorism prevention: Study at BIN-BNPT-Densus 88. ETTISAL: Journal of Communication, 10(2).

Prawira, B. Y. (2025). Applying Prunckun's intelligence strategy model in counter-radicalism and terrorism efforts in Indonesia: A defensive–offensive approach. *Security Intelligence Terrorism Journal*, 2(1), 1–18.

Safri, H. M., Utomo, S. L., & Hakim, L. (2025). Terorisme di era digital. *Jurnal Hukum Pelita*, 6(2), 639–652 .

Schulze, K. E. (2018). The Surabaya bombings and the evolution of the jihadi threat in Indonesia. *CTC Sentinel*, 11(6), 1–6.

Situmeang, S. M. T. (2026). Law enforcement of cyber terrorism crimes in strengthening national data security from the perspective of Indonesian positive law. *Sortuz: Oñati Journal of Emergent Socio-Legal Studies*, 16(1), 5–24.

Van Puyvelde, D., & Tabarah, F. (2025). The rise of open-source intelligence. *European Journal of International Security*, 10(1), 1–22.

Virgantara, A. P., Nita, S., & Rahmanto, D. N. (2024a). Optimizing social media intelligence for countering radicalism by the Subdirectorate of Counter-Narrative, Densus 88. *Policy Law Notary and Regulatory Issues*, 3(2), 145–162.

Virgantara, A. P., Nita, S., & Rahmanto, D. N. (2024b). The role of social media in supporting information and intelligence gathering by Densus 88. *Security Intelligence Terrorism Journal*, 1(2), 92–100.

VOI. (2026, January 7). Densus 88: Tidak ada aksi terorisme sepanjang 2025. *VOI*. https://voi.id

Wiil, U. K. (Ed.). (2011). *Counterterrorism and open source intelligence*. Springer.

Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise* (RR-1964-OSD). RAND Corporation.

Yadav, A., Kumar, A., & Singh, V. (2023). Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security. *Artificial Intelligence Review*, 56(11), 12407–12440.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.