BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

# Complex vs. Complicated Systems in the Social Network HUMINT Arena

**Anastasios-Nikolaos KANELLOPOULOS, PhD Candidate***

*Department of Business Administration, Athens University
of Economics and Business, Greece
e-mail: ankanell@aueb.gr

## Abstract

Understanding Human Intelligence (HUMINT) within the context of social networks requires a clear distinction between Complicated and Complex systems. Complicated systems are predictable, decomposable, and governed by linear relationships. Complex systems, by contrast, are adaptive, nonlinear, and characterized by emergent behaviors that cannot be fully anticipated.

This paper argues that clandestine and illicit networks—such as terrorist cells, insurgent groups, and criminal syndicates—function as Complex adaptive systems rather than merely complicated organizations. These systems challenge conventional intelligence methodologies because they can absorb disruption, self-organize, and continuously adapt to changing circumstances. Applying complexity thinking can enable HUMINT professionals to detect potential shifts, exploit vulnerabilities, and navigate uncertainty more effectively. The paper ultimately contends that embracing complexity is essential to enhancing HUMINT's effectiveness within dynamic and unpredictable social network environments.

**Keywords:**

Complex Adaptive Systems; Complicated Systems; HUMINT;
Social Networks; Counterintelligence.

**Article info**

Received: 31 October 2025; Revised: 26 November 2025; Accepted: 2 December 2025; Available online: 9 January 2026

Citation: Kanellopoulos, A.N. 2025. "Complex vs. Complicated Systems in the Social Network HUMINT Arena." *Bulletin of "Carol I" National Defence University*, 14(4): 19-30. https://doi.org/10.53477/2284-9378-25-55

## Introduction

Human Intelligence (HUMINT) remains one of the most vital and enduring methods of information collection. Despite the technological revolutions of the 20th and 21st centuries, such as satellite imagery, signals, and artificial intelligence, HUMINT continues to provide unparalleled access to human behavior, motivation, and trust (Clark 2014; Miller 2022). However, the environments in which HUMINT operates are increasingly shaped by social networks (Kanellopoulos 2025). These networks may be physical, grounded in family ties, tribal affiliations, clandestine cells, or insurgent groups, or they may be digital, formed through encrypted platforms, online forums, and global communication infrastructures (Sterelny 2007).

Analysts and practitioners need clear conceptual frameworks to distinguish between systems that are merely Complicated and those that are genuinely Complex in order to operate effectively in such environments (Menkveld 2021). While Complicated systems may appear intricate, they remain fundamentally mechanical, capable of being mapped, decomposed, and addressed through linear analysis. Complex systems, by contrast, are defined by feedback, emergence, and adaptability, meaning their behaviors cannot be understood simply by examining their constituent parts (Lahneman 2010). This distinction is not just theoretical; it has practical implications for how intelligence officers perceive and interact with human networks.

This paper presents a literature review and synthesis of ideas drawn from intelligence studies, systems theory, and social network analysis so as to examine how the Complicated/Complex distinction influences HUMINT practice. It highlights the aspects where traditional approaches remain effective and where they fall short, based on existing research. Furthermore, it demonstrates how adopting complexity thinking can foster greater stability and effectiveness in intelligence operations. The paper argues that HUMINT officers should move beyond mechanistic metaphors and instead adopt methodologies that view human networks as dynamic, adaptive, and emergent systems, best approached through iterative, flexible, and holistic engagement.

## Complicated Systems: Linear but Intricate

Complicated systems can be difficult to comprehend, yet their behavior remains largely predictable. They consist of numerous interdependent components, each performing a specific function, with interactions that are primarily linear and governed by established rules (Kravtsov and Kadtke 1996; Sitte 2009). This principle is most evident in classical engineering. For instance, an aircraft engine comprises thousands of precisely aligned parts that must work together seamlessly to operate correctly. Similarly, modern computer systems integrate hardware and software into

intricate yet comprehensible architectures. Though complicated in construction, such systems can be disassembled, analyzed, and reassembled through systematic procedures that almost always restore functionality. Errors in these systems are rarely mysterious; rather, they can typically be traced to identifiable components. Diagnostic tests allow these issues to be located, repaired, and verified against predefined performance standards. This capacity for restoration illustrates the linear causality inherent in Complicated systems: when a component fails, the system's underlying rules remain unchanged, only its temporary performance is affected (Prencipe, Davies, and Hobday 2003; Huang, Darrin, and Knuth 2012).

This conceptual reasoning is commonly applied to human networks in intelligence operations. Analysts and practitioners have frequently considered clandestine organizations as mechanistic entities: frameworks that, once delineated, could be systematically deconstructed by pinpointing pivotal nodes and removing key individuals. The fundamental assumption is that the isolation or elimination of "high-value targets" would trigger a series of disturbances that would destabilize the entire network (Magee 2010). This kind of mechanistic thinking could be encountered in both HUMINT and Counterintelligence operations. For example, Western intelligence agencies have often designed campaigns around leadership decapitation strategies, whereas state-run services, such as the Russian security apparatus, have historically planned HUMINT operations in a mechanistic manner, assuming a direct and predictable relationship between command decisions and operational execution (Anderson 2007).

Eventually, it is important not to underestimate the value of this approach. By interpreting networks as Complicated systems, intelligence personnel can impose analytical order on uncertain and opaque environments. This paradigm has given rise to tools such as link analysis, network mapping, and computational prioritization techniques, which allow practitioners to systematically visualize relational structures, rank stakeholders by relevance, and identify potential vulnerabilities (Strang 2014). Such methods can yield valuable insights and practical advantages, particularly within highly hierarchical organizations such as bureaucracies, traditional militaries, or doctrinally uniform groups. However, when applied to covert or illicit networks, this mechanistic paradigm reveals significant limitations. Human systems are adaptive, creative, and self-directed; they do not operate as inert, rule-bound mechanisms like engines or computers. When a leader is removed, a successor often emerges; when communication channels are disrupted, actors devise new methods of coordination; and when infiltration occurs, relational trust is recalibrated to mitigate future risk. The central risk lies in assuming that meticulous mapping equates to comprehensive control. Overreliance on mechanistic metaphors can foster overconfidence and strategies that fail under the pressures of human adaptability.

## Complex Systems: Adaptive, Emergent, and Resilient

In Complex systems, behavior arises from the often-unpredictable interactions among individual components rather than from the mere sum of those components (Bishop and Silberstein 2019; Gao and Xu 2021). A single act of betrayal, a shift in resource allocation, or even a minor rumor can propagate through the entire network, triggering cascading effects disproportionate to the original cause. Consequently, Complex systems are inherently dynamic, resistant to direct control, and they defy explanation through reductionist frameworks (Taleb 2007; Kamensky 2011; Zuccaro, De Gregorio, and Leone 2018).

Human networks exemplify these complex dynamics. Unlike fixed hierarchies, such networks are in constant flux, adapting to external pressures such as surveillance, infiltration, and disruption. Leadership within them is seldom stable; authority often shifts in response to situational demands. When crises arise, a charismatic individual may emerge to unify the group, whereas during periods of stability, leadership may devolve to those with specialized expertise (Taleb 2016). Moreover, clandestine networks often fragment under threat, yet these fragments rarely vanish. Instead, they reorganize into new configurations, enhancing their resilience and redundancy (Kanellopoulos 2024a, 2024b). This behavior mirrors that of ecological systems, where disruption does not necessarily precipitate collapse but can instead drive adaptation and renewal (Gharajedaghi 2011; Arthur 2023).

Moreover, feedback loops further intensify these dynamics. In clandestine environments, information flows, whether accurate or deliberately deceptive, have recursive effects on the system. A mere rumor of betrayal can fracture alliances, while shared successes can reinforce trust and solidarity. Conversely, failed operations or poorly calibrated intelligence interventions may be interpreted as signs of external hostility, thereby strengthening group cohesion rather than weakening it. Such recursive processes alter network trajectories in ways that render linear prediction impossible, producing conditions where small perturbations can yield disproportionate and unforeseen outcomes (Clark 2025). Thus, the expansion of cyberspace has compounded the complexity of HUMINT environments. Intelligence activities now unfold within nonlinear and self-adaptive digital ecosystems marked by high degrees of resilience and fluidity (Gilad 2021; Alberti and Belfanti 2023; Broeders 2024). Encrypted communication channels, platform migration, and transnational online communities create dynamic conditions in which disruption is rarely permanent. The integration of artificial intelligence adds another layer of complexity, enabling adversaries to devise novel methods of communication, recruitment, and surveillance, while simultaneously transforming how intelligence is collected, processed, and analyzed (Moran, Burton, and Christou 2023).

## HUMINT in the Social Network Arena

HUMINT is inherently relational, embedded within networks of trust, loyalty, obligation, and manipulation that shape the behavior of both individuals and collectives. Every act of recruitment, infiltration, or influence takes place within networks that are not static but continuously evolve in response to external pressures and internal dynamics. Unlike technical intelligence disciplines that rely on discrete data points, HUMINT depends on the fluid and adaptive structure of human relationships (Barnea 2019).

In contemporary practice, HUMINT officers must operate across both physical and digital domains, each characterized by distinct complexities and constraints. Physical networks, such as those comprising tribal elders, insurgent cells, or organized crime groups, are often rooted in kinship, cultural codes of honor, and enduring historical ties (Kanellopoulos 2023). Recruitment within these contexts cannot be understood as an isolated individual transaction; rather, the defection or cooperation of a single actor reverberates through broader relational structures, influencing patterns of trust, suspicion, and cohesion. A compromised individual may provoke resistance, trigger retaliation, or activate mechanisms of social sanction at the familial or communal level (Serscikov 2024). Historical examples underscore the resilience of such systems. The foreign intelligence service of the German Democratic Republic, for instance, demonstrated how HUMINT architectures grounded in relational networks could sustain operational capacity under continuous external pressure, highlighting the adaptability inherent in socially embedded intelligence frameworks (Kanellopoulos 2025; Maddrell 2025).

Subsequently, cultural dynamics further complicate HUMINT operations. In paternalistic or gender-stratified societies, the participation of female intelligence professionals has proven essential for accessing networks that would otherwise remain closed to male operatives, thereby broadening the range of actionable opportunities and deepening the sophistication of engagement (Lau and Bauer 2022). These dynamics underscore that the effectiveness of HUMINT is inseparable from its cultural context, co-produced by the prevailing norms, hierarchies, and symbolic structures of the operational environment. In addition, the rise of the digital realm amplifies these challenges by introducing additional layers of fluidity and redundancy. Online extremist forums, encrypted communication platforms, and transnational communities linked through diasporas exhibit remarkable resilience, rapidly reconstituting after disruption by migrating to alternative or more secure digital spaces (Broeders 2024). For HUMINT practitioners, effective digital operations require the cultivation of credible virtual identities, sustained immersion in closed online networks, and continuous monitoring of evolving narratives and allegiances. The convergence of online and offline identities further demands adaptive strategies capable of functioning within hybrid spaces, where

digital discourse, physical action, and interpersonal trust intersect and mutually reinforce one another.

## Applying Complexity Thinking to HUMINT

To effectively apply complexity thinking in HUMINT, it is crucial to move beyond linear and reductionist approaches and adopt frameworks that account for the unpredictable, adaptive, and emergent properties of human networks. Traditional paradigms often suggest that covert organizations can be dismantled by targeting key individuals or disrupting communication nodes, based on a mechanistic view of causality. Complexity thinking challenges this assumption by emphasizing four interrelated dynamic processes: emergence, adaptation, resilience, and feedback loops, which collectively illuminate the behavior of networks under stress and intervention.

**Emergence** emphasizes the unpredictable appearance of new structures, leaders, or tactical innovations within clandestine settings. Leadership vacuums rarely persist; instead, they often give rise to unexpected leaders whose legitimacy derives not from formal hierarchy, but from charisma, ideological commitment, or control over exclusive resources (Carnabuci, Emery, and Brinberg 2018; Clark 2025). For HUMINT professionals, this necessitates an analytical approach that goes beyond traditional command structures, seeking out cultural, symbolic, or relational indicators that may signal the consolidation of new authority (Coulson 2025).

**Adaptation** highlights the learning capacity of illicit networks. Operational setbacks, such as failed infiltrations, disrupted nodes, or exposed recruitment pipelines, rarely bring activity to a halt. Rather, they prompt the network to adopt countermeasures designed to mitigate future vulnerabilities (Catanese, et al. 2016; Bright, Koskinen, and Malm 2018). These may include more stringent vetting processes, the implementation of encrypted communication tools, or the redistribution of trust and authority within the network. Every HUMINT intervention thus produces second-order effects, reshaping the adversary's risk calculus and influencing its future actions (Stottlemyre 2024).

**Resilience** refers to the ability of networks to reorganize and persist in the face of significant disruption (Holling 1973). After decapitation strikes, terrorist groups often fragment into smaller cells, which later recombine in new configurations, typically increasing their agility and reducing their detectability. Similarly, criminal organizations displaced by law enforcement frequently relocate across borders, using diasporic ties to maintain illicit operations (Duxbury and Haynie 2019; Cavallaro, et al. 2020). For HUMINT officers, this necessitates continuous monitoring, as disruption tends to redistribute, rather than eliminate, adversarial capabilities.

**Feedback loops** capture the recursive and sometimes paradoxical effects of HUMINT interventions. Information, whether disinformation, selective leaks, or rumors, does not spread linearly within a network; it interacts with preexisting rivalries, suspicions, and narratives. A campaign designed to fragment a group might unintentionally strengthen its cohesion in response to an external threat (Kis 2023). Conversely, a strategically placed rumor may destabilize trust and accelerate internal conflicts. Effective HUMINT requires an acute awareness of second- and third-order effects, with interventions rigorously tested against multiple potential outcomes.

## Practical Implications for Intelligence Practice

Recognizing social networks as Complex, rather than merely Complicated, these systems represent a fundamental shift in how HUMINT is conceptualized and executed. Within this framework, recruitment, disruption, analysis, and training can no longer be treated as discrete, linear tasks; instead, they must be understood as adaptive, iterative processes embedded within dynamic and evolving environments.

**Recruitment** strategies must move beyond the reductionist assumption that individuals can be isolated from their relational context. Every potential source exists within interconnected webs of kinship, ideological alignment, economic dependence, and reputational obligation. Persuading a target to cooperate is not an isolated act of negotiation but an intervention within a broader social matrix (Kanellopoulos 2025). When one person agrees to cooperate, it can trigger ripple effects within family structures, raise suspicions in clandestine groups, or destabilize already fragile trust networks. Effective recruitment, therefore, requires systematic mapping of relational dependencies, anticipation of second- and third-order effects, and, in many cases, the cultivation of tacit acceptance or tolerance from broader kinship or community structures.

**Disruption** strategies also need recalibration. Approaches based on targeting individual nodes—such as the leader of a terrorist cell, the financier of a trafficking network, or the patriarch of a clan—often assume that the removal of a central actor will lead to systemic collapse. In practice, however, such interventions frequently trigger succession processes, producing replacements who may be more radical, adaptive, or operationally competent. HUMINT operations are therefore most effective when integrated into broader, multi-layered strategies, including psychological operations to erode morale, disinformation campaigns to sow doubt and fragmentation, and protracted engagements designed to gradually weaken cohesion. The goal is not a decisive rupture but the continuous shaping of internal dynamics to push networks toward fragmentation, vulnerability, or eventual strategic irrelevance (Sargut and McGrath 2011).

**Analysis** must also shift from static to dynamic assessments. While conventional network charts and link analysis provide useful snapshots of relational ties, they quickly lose relevance in adaptive environments. Complexity thinking necessitates monitoring the flows of trust, influence, and loyalty over time, incorporating iterative assessment cycles that account for shifting allegiances, emergent leaders, and hidden brokers. In this model, HUMINT becomes a recursive feedback system, where each intervention generates data and alters the environment in ways that require constant reassessment.

**Training and doctrine** must institutionalize an understanding of complexity. Intelligence officers need to approach networks through the lenses of nonlinearity, feedback loops, and emergent behaviors, rather than just mechanical outcomes. This requires a pedagogical approach that combines theoretical instruction with scenario-based experiential learning, immersing practitioners in environments where minor interventions produce disproportionate consequences, alliances shift unpredictably, and outcomes defy linear causality (Stacey 2001). Such training fosters agility, resilience, and humility—key attributes for navigating the uncertainty and unpredictability inherent in HUMINT operations within Complex social networks.

## Key Takeaways: Navigating Complexity in HUMINT for Enhanced Efficacy

The distinction between Complicated and Complex systems is not merely semantic; it represents a fundamental conceptual divide with profound and lasting implications for HUMINT practice. When clandestine or illicit networks are viewed through the lens of complication, analysts and practitioners often prioritize structural mapping, the identification of key nodes, and the targeted removal of high-value individuals. These strategies are appealing because they offer analytic clarity, measurable results, and a sense of operational control. However, this mechanistic logic oversimplifies the complexities of human systems. Social networks are not rigid machines made of interchangeable parts; they are dynamic communities shaped by cultural contexts, human relationships, and evolving motivations. While a Complicated systems approach may yield tactical successes—such as the arrest of a leader or the disruption of communication channels—these interventions often fail to create lasting degradation. Instead, networks typically reconstitute, shift allegiances, or, paradoxically, emerge strengthened by disruption.

Complexity-informed approaches require a fundamental rethinking of HUMINT practice. Instead of focusing solely on the static structure of networks, complexity thinking highlights the nonlinear interactions, feedback processes, and emergent behaviors that influence outcomes. This approach demands an interpretive mindset, sensitive to cultural cues, adaptive behaviors, and recursive effects

that cannot be captured by static diagrams or linear models of causality. From this perspective, HUMINT practitioners must recognize that outcomes arise probabilistically, not with certainty. For example, the removal of a node might lead to fragmentation in one case, but catalyze consolidation in another. Similarly, disinformation may undermine trust among adversaries or, conversely, strengthen solidarity in response to an external threat. Complexity thinking equips intelligence professionals to anticipate diverse outcomes, introduce flexibility into planning, and view interventions as ongoing engagements rather than one-time actions.

Moreover, complexity thinking underscores the temporal dimension of these systems. Effects are rarely immediate; they unfold over extended time frames, requiring continuous observation, adaptive recalibration, and a tolerance for uncertainty. HUMINT officers must, therefore, evolve from roles as mere collectors or disruptors to positions of cultural interpreters and relational brokers, adept at detecting subtle shifts in trust, sentiment, and morale that signal potential structural changes. In the modern operational landscape—where adversaries increasingly exploit decentralized digital platforms, hybrid organizational forms, and transnational networks—linear methods of analysis and intervention are insufficient. HUMINT's success depends on embracing complexity as a core principle, fostering adaptability, resilience, and humility in navigating uncertainty. Ultimately, the future of HUMINT lies not in treating networks as puzzles to be solved definitively, but as living systems to be understood, influenced, and carefully navigated. By adopting complexity-informed tools such as network theory, systems thinking, scenario modeling, and adaptive feedback, intelligence agencies can remain responsive to the unpredictable realities of modern conflict and security competition.

## References

**Alberti, Fabio G., and Fabio Belfanti.** 2023. "Complexity and Resilience in Entrepreneurial Ecosystems." *Journal of Innovation and Entrepreneurship* 12 (1): 1–16. https://doi.org/10.1186/s13731-023-00345-5.

**Anderson, John.** 2007. "The HUMINT Offensive from Putin's Chekist State." *International Journal of Intelligence and CounterIntelligence* 20 (1): 1–21. https://doi.org/10.1080/08850600601079958.

**Barnea, Avner.** 2019. "Big Data and Counterintelligence in Western Countries." *International Journal of Intelligence and CounterIntelligence* 32 (3): 433–447. https://doi.org/10.1080/08850607.2019.1605804.

**Bishop, Robert, and Michael Silberstein.** 2019. "Complexity and Feedback." *Routledge EBooks*, 145–156. https://doi.org/10.4324/9781315675213-12.

**Bright, David, Johan Koskinen, and Aili Malm.** 2018. "Illicit Network Dynamics: The Formation and Evolution of a Drug Trafficking Network." *Journal of Quantitative Criminology* 35 (2): 237–258. https://doi.org/10.1007/s10940-018-9379-8.

**Broeders, Dennis.** 2024. "Cyber Intelligence and International Security." *Intelligence and National Security* 39 (7): 1213–29. https://doi.org/10.1080/02684527.2024.2398077.

**Carnabuci, Gianluca, Christopher Emery, and David Brinberg.** 2018. "Emergent Leadership Structures in Informal Groups: A Dynamic, Cognitively Informed Network Model." *Organization Science* 29 (1): 118–133. https://doi.org/10.1287/orsc.2017.1171.

**Cavallaro, Luigi, Alessandro Ficara, Pasquale De Meo, Giuseppe Fiumara, Salvatore Catanese, Ovidiu Bagdasar, Wei Song, and Antonio Liotta.** 2020. "Disrupting Resilient Criminal Networks through Data Analysis: The Case of Sicilian Mafia." *PLOS ONE* 15 (8). https://doi.org/10.1371/journal.pone.0236476.

**Clark, C.R.** 2025. *Modeling and Analysis of Clandestine Networks.* Hutson Street Press.

**Clark, R.M.** 2014. *Intelligence Collection.* Sage.

**Coulson, S.** 2025. "Tactical Indicators and Warnings from Strategic Human Intelligence." *International Journal of Intelligence and CounterIntelligence.* https://doi.org/10.1080/08850607.2025.2504000.

**Gao, Jian, and Bin Xu.** 2021. "Complex Systems, Emergence, and Multiscale Analysis: A Tutorial and Brief Survey." *Applied Sciences* 11 (12): 5736. https://doi.org/10.3390/app11125736.

**Gilad, Amos.** 2021. "Intelligence, Cyberspace, and National Security." *Intelligence and National Security.* https://doi.org/10.1080/10242694.2020.1778966.

**Holling, C.S.** 1973. "Resilience and Stability of Ecological Systems." *Annual Review of Ecology and Systematics* 4 (1): 1–23. https://pure.iiasa.ac.at/id/eprint/26/1/RP-73-003.pdf.

**Huang, P.M., A.G. Darrin, and A.A. Knuth.** 2012. "Agile Hardware and Software System Engineering for Innovation." *2012 IEEE Aerospace Conference.* https://doi.org/10.1109/aero.2012.6187425.

**Kamensky, John M.** 2011. "Managing the Complicated vs. the Complex." *The Business of Government.* https://www.businessofgovernment.org/sites/default/files/JohnKamensky.pdf.

**Kanellopoulos, A.N.** 2023. "The Dimensions of Counterintelligence and Their Role in National Security." *Journal of European and American Intelligence Studies* 6 (2): 85–104.

**___.** 2024a. "Insider Threat Mitigation through Human Intelligence and Counterintelligence: A Case Study in the Shipping Industry." *Defense and Security Studies* 5 (1): 10–19. https://doi.org/10.37868/dss.v5.id261.

**___.** 2024b. "Counterintelligence Risks in Crew Management and Recruitment: The Role of Profiling and Screening in Shipping Companies." *Bulletin of Carol I National Defence University* 13 (2): 44–59. https://doi.org/10.53477/2284-9378-24-19.

**___.** 2025. "Shielding Against Social Engineering Threats: A Counterintelligence Approach." *Bulletin of "Carol I" National Defence University* 14(3): 245-259. https://doi.org/10.53477/2284-9378-25-46.

**Kis, Andrei.** 2023. "A Projection of the Cognitive Warfare in Human Intelligence." *Proceedings of the International Scientific Conference Strategies XXI.* Volume XIX, 130-141. Carol I National Defence University Publishing House. https://www.ceeol.com/search/chapter-detail?id=1244819.

**Kravtsov, Yury A., and Joseph B. Kadtke.** 1996. "Predictability of Complex Dynamical Systems." In *Springer Series in Synergetics* vol. 69. Springer Nature. https://doi.org/10.1007/978-3-642-80254-6.

**Lahneman, William J.** 2010. "The Need for a New Intelligence Paradigm." *International Journal of Intelligence and CounterIntelligence* 23 (2): 201–225. https://doi.org/10.1080/08850600903565589.

**Lau, Sophie, and Franz T. S. Bauer.** 2022. "What About Her? Increasing the Actionability of HUMINT in Paternalistic Cultures by Considering Female Intelligence." *International Journal of Intelligence and CounterIntelligence:* 35 (4): 726–43. https://doi.org/10.1080/08850607.2022.2068890.

**Maddrell, Paul.** 2025. "The Triumph of HUMINT: The GDR Foreign Intelligence Services' Collection of Defense Intelligence, 1951–1989." *International Journal of Intelligence and CounterIntelligence* 38 (1): 48–71. https://doi.org/10.1080/08850607.2024.2340955.

**Magee, A.C.** 2010. "Countering Nontraditional HUMINT Collection Threats." *International Journal of Intelligence and CounterIntelligence* 23 (3): 509–520. https://doi.org/10.1080/08850601003798807.

**Menkveld, C.** 2021. "Understanding the Complexity of Intelligence Problems." *Intelligence and National Security* 36 (5): 621–41. https://doi.org/10.1080/02684527.2021.1881865.

**Miller, Seumas.** 2022. "National Security Intelligence Activity: A Philosophical Analysis." *Intelligence and National Security* 37(6): 791–808. https://doi.org/10.1080/02684527.2022.2076329.

**Moran, Chris R., Joe Burton, and George Christou.** 2023. "The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying." *Journal of Global Security Studies* 8 (2). https://doi.org/10.1093/jogss/ogad005.

**Prencipe, Andrea, Andrew Davies, and Michael Hobday.** 2003. *The Business of Systems Integration.* Oxford University Press.

**Sargut, Gökçe, and Rita Gunther McGrath.** 2011. "Embracing Complexity." *Harvard Business Review.* https://hbr.org/2011/09/embracing-complexity.

**Serscikov, George.** 2024. "HUMINT Operations Abroad: Challenges to Japan's Intelligence Capabilities." *International Journal of Intelligence and CounterIntelligence* 37 (2): 482–512. https://doi.org/10.1080/08850607.2023.2214325.

**Sitte, Renate.** 2009. "About the Predictability and Complexity of Complex Systems." In *Understanding Complex Systems,* 23–48. https://doi.org/10.1007/978-3-642-02199-2_2.

**Stacey, Ralph D.** 2001. *Complex Responsive Processes in Organizations: Learning and Knowledge Creation.* Routledge. https://www.sfu.ca/complex-systems-frameworks/frameworks/complex-vs-complicated/stacey-matrix.html.

**Sterelny, Kim.** 2007. "Social Intelligence, Human Intelligence and Niche Construction." *Philosophical Transactions of the Royal Society B: Biological Sciences* 362 (1480): 719–730. https://doi.org/10.1098/rstb.2006.2006.

**Stottlemyre, Steve.** 2024. "Intelligence for Human Security: Measuring Outcomes." *Intelligence and National Security* 39 (1): 93–118. https://doi.org/10.1080/02684527.2023.2250478.

**Taleb, Nassim Nicholas.** 2007. *The Black Swan.* Allen Lane.

**___.** 2016. "Complex Systems Archives." *Nassim Taleb.* https://nassimtaleb.org/tag/complex-systems/.

**Zuccaro, Giulio, Davide De Gregorio, and Maria Francesca Leone.** 2018. "Theoretical Model for Cascading Effects Analyses." *International Journal of Disaster Risk Reduction* 30 (B): 199–215. https://doi.org/10.1016/j.ijdrr.2018.04.019.