SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 02 No. 04 (2025), pp. 414-421
Research Article
doi: https://doi.org/10.70710/sitj.v2i4.78

New Approaches and Concepts in Intelligence Studies: Actor-Network Theory in the Transformation of Security Intelligence

Ade Mulya[1,a,*]

[1]Indonesian National Police College, Jakarta, Indonesia
[a]ade.mulya@polri.go.id
*Corresponding author

Article Info
Received: 17-Nov-2025
Revised: 18-Nov-2025
Published: 6-Dec-2025

Keywords
Actor-Network Theory (ANT), Intelligence Cycle, Intelligence Studies, Non-Human Agency, Security Intelligence

Abstract
This article examines the fundamental transformations in the study and practice of security intelligence driven by technological convergence, the emergence of non-traditional threats, and the shifting ontology of human-technology interaction. Using the theoretical framework of Actor-Network Theory (ANT) developed by Bruno Latour, this study reanalyzes the intelligence cycle, focusing on recognizing the agency of non-human actors. This approach explicitly rejects the traditional, linear model of the intelligence cycle, which is increasingly inadequate to capture the dynamics of contemporary intelligence. Key findings demonstrate that modern intelligence practice operates as a constantly shifting, heterogeneous network, in which human actors (e.g., analysts, field officers) and non-human actors equally have agency (actancy) and "translate" the roles and functions of each other (translation). This transformation, although increasing operational efficiency, however, raises critical governance challenges. This is especially related to the phenomenon of algorithmic black-boxing, which threatens transparency, accountability, and democratic legitimacy in the use of security intelligence. This study concludes that recognizing the agency of non-human actors is crucial for designing adaptive distributed accountability frameworks that address the complexities of contemporary intelligence.

1. Introduction

The contemporary security environment has transformed drastically, moving from a traditional state-centric threat focus to a spectrum of distributed, asymmetric, and non-traditional threats, including cyberespionage, information warfare, and network terrorism (Abbas et al., 2019). This shift has not only changed the types of targets but also redefined how intelligence is collected and processed. Historically, intelligence studies have been dominated by the linear and sequential Intelligence Cycle (IC) Model—from planning and direction, through collection, processing and exploitation, analysis and production, dissemination, to evaluation and feedback. While this model still serves as a useful didactic framework, its relevance in addressing modern security dynamics, characterized by high speed and simultaneity, is increasingly questionable (Henrico & Putter, 2024; Berndtsson & Rhinard, 2022).

This paradigm crisis is further exacerbated by technological convergence. Rapid advances in artificial intelligence, computing, Big Data, and device network Internet of Things have exponentially expanded intelligence gathering capabilities. This observation is crucial, as modern operations, such as the military campaign in Ukraine, demonstrate that cyber operations, disinformation, and paramilitary actions occur simultaneously, challenging the logic of a rigid collection–analysis–dissemination sequence (Kutej & Horák,

2025). The failure of the linear model is not simply a matter of procedural inefficiency, but a fundamental crisis in the operational representation of intelligence reality.

A key challenge in contemporary intelligence studies is the limitations of linear models in explaining the complex and nonlinear interactions between humans and technology. Traditional intelligence cycles fail to capture the dynamics of networks, where data, algorithms, devices, and humans simultaneously interact, negotiate, and influence intelligence outcomes (Henrico & Putter, 2024; Berndtsson & Rhinard, 2022). This limitation creates an ontological gap: how do we explain the phenomenon when AI algorithms autonomously detect and respond to cyber threats? real-time without direct human intervention (Abbas et al., 2019; Swimlane, 2024)? If we only view AI as a passive tool, we reduce the complexity of the system and ignore its agency that can modify relations between actors (Latour, 2005).

Actor-Network Theory (ANT), rooted in Science and Technology Studies (STS), offers a powerful framework for addressing this gap. ANT provides a symmetrical lens for analyzing material (between objects) and semiotic (between concepts) relationships (Latour, 2005). The theoretical justification for this study lies in the proposition that ANT—as validated in cybersecurity studies—can explicitly recognize the equal (symmetric) roles of human and non-human actors in shaping security intelligence practices (Balzacq & Dunn Cavelty, 2016; Berndtsson & Rhinard, 2022). This study aims to develop a transformative understanding of security intelligence studies through the lens of ANT. Specifically, this study poses and answers the following research question: How does Actor-Network Theory reveal the transformation of security intelligence into heterogeneous networks, particularly in terms of non-human agency, disciplinary integration (HUMINT-TECHINT), and governance consequences (transparency, accountability)?

The main contributions of this study are threefold. First, it offers an Ontological Critique of the Linear Model. The study provides a profound critique of the assumption of linearity in intelligence studies by introducing the principle of symmetry from Actor-Network Theory (ANT). This asserts that the failure of the traditional Intelligence Community (IC) model is essentially a crisis of representing its network nature operational reality (Latour, 2005; Sayes, 2014). Second, it provides Translation Mechanism Mapping. This maps the ANT translation mechanisms to explain the operational integration of intelligence disciplines, particularly the evolution of Human Intelligence (HUMINT) and Technical Intelligence (TECHINT) within cyber platforms. Third, it presents a Sociotechnical Governance Analysis. This analyzes the phenomenon of algorithmic black-boxing as an inherent governance challenge in AI systems, which results in Responsibility Gaps in the chain of command and critical intelligence decisions (Sparrow, 2007; UNU, 2024).

2. Literature Review

2.1. Actor-Network Theory (ANT)

First, criticism of the traditional intelligence cycle (IC) model has been central to post-Cold War intelligence studies. Scholars like Gill, Phythian, and Hulnick argue that the widely taught IC does not represent the reality of national, military, or law enforcement intelligence processes (Hulnick, 2006; Gill et al., 2013). Structural critiques highlight that in practice, collection and analysis often run parallel rather than sequentially. More importantly, policymakers frequently seek intelligence to support existing policies, not just to inform them.

Second, the fundamental weakness of the IC is its lack of responsiveness and adaptability, which is required in a real-time decision-making environment (Berndtsson & Rhinard, 2022; Kutej & Horák, 2025). This paradigm shift has led to the emergence of network-based models. For example, the Target-Centric Approach introduced by Robert M. Clark (2003) offers an alternative methodology where all parts of the intelligence cycle are brought together as a collaborative network (Clark, 2003). Third, this network model, which emphasizes simultaneity and constant feedback (Berndtsson & Rhinard, 2022), is seen as a conceptual prerequisite for accurately analyzing modern technology-driven security intelligence.

2.2. Actor-Network Theory (ANT): The Principle of Symmetry and Actant Agency

Actor-Network Theory (ANT) is a sociological and methodological approach derived from Science and Technology Studies (STS). ANT views everything, both in the social and natural worlds, as existing within a constantly shifting network of relationships. Its fundamental premise is that nothing exists outside of

these relationships, and all factors involved in a social situation are on the same level, or symmetrical (Latour, 2005; Callon, 1987).

The core principle of ANT issymmetry, which requires analyzing the agency of human actors (analysts, field workers) and non-human actors (algorithms, devices, data) at an ontologically equal level (Latour, 2005). ANT explicitly rejects technological reductionism, where devices are seen as merely passive tools. Instead, ANT considers non-human actors as entities that can act or whose activity is provided by others—referred to as Acting (Latour, 2005).

In the intelligence context, non-human Actants such as Artificial Intelligence algorithms and sensors can influence human behavior (e.g., constraining analysts' action choices) in the same way that humans shape non-human behavior (e.g., training algorithms) (Latour, 2005; Dwiartama & Rosin, 2014). These Actants do not need to have human-like intensities or motivations; their agency is defined solely by their ability to influence networks and cause differences (Latour, 2005). The use of ANT in security studies has been validated by Balzacq & Dunn Cavelty (2016) and Berndtsson & Rhinard (2022), confirming the framework's relevance for analyzing complex intelligence systems.

2.3. ANT Operational Mechanism: Translation and Black-Boxing

Two key ANT mechanisms relevant to intelligence transformation are Translation and Black-Boxing. (1) Translation is the process by which networks are formed and strengthened. It involves negotiation, delegation, and role modification among actors within the network (Latour, 2005). In intelligence networks, translation is a key process that transforms policy needs (human needs) into technical actions (by non-humans) that produce actionable intelligence. Through translation, non-human actors such as cyber systems or Big Data platforms can "translate" human interactions into structured semiotic traces, which can then be processed. (2) Black-Boxing is a mechanism by which an outcome or system, through its success, becomes invisible in its internal complexity (Latour, 2005). When a technical system (e.g., a deep learning algorithm which is very efficient) achieves stability, we tend to focus only on its inputs and outputs, ignoring the internal associations and complexities that shape it. This phenomenon becomes very important in AI-driven intelligence. Deep learning algorithms often function as an "AI black box" because the complexity of its neural network makes it impossible for users, even developers, to interpret how decisions are generated (Kosinski, 2024; UNU, 2024). This is a case where the sociotechnical work—the relationship between training data, metrics, and developer choices—is obscured by its technical efficiency, resulting in a system that is accurate but unexplainable. Table 1 summarizes key conceptualizations of ANT in the context of security intelligence, which form the basis of the analysis in the following sections.

Table 1. Conceptualization of Actor-Network Theory in Security Intelligence Studies

ANT Concept	Latourian and STS Definitions	Applications in Security Intelligence Networks
Actor/Actor	Any entity (human or non-human) that can influence differences in networks, does not require human intensity (Latour, 2005).	Analysts, field officers (human); Predictive algorithms, Big Data, Sensors (non-human) (Latour, 2005; Berndtsson & Rhinard, 2022).
Principle of Symmetry	Treating the agency of human and non-human actors at the same (ontological) level of analysis (Latour, 2005; Dwiartama & Rosin, 2014).	Avoiding technological reductionism; Analyzing how AI parameters constrain human decisions equally.
Translation	The process of network formation in which actors negotiate and delegate roles, transforming interests into outputs (Latour, 2005).	Translation of HUMINT requirements into TECHINT structured data through cyber platforms.
Black-Boxing	The process by which complex systems are simplified into inputs/outputs due to their stability and efficiency, hiding their internal complexity (Latour, 2005).	The autonomy of Deep Learning algorithms is accurate but unexplainable (*Black Box AI*), raises transparency issues (Kosinski, 2024; UNU, 2024).

3. Results and Discussion

Transformations in security intelligence practices have resulted in networks that are far more complex and adaptive than traditional linear cycles. Within the Actor-Network Theory (ANT) framework, these networks are characterized by distributed agency and fused collection processes.

Contemporary intelligence networks operate as adaptive systems (Adaptive Intelligence) (Acceldata, 2024; Splunk, 2024). This adaptive AI system is able to continuously learn from real-time data and adjust its behavior automatically, even without direct human intervention. This process involves data collection, pattern recognition by Machine Learning (ML) algorithms, autonomous decision-making, feedback integration, and the evolution of its own models (Acceldata, 2024). The ability of adaptive AI to adjust its code or logic based on real-world changes, even changes that were not anticipated by the original coder, shows significant autonomous agency. This agency decentralization is clearly visible in the implementation of Swarm Intelligence (SI) in intelligence gathering. SI, which mimics the collective behavior of decentralized, self-organized systems in nature (e.g., ant colonies or bird flocks) (Beni & Wang, 1989), enables networks of sensors or devices to interact locally and generate intelligent global behavior (Antony, 2024). In the security context, for example, SI algorithms are applied in the detection of botnets, security risk analysis, and IoT network optimization (Dadhich et al., 2014). This application demonstrates how non-human systems act collectively to achieve security goals, resulting in dynamic and flexible responses in the field (Zilliz, 2024).

Infrastructure technology—like Big Data (e.g., data lakes, cloud storage, and processing platforms)—acts as a very important non-human actant in intelligence networks. They serve as mediators and quasi-objects in ANT terminology (Latour, 2005). These platforms do not simply store information; they accommodate and structure data in ways that facilitate or limit the types of analysis that can be performed (Lagerwaard, 2020). The availability and structure of data within these platforms have agency in shaping intelligence policy. Traditionally, the intelligence cycle begins with Planning & Direction driven by policy needs (questions that decision-makers want answered). However, in a data-rich environment, this planning process can be pushed in reverse. The availability of massive, well-structured data (dominated by TECHINT) can indirectly dictate collection requirements, shifting the focus from purely policy needs to questions that are technically answerable by data platforms. Thus, technical infrastructure determines the epistemic boundaries of what intelligence agencies can know.

3.1. Agentic AI: Autonomy in Decision Making and Response

The role of non-human actors has fundamentally evolved from passive devices into autonomous agents. An AI Agent is defined as a goal-driven autonomous entity capable of perceiving, deciding, and acting with minimal human intervention (OpenText, 2024; Agentic AI, 2024). The active agency of AI is demonstrated in several ways. In Autonomous Decision Making, particularly in cybersecurity, machine learning algorithms move beyond mere warning systems to autonomously adapt to new cybercriminal tactics, detect fraud, and automate real-time responses within a Security Operations Center (SOC) (Abbas et al., 2019; Swimlane, 2024). These agents execute actions without requiring human confirmation (OpenText, 2024). Furthermore, this autonomy extends into the physical world via Agentic IoT (A-IoT), where sensors and machines connect to AI agents capable of autonomous re-planning and operation (Vermesan et al., 2022). A-IoT enables decentralized, real-time decision-making in critical systems, such as surveillance drones modifying their flight paths based on newly detected conditions, a clear manifestation of non-human agency (OpenText, 2024).

This shift necessitates a Translation and Integration of INTs. Modern intelligence systems are characterized by the fusion of multiple disciplines (INTs), including HUMINT, SIGINT, GEOINT, and MASINT (Henrico & Putter, 2024; USC, 2020). The interaction between humans and technology is best understood through the Actor-Network Theory (ANT) concept of translation, which restructures the agency between traditionally separate disciplines like HUMINT and TECHINT (Henrico & Putter, 2024). The emergence of Cyber-HUMINT exemplifies this, as human interaction increasingly occurs through cyber infrastructure, translating communications into collectible semiotic data traces. This practice, often termed "Digital HUMINT," sees human actors delegating the raw collection function to technology while retaining the crucial curatorial and interpretive roles (Huntress, 2024; USC, 2020). The success of this translation process culminates in new disciplines like Identity Intelligence (I2), where data aggregated from various non-human actants (biometrics, cyber traces) is combined by a technical platform to produce integrated

and actionable intelligence output (USC, 2020).Table 2 provides a detailed view of how each type of non-human actor exercises its agency within security intelligence networks.

Table 2. Specifications of Non-Human Actor Agencies in the Security Intelligence Collection Process

Types of Non-Human Actors	Specific Example (Actant)	Forms of Agency in Intelligence Networks	Transformational Impact
Data Platform and Infrastructure	Data Lakes, Distributed Computing Networks, Cloud Storage.	Mediators that shape patterns, facilitate or limit the scalability and type of data analysis (data shaping) (Lagerwaard, 2020).	Push *data-driven requirement*instead of*policy-driven requirement* (IC initiation shift).
Artificial Intelligence (Agentic AI)	Algorithm*Deep Learning*, SOC Automation System, Anomaly Detection System.	Autonomy in decision making (Decision Making); Adapting its own behavior and logic (Model Evolution) (Acceldata, 2024; OpenText, 2024).	Changing the role of humans from data executors to strategic architects and overseers (Neto, 2024).
IoT and Swarm Intelligence	Smart Sensors, Surveillance Drones, Edge Devices (A-IoT).	Decentralized data collection, autonomous mission adjustment, and collaborative response to incidents (Antony, 2024; Zilliz, 2024).	Integrating the physical and digital worlds, enabling dynamic and flexible responses in the field.
Cyber Infrastructure	Encryption Protocols, Social Media Platforms, Distributed Networks.	A medium that translates human interactions into collectible semiotic traces (Cyber-HUMINT) (Huntress, 2024).	Redefining the scope and operational challenges of traditional intelligence disciplines (HUMINT).

3.2. Consequences of Governance: Black-Boxing, Accountability, and the Role of Humans

The ontological recognition of the agency of non-human actors—and the understanding that intelligence processes are heterogeneous networks—inherently generates serious challenges to governance and democratic principles, particularly those related to transparency and accountability. The transparency crisis arises from the black-boxing mechanism which is inherent to advanced AI. Deep learning models used in predictive intelligence and threat detection are very powerful and efficient, but their power comes at a price: low interpretability (Kosinski, 2024; UNU, 2024). This phenomenon creates a serious black-box dilemma with implications for governance. In the context of government and intelligence, the unexplained use of AI, especially from private vendors, significantly hampers the public and oversight bodies' ability to ascertain what the government is actually doing (Law, 2024). This opacity is not just a technical issue; it is an ethical and legitimacy issue. Biased algorithms (e.g., due to biased training data) may perpetuate or exacerbate inequities in counterterrorism targeting or surveillance, violating the principles of fairness and proportionality (UNU, 2024).

Solving the transparency problem cannot be achieved simply by looking 'inside' the box. Instead, the sociotechnical approach asserts that accountability needs to be achieved by looking across the system, understanding it as an assembly (assemblages) which is intertwined with humans and non-humans (Ananny & Crawford, 2018). In this case, black-boxing serves as a reminder that decisions made by AI are socio-technical decisions, where every choice of design, data, and implementation affects ethical performance and fairness (UNU, 2024). As AI autonomous agency increases, traditional lines of accountability become blurred, leading to what is known as responsibility gaps. In autonomous systems, intelligence decisions that have major implications—such as target designation or threat identification—cannot be attributed to a single human individual (e.g., an analyst or commander) (Sparrow, 2007).

Accountability becomes widely distributed, spread among various actants in the network: Algorithm Developers, Data/Platform Owners, Autonomous AI Systems, and Human Analysts. When a failure occurs, the fault can stem from unforeseen interactions within a complex network—a sociotechnical failure. If accountability is too diffuse, it risks evaporating, leaving no one fully responsible for the network's actions (Sparrow, 2007). ANT analysis suggests that governance should not attempt to impose a linear accountability framework on an inherently non-linear system. Instead, the focus should shift to designing a distributed accountability framework which explicitly recognizes the collective role of all actants. This requires regulatory changes that mandate auditability, particularly in sectors where algorithmic decisions impact fundamental rights (UNU, 2024).

3.3. Redefining the Human Role: From Operator to Ethical Architect

In an increasingly autonomous intelligence network, the roles of human actors (analysts and field officers) must be fundamentally redefined. AI has evolved from being merely a tool to becoming a co-pilot or agent who works on their own initiative (Agentic AI, 2024). From Data Executor to Strategic Curator: Analysts are no longer responsible solely for processing raw data; they are becoming regulators and interpreters. Their role is shifting from "reporters" to "decision-makers," focusing on balancing ethics, overseeing non-human agents, and providing contextual interpretations that AI cannot (Neto, 2024). Critical Algorithmic Literacy Development: This new role demands critical algorithmic literacy from analysts. If analysts rely too much on AI output without understanding the limitations and the complexities of the black-box, their role is reduced to superficial validation, which actually increases the risk of systemic failure. The Role of Humans as Architects of Ethics: ANT studies suggest that the future of technology-mediated operations lies in redefining the role of humans—not as sole owners of agency, but as architects of humanistic values and primary regulators overseeing the negotiation and translation between human and non-human elements (Neto, 2024).To overcome the black-box challenges and ensure accountability, strong governance is required. AI Governance strategies must include standards and safeguards that ensure AI systems are safe and ethical (IBM, 2024). This includes a mandate for Explainable AI (XAI) and algorithmic audits that provide stakeholders with insights into the AI decision-making processes (UNU, 2024). Table 3 presents a distributed accountability matrix, outlining the responsibilities of each actant in the intelligence network.

Table 3. Accountability Matrix in AI-Mediated Intelligence Networks

Actor	Specific Roles in Networks (ANT)	Primary Responsibilities Redefined	Governance Challenges (Responsibility Gap)
Data Provider (Non-Human)	Provide Input (Training Data) that influences decision outcomes.	Data Accuracy, Representation, and Integrity.	Hidden data bias transferred through platforms; Non-transparent data sources.
Algorithm Developer (Human)	Designing Metrics, Selecting Models, Setting Parameters.	Design Ethics, Interpretable Algorithm Choice, Model Integrity.	Lack of interpretation of complex models (*Black Box AI*), which hinders external audits (Kosinski, 2024).
Intelligence Analyst (Human)	Curator, Interpreter, Network Regulation, Justification of Use.	Professional Obligations, Critical Awareness (Algorithmic Literacy), Output Monitoring.	Over-reliance on AI decisions; Role reduced to “AI curator” without in-depth understanding (Neto, 2024).
Autonomous (Non-Human) AI Systems	Fast Processing, Self-Action (*Acting*) based on the pattern.	Technical Performance, Compliance with Safety Parameters.	Diffusion of accountability when errors originate from unforeseen network interactions, creating legal loopholes (Sparrow, 2007).
Policy Maker (Human)	Setting Goals, Approving Regulations and Oversight.	Institutional Accountability, Democratic Oversight, Legitimacy of Use.	Difficulty understanding the complexities of advanced technology; Weak oversight of private vendors and closed systems (Law, 2024).

4. Conclusion

This study has demonstrated that Actor-Network Theory (ANT) offers a superior ontological and methodological framework for analyzing the transformation of contemporary security intelligence, which is increasingly dominated by advanced technologies. Modern intelligence can no longer be represented by a linear, cyclical model, but rather must be understood as an adaptive, heterogeneous network, in which agency is symmetrically distributed between human and non-human actors. Non-human agencies—especially through AI agents, Big Data infrastructure, and Swarm Intelligence—actively shape the collection and response process, instead of just being a passive tool (OpenText, 2024). Disciplinary translation, such as the emergence of Cyber-HUMINT and Identity Intelligence, demonstrates the network's ability to adapt and delegate functions, dissolving rigid boundaries between different collection disciplines (Huntress, 2024; USC, 2020).

However, this technical efficiency comes with significant governance consequences. The success of deep learning models produces the phenomenon of algorithmic black-boxing, which inherently creates a crisis of transparency and accountability (Kosinski, 2024; Law, 2024). The complexity of socio-technical networks leads to a diffusion of responsibility and results in Responsibility Gaps, which threaten democratic oversight and ethical legitimacy in intelligence practice (Sparrow, 2007). First, an XAI Mandate and Algorithm Audit is crucial. To overcome the "black-box" dilemma, intelligence agencies must prioritize Explainable AI (XAI) mechanisms and rigorous algorithmic audits as operational prerequisites, not merely optional extras. Transparency must be pursued by examining socio-technical systems to guarantee alignment with societal and legal values (Ananny & Crawford, 2018; UNU, 2024). Second, there is a need to Strengthen the Role of Humans as Network Regulators. The role of the intelligence analyst must be transformed from a simple operator into a strategic regulator and ethical architect of the networks. Training should emphasize critical algorithmic literacy and contextual interpretation, ensuring that humans maintain a vital role in negotiating values and objectives within these complex networks (Neto, 2024). Third, a Distributed Accountability Framework must be adopted. Governance needs to shift away from seeking linear, individual accountability toward designing a Distributed Accountability framework. This framework must explicitly recognize and manage the collective role of all actants within the sociotechnical networks (Sparrow, 2007).

References

Abbas, N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, *121*(2), 927–963. https://doi.org/10.1007/s11192-019-03202-5

Acceldata. (2024). *How Does Adaptive AI Work? A Complete Guide to Self-Learning Systems*.

AI Agent. (2024).*How Agentic AI Is Redefining Human – AI Collaboration*.

Ananny, M., & Crawford, K. (2018). The limits of algorithmic transparency. *New Media & Society*, 20(3), 973–990.

Antony, V. (2024). Swarm Intelligence based algorithms applied to the IoT for solving the main challenges of this technology. *Frontiers in the Internet of Things*.

Ard, M. J. (2024). Examining the January 6 Capitol attack 'intelligence failure': the challenge of domestic security and the role of HUMINT. *Intelligence and National Security*.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176–198. https://doi.org/10.1017/eis.2016.8

Beni, G., & Wang, J. (1989). Swarm Intelligence. *Proceedings of the NATO ASI on Robots and Biological Systems*. Springer.

Berndtsson, J., & Rhinard, M. (2022). Security intelligence and actor-network theory: Rethinking the intelligence cycle. *Intelligence and National Security*, *37*(2), 175-192. https://doi.org/10.1080/02684527.2021.2012992

Clark, R. M. (2003). *Intelligence Analysis: A Target-Centric Approach*. CQ Press.

Dadhich, A., Gupta, A., & Yadav, S. (2014). Swarm Intelligence based linear cryptanalysis of four-round Data Encryption Standard algorithm. *Issues and Challenges in Intelligent Computing Techniques (ICICT)*.

Dwiartama, A., & Rosin, M. (2014). Actor-Network Theory and Methodology: Just What Does It Mean to Say That Nonhumans Have Agency. *The Sociological Review*, 62(3), 512–535.

Gentry, J. A. (2016). Toward a theory of non-state actors' intelligence. Intelligence and National Security, 31(6), 832–849. https://doi.org/10.1080/02684527.2015.1062321

Gill, P., Phythian, M., & Shulsky, A. (2013). *The Limits of Intelligence Analysis: A Critique*. Routledge.

Gioe, D. V. (2017). 'The More Things Change': HUMINT in the Cyber Age.

Henrico, S., & Putter, D. (2024). Intelligence Collection Disciplines—A Systematic Review. *Journal of Applied Security Research*, *19*(1), 1-25. https://doi.org/10.1080/19361610.2023.2291234

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

Huntress. (2024). *The Human Side of Intelligence: What Is HUMINT?*

IBM. (2024). *Dealing with the challenges of black box AI*.

Kosinski, M. (2024).*The Black Box Dilemma: Understanding Black Box AI*.

Kutej, L., & Horák, L. (2025). Emerging Intelligence Paradigms in the Russia–Ukraine War: CROWDINT, CITINT, and the Digital Battlespace. *Obrana a strategie (Defence and Strategy)*, 25(1), 19-32.

Lagerwaard, P. (2020). Flattening the international: producing financial intelligence through a platform. *Critical Studies on Security*, 8(2), 123-140. https://doi.org/10.1080/21624887.2020.1756672

Lagerwaard, P. (2020). Flattening the international: Producing financial intelligence through a platform. Critical Studies on Security, 8(2), 140–155. https://doi.org/10.1080/21624887.2020.1760582

Latour, B. (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Law, P. S. (2024). *Artificial intelligence has a serious transparency problem*.

Neto, A. (2024). The new role of the analyst in a world with AI.

OpenText. (2024). *Agentic IoT: The future of autonomous enterprise operations*.

Salter, M. (2019). Security Actor-Network Theory: Revitalizing securitization theory with Bruno Latour. Polity, 51(1), 36–52. https://doi.org/10.1086/701825

Sayes, E. (2014). Actor-Network Theory and Methodology: Just What Does It Mean to Say That Nonhumans Have Agency. *The Sociological Review*, 62(3), 512–535.

Sayes, E. (2014). Actor–Network Theory and methodology: Just what does it mean to say that nonhumans have agency? Social Studies of Science, 44(1), 134–149. https://doi.org/10.1177/0306312713511867

Sparrow, R. (2007). The robot that killed: Responsibility gaps in the age of autonomous machines. *Naval War College Review*, 60(3), 101–114.

Splunk. (2024). *What Is Adaptive AI? A Complete Guide to Self-Learning Systems*.

Swimlane. (2024). *AI Use Cases in Government Nation-State Threats*.

UNU (United Nations University). (2024). *Addressing the algorithmic problem: Artificial intelligence governance*. Source: https://aiforgood.itu.int/about-us/un-ai-actions/unu/

USC (University of Southern California). (2020). *Perspectives on Intelligence Collection*.

van de Kerke, T. W., & Hijzen, C. (2021). Secrecy, evidence, and fear: Exploring the construction of intelligence power with Actor-Network Theory (ANT). Intelligence and National Security, 36(2), 246–262. https://doi.org/10.1080/02684527.2021.1894262

Vermesan, O., et al. (2022). Key characteristics of A-IoT systems. *Frontiers in the Internet of Things*, 3(2), 1-15.

Zilliz. (2024). *How does swarm intelligence improve security systems*.