



The Evolution of GEOINT-Cyber Integration in Modern Warfare: A Systematic Review of Operational Paradigms, Enabling Technologies, and Implementation Challenges

Ryan Sabian¹, Sukendra Martha², Yosef Prihanto³

¹ Magister student of Remote Sensing Technology at Republic of Indonesia Defense University, Sentul, West Java, Indonesia

^{2,3} Lecturer of Remote Sensing Technology at Republic of Indonesia Defense University, Sentul, West Java, Indonesia

Corresponding Author: ryansbn@gmail.com

Abstract

In an era of converging digital and physical realities, the integration of Geospatial Intelligence (GEOINT) and cyber operations has become a strategic imperative for modern defense. This systematic review examines the evolution of GEOINT-cyber integration from 2016 to 2025, synthesizing operational paradigms, enabling technologies, and implementation challenges. Methodologically, the study adopts a Systematic Literature Review (SLR) following the PRISMA 2020 framework. Data were collected using Publish or Perish (PoP) from Crossref and Google Scholar, with keywords including “cyber warfare” and “GEOINT.” From an initial pool of 216 articles obtained, only 4 articles met the inclusion criteria for the analysis stage. Key findings highlight three pivotal developments: (1) the Internet of Things (IoT) serves as both a distributed GEOINT sensor network and a cyberattack vector; (2) epidemiological models provide an analytical framework for tracking cyber threats across spatial and cognitive domains; and (3) Cognitive Intelligence (COGINT) enables the geospatial mapping and influence of human decision-making. Case studies such as the Ukraine conflict and Operation “Salt Typhoon” illustrate real-world applications while revealing tensions between security efficacy, ethical governance, and human dignity. The study concludes that the future of GEOINT-cyber integration will be shaped not only by technological advances but also by principled frameworks that balance operational effectiveness with societal values. This review offers a structured, human-centric overview of a rapidly evolving domain, contributing to both academic discourse and professional practice.





Keyword: Cognitive Intelligence (COGINT), Cyber Warfare, GEOINT-Cyber Integration, Human-Centric Security, Systematic Literature Review.

INTRODUCTION

Amidst the hustle and bustle of 21st-century digital life, where internet connectivity has become the driving force behind the economy, government, and society, a paradox has emerged. The more connected we are, the more vulnerable we become. For example, Internet of Things (IoT) based agricultural irrigation systems can be optimized through smart devices (Dong et al., 2024). However, at the same time, it is vulnerable to cyberattacks that could disrupt national food security (Ileri, 2025). This example is no longer a fictional scenario, but a real portrait of the contemporary threat landscape, where the boundaries between the physical and digital worlds are becoming increasingly blurred. In this context, Geospatial Intelligence (GEOINT) is not only a supporting instrument (Clarke, 2019), but also a critical bridge connecting the abstract cyber realm with concrete geographical realities.

The development of cyber warfare has fundamentally shifted the paradigm of national security threats (Dawson, 2015, 2018). Whereas in the past, national borders were fortified with walls and troops, today, the front lines of defense are located within servers, undersea fiber optic cables, and globally distributed data centers. Cyber operations, ranging from espionage (Sin & Washburn, 2022) and disinformation to attacks capable of crippling critical infrastructure such as electricity, water, and transportation networks, have become strategic tools for major countries (Ai et al., 2025; Smyth, 2018; Tsetsos, 2025). The biggest challenge is its asymmetrical nature; a small group with limited resources can launch attacks with national impact (Rugge, 2018), while hiding their identity and location behind layers of digital protection. The attribution problem, or the difficulty of conclusively identifying the perpetrators, is a key weapon in this war, creating a safe space for malicious actors to operate. Cyber warfare affects not only national security but also international security, with many countries developing strong cyber capabilities that have the potential to disrupt global stability (Siroli, 2018).

The integration between GEOINT and cyber operations is not merely a technical combination, but rather an operational unity necessary to achieve information superiority in modern conflicts. Without geospatial context, cyber intelligence is like having data without a map: it can detect anomalies, but has difficulty placing them in real space (Stanik & Kiedrowicz, 2025). Conversely, without cyber understanding, GEOINT is only capable of mapping physical structures without understanding the digital vulnerabilities inherent in them (Veerasamy et al., 2022). This integration gap is still apparent in many defense and intelligence organizations, where the two





domains often operate in separate functional silos, whether technically, culturally, or doctrinally.

Although the integration of GEOINT and the cyber domain is increasingly discussed in academic literature and military doctrine, there is still a significant knowledge gap regarding how this evolution has occurred systematically over the past decade (2016-2025). Most studies tend to focus on technical aspects or specific cases, without providing a comprehensive overview that connects the development of operational paradigms (Eslam & Tiwari, 2025), supporting technologies, and implementation challenges faced by state and non-state actors (Shekhawat et al., 2025). In fact, a comprehensive understanding of the dynamics of this integration is crucial not only for defense policymakers, but also for researchers, cybersecurity practitioners, and technology developers who want to contribute to a more resilient defense ecosystem (Okano et al., 2026; Stefanov & Berchev, 2025). Through a literature review and case study analysis, this paper will answer fundamental questions: How does GEOINT strengthen the cyber intelligence cycle, what technologies support this integration, and what challenges hinder optimal synergy between the two domains? By answering these questions, this research is expected to provide academic and practical contributions to the development of cyber defense capabilities that are more integrated, contextual, and responsive to the dynamics of threats in the digital age.

METHOD

This study uses a descriptive qualitative method with a systematic literature review approach (Fundoni et al., 2023; García-Peñalvo, 2022). This method was chosen to identify, analyze, and synthesize conceptual developments, technical implementations, and integration challenges between geospatial intelligence (GEOINT) and cyber warfare in the context of modern warfare during the period 2016-2025. The research data was sourced from a collection of secondary literature obtained through a systematic search using the Publish or Perish (PoP) application with the keywords "cyber warfare" and "GEOINT" or "geospatial intelligence" and "cyber operations". The search was limited to publications from 2016 to 2025. The search results yielded 216 documents consisting of journal articles, conference proceedings, books, technical reports, and strategic publications from government institutions and related research institutions.



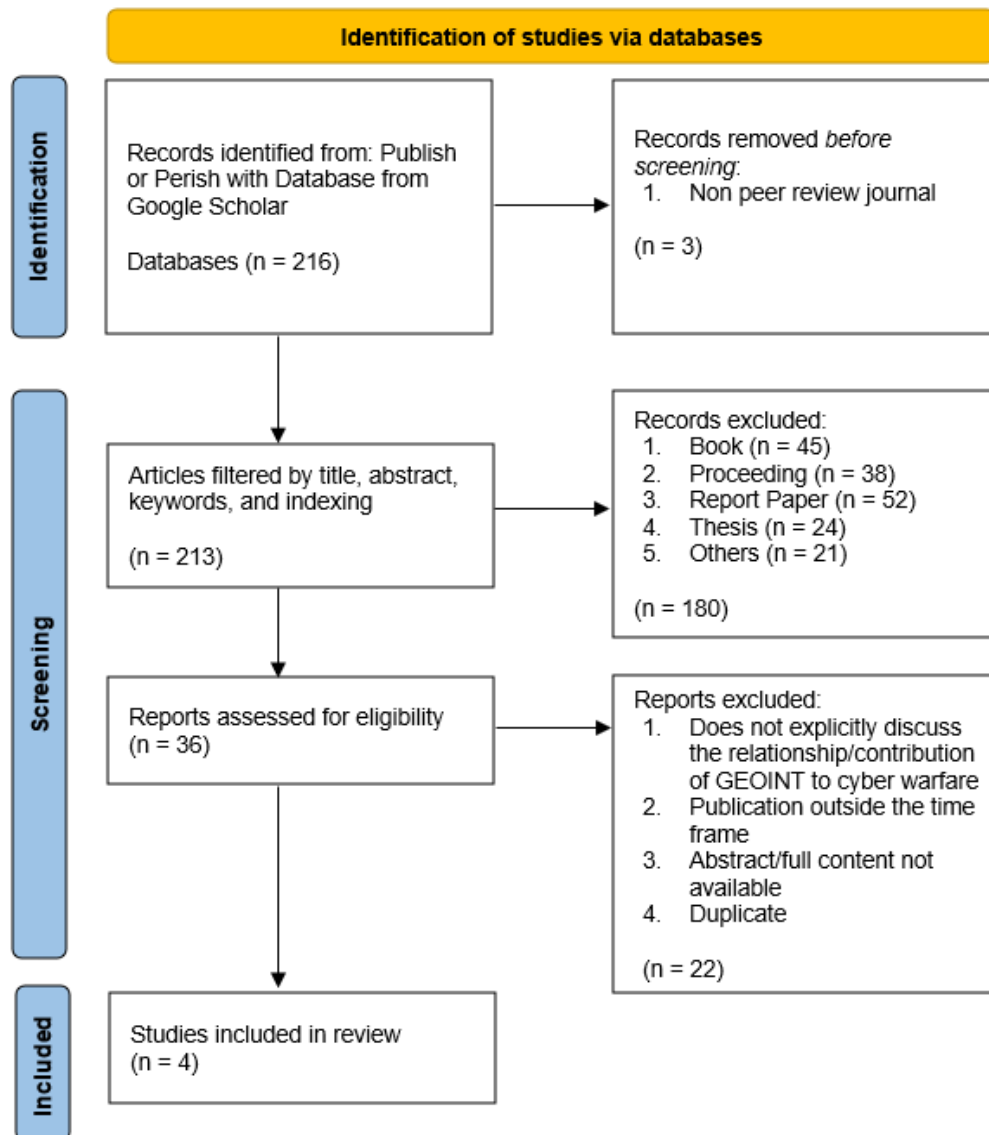


Figure 1. Prism flow diagram
Processed: by researcher, 2026

RESULTS AND DISCUSSION

1. IoT as Geoint Sensors and Cyber Vectors in Modern Warfare: Comparative Analysis and Convergence

The development of integration between GEOINT (Geospatial Intelligence) and the cyber domain is currently greatly influenced by the emergence of the Internet of Things (IoT). Devices such as smart cameras, industrial sensors, or digital assistants at home, which were originally

designed for convenience, turn out to have a dual purpose. On the one hand, they form a very extensive geolocation sensor network, capable of collecting real-time data in areas that are difficult for satellites to reach. On the other hand, as Caton (2020) points out, these devices are vulnerable to exploitation, turning them into tools for intelligence, surveillance, and reconnaissance (ISR) as well as gateways for cyberattacks. Simple vulnerabilities, such as users forgetting to change default passwords, can create systemic loopholes for national security. The issue becomes even more complex because the root of the problem lies not only in technology but also in governance. Bilgin's (2025) analysis shifts the focus from the technical vulnerability of individual devices to the failure of digital ecosystem management as a whole. Pioneering countries such as Estonia are beginning to realize that securing the cyber world means regulating billions of interconnected devices. In the context of cyber GEOINT, this approach requires intelligent intelligence filtering mechanisms that not only detect compromised devices but also map threats in a geospatial context.

This is where Brantly's (2015) legal-operational framework provides clarity. With his epidemiological model, Brantly helps distinguish between cyber espionage and cyber attacks. The difference is often subtle, especially when IoT devices are used to map locations or monitor activities. According to Brantly, the answer depends on the intent and consequences, which can be measured by the extent of the infection (prevalence) and the level of damage caused (case fatality rate). The Mirai botnet attack in 2016, which crippled internet services by exploiting IoT devices, clearly falls into the attack category because it disrupted service availability.

Furthermore, this convergence is beginning to touch on a more personal realm. Conde and Whiskeyman (2025) remind us that IoT not only observes the environment around us, but also begins to understand the thoughts and habits of its users. Virtual assistants that listen to conversations, watches that monitor heart rates, or social media such as TikTok that records our location and content preferences are all GEOINT sensors that simultaneously compile individual cognitive profiles. This is the highest form of convergence: when geospatial data collection meets mind mapping, creating tools that not only observe but also have the potential to influence.

Table 1. Comparison of Journal Perspectives on IoT in GEOINT-Cyber Integration

Analysis Aspects	Caton's Perspective (2020)	Bilgin's Perspective (2025)	Brantly's Perspective (2015)	Conde & Whiskeyman's Perspective (2025)
Status IoT	ISR platform & two-way attack vector	Components in the digital ecosystem that need to be regulated	Objects in the continuum from espionage to attack	Integrated geospatial & cognitive data

				sensors
Risk Focus	Technical vulnerabilities of devices (default passwords, zero-day)	Systemic vulnerabilities (interdependencies, misinformation)	Legal ambiguity and intent in an action	Cognitive manipulation & erosion of thinking sovereignty
Solution/Framework	IoT security regulations, routine patching	Ecosystem management, digital twins, filtering intelligence	Epidemiological models for attribution and legal response	Protection of cognitive sovereignty, COGINT ethics
Operational Examples	Mirai botnet (DDoS attack via IoT)	Digital twins for simulating attacks on critical infrastructure	The "Weeping Angel" case (exploitation of smart TVs for surveillance)	Psychographic profiling based on location and behavior data
Implications for GEOINT	1. Spatial mapping of IoT vulnerabilities 2. Real-time data from sensors	1. Integration of IoT data into the common operational picture 2. Geospatial impact simulation	1. Legal parameters and location 2. Threat classification	1. Geo-psychographic mapping 2. Targeted influence operations

Processed: by researcher, 2026

2. Epidemiological Model for Integrated Cyber-Geoint Threat Analysis: Classification Framework and Operational Response

Amidst the classic challenge of distinguishing cyber espionage from cyber attacks, a problem he refers to as deceptive appearance, Brantly (2015) offers an unconventional breakthrough. He uses an epidemiological model from public health science. This framework changes the way cyber incidents are viewed by applying four key parameters: incidence rate, prevalence, case fatality rate, and malware reproduction number (R_0). Through this lens, cyber outbreaks can be mapped spatially and temporally like disease outbreaks, helping to identify patient zero and predict patterns of spread based on networks and locations. For example, malware with $R_0 > 1$, which consistently appears in critical infrastructure in certain regions, may indicate a coordinated attack, requiring a response integrated with geospatial threat maps. In essence, Brantly argues that this parameter-based analysis can distinguish between espionage,



attacks, and ordinary crimes more objectively, resulting in a more proportional and targeted response.

If Brantly's model is a theory, then the case raised by Caton (2020) is empirical evidence. The Mirai botnet outbreak in 2016 is a perfect example to be autopsied with epidemiological analysis tools. Through this lens, Mirai shows a high R_0 with explosive spread to vulnerable IoT devices, very wide prevalence (hundreds of thousands of devices globally), but a relatively low case fatality rate when measured by permanent physical damage. The main effect was massive service disruption (DDoS), not destruction. This analysis confirms Brantly's core thesis: scale and impact (effect) should be the determining factors for classification. Furthermore, Caton's finding that 15% of IoT devices still use default passwords provides another critical parameter in the epidemiological model: the susceptible population. This data reveals a reservoir of vulnerabilities ready to be exploited to trigger the next mass cyber outbreak.

Bilgin's (2025) perspective elevates the discussion from the technical level to governance architecture. In a digital ecosystem saturated with information overload, he introduces the concept of intelligence filtering as a critical capability. This concept synergizes with the prevalence and incidence rate parameters in Brantly's model. An effective filtering system must be able to identify true threat signals from massive data noise. This is where the digital twins technology advocated by Bilgin finds its relevance. This technology can function as a virtual cyber epidemiology laboratory, where malware spread and policy response effectiveness can be simulated in various geospatial scenarios before being implemented in the real world. Therefore, Bilgin's approach not only diagnoses the "disease" but also builds an "immune system" and prevention protocols for the entire ecosystem. At the deepest and most personal level, Conde and Whiskeyman (2025) apply the same epidemiological logic to a completely new domain: human cognition. They identify how narratives, disinformation, and influence can spread through populations like pathogens, with similar parameters: cognitive R_0 (the transmissibility of a narrative), cognitive prevalence (the spread of a belief), and cognitive fatality (the degree of damage to healthy thinking). In this model, platforms such as social media act as the primary vectors of cognitive transmission, where algorithms designed for engagement actually accelerate the spread of emotionally charged "content-viruses," often disregarding the truth. This concept forms the theoretical basis for understanding cognitive warfare, where the ultimate goal is not to infect systems, but to "infect" the decision-making processes of opponents and civil society with narratives that undermine the sovereignty of thought.



Table 2. Application of Brantly's Epidemiological Model (2015) to Three Contemporary Domains

Parameter Epidemiologi (Brantly, 2015)	Applications in IoT Vulnerabilities (Based on Caton, 2020)	Applications in Digital Ecosystem Governance (Based on Bilgin, 2025)	Applications in Cognitive Warfare (Based on Conde & Whiskeyman, 2025)
Incidence Rate (New infection rate)	The speed of exploitation of new vulnerabilities, such as the use of default passwords on 15% of IoT devices or zero-day exploitation on certain devices.	The volume and frequency of new threats detected in the national digital ecosystem, such as data poisoning attacks against AI training data sets.	The viral speed of a disinformation narrative or deepfake on social media platforms, measuring how quickly the "infection" of ideas spreads.
Prevalence (Proportion of infected systems)	The absolute number of compromised devices (e.g., 600,000+ devices in the Mirai botnet).	The percentage of critical infrastructure in an ecosystem that has been compromised or is at risk.	Percentage of the target population that has adopted or believes a false narrative or foreign influence agenda.
Case Fatality Rate (System "mortality" rate / Fatal impact)	The level of damage caused. In a Mirai DDoS attack, the impact is disruption to service availability. In a compromise of SCADA/OT systems, the impact can be physical damage or loss of process integrity.	Severity of consequences of violations. Example: Data corruption in digital twins can lead to simulation failures and wrong strategic decisions. Ransomware attacks can paralyze essential services.	The degree of damage to cognitive or social processes. Example: Belief in false narratives can cause damage to democratic norms or political/strategic decision-making that is detrimental to sovereignty.
Reproductive Number (R_0) (Reproduction)	The ability of malware (such as Mirai) to autonomously spread	The potential for a vulnerability or attack to cause cascading	The intrinsic contagiousness of a narrative or

Number / Spread Rate)	to new vulnerable devices within an IoT network creates a botnet explosion effect.	failures throughout interconnected ecosystems.	manipulation technique, amplified by social media algorithms and echo chambers, determines its potential to become a cognitive epidemic.
------------------------------	--	--	--

Processed: by researcher, 2026

These four perspectives form a coherent analytical continuum, ranging from cyber outbreaks at the technical level to epidemics in the cognitive realm. The epidemiological model introduced by Brantly (2015) serves as a flexible unifying framework, capable of being translated into various layers of GEOINT-cyber integration:

- 1) **Technical Layer (Caton):** This model is used to analyze the dynamics of malware spread in IoT networks, with parameters such as R_0 (reproduction number) and prevalence (proportion infected) helping to predict the scale and speed of infection.
- 2) **Systemic Layer (Bilgin):** At this level, the model is applied to map vulnerabilities in complex digital ecosystems. Concepts such as incidence rate (rate of new infections) and intelligence filtering are key to identifying systemic threats before they spread.
- 3) **Cognitive Layer (Conde & Whiskeyman):** The same framework is applied to track the spread of narratives and disinformation. Metrics such as cognitive R_0 and cognitive prevalence measure the spread and adoption rate of an information "pathogen" within a population.

In the context of integrated multidomain military operations, the application of this model enables a more holistic threat analysis. A cyberattack on GEOINT infrastructure, such as GPS signal spoofing, is no longer viewed as an isolated technical incident. Rather, it can be understood as part of a broader outbreak, with patterns of spread, points of origin, and cascading effects that can be mapped geospatially and temporally. The conflict in Ukraine, for example, provides a real-world illustration: cyber epidemiological analysis was used to track the spread of malware targeting energy infrastructure, while cognitive epidemiological analysis was applied to map the dynamics of propaganda in occupied territories.

Despite its strength, the epidemiological model has limitations in dealing with highly targeted cyber attacks (such as Stuxnet) that have a low incidence but high case fatality in specific

targets. Furthermore, the application of these models to the cognitive domain raises ethical questions about the measurement of and response to cognitive infections in civilian populations. Future research needs to develop hybrid models that integrate technical, systemic, and cognitive epidemiological parameters into a comprehensive cyber-GEOINT framework, with particular attention to privacy, ethics, and international humanitarian law.

3. The Role of Cognitive Intelligence (COGINT) and Cognitive Warfare in the Integrated Geospatial-Cyber Landscape

Conde and Whiskeyman (2025) introduce Cognitive Intelligence (COGINT) as a revolutionary intelligence discipline that systematically maps, protects, and exploits human decision-making architecture in contemporary conflicts. They argue that while the physical and cyber domains remain critical, cognitive dominance has become a strategic determinant in fifth-generation warfare (5GW). COGINT leverages the convergence of neuroscience, artificial intelligence (AI), and the proliferation of personal devices to build individual and group cognitive blueprints mapping biases, heuristics, emotional vulnerabilities, and decision-making patterns on a previously impossible scale (Conde & Whiskeyman, 2025). Key technologies such as Stealth Autonomous Brain Reconnaissance Hacking (SABRH) and Machine Neurobehavioral Engineering (MNE) enable precision-targeted influence operations based on psychographic profiles supplemented with location data, effectively unifying the GEOINT and cognitive domains within a single operational framework.

Bilgin (2025) provides the context of digital ecosystem governance that is essential for understanding COGINT implementation. His concept of digital twins can be expanded to include not only replicas of physical infrastructure but also cognitive models of target populations. Cognitive digital twins will enable simulations of how specific narratives spread across different demographic groups based on geographic location, media access, and psychological preconditions. Furthermore, Bilgin's intelligence filtering framework becomes particularly relevant in the context of COGINT, where the challenge is not a lack of data but an excess of behavioral and cognitive data that must be filtered for actionable insights. Platforms such as social media generate enormous volumes of cognitive "exhaust data" likes, shares, viewing times, search patterns which require sophisticated filtering algorithms to identify intelligence signals from noise (Bilgin, 2025).

Caton (2020) provides the technical foundation explaining how IoT devices collect data that serves as the raw material for COGINT. Surveillance cameras with facial analytics, smart speakers that analyze voice tones, and wearable devices that track physiological responses are all

distributed cognitive-geospatial sensors that collect data not only about the physical environment but also about the cognitive and emotional states of users. Data from these IoT devices, when collected at scale and analyzed with AI, can reveal patterns such as collective stress levels in a given area, political preferences correlated with geographic location, or vulnerability to certain types of messages based on environmental context. The CIA's "Weeping Angel" exploitation of Samsung smart TVs, revealed by Caton, is an early example of how consumer devices can be hijacked for cognitive-visual data collection, combining geospatial surveillance with behavioral analysis (Caton, 2020).

Brantly (2015) provides an important legal-operational lens with his classification framework that distinguishes espionage from attack. Based on Brantly's parameters, COGINT operations aimed at mapping the cognitive architecture of a target may be classified as espionage, while operations that use this mapping to actively manipulate decision-making, especially if it causes real harm, would fall closer to the category of attack. The cognitive case fatality rate will measure the extent to which influence operations disrupt normal cognitive function or cause damage to sound decision-making processes.

The convergence of GEOINT, cyber, and COGINT marks a fundamental evolution in the nature of conflict and intelligence. As Conde and Whiskeyman conclude, "Cognitive supremacy, once secured, can constitute a central axis of war exerting influence across all other warfighting domains" (Conde & Whiskeyman). The integration of these three domains is not a future option but a strategic imperative now for nations that wish to maintain superiority in an increasingly complex and multidimensional security landscape.

4. Geoint-Cyber Integration Case Study (2016-2025): Narrative of Operational Convergence

4.1. Ukraine Conflict: Collaborative Intelligence Ecosystem

This conflict realized Bilgin's (2025) prediction about digital ecosystem governance under pressure. Ukrainian civilians with smartphones and commercial drones transformed into a distributed GEOINT sensor network, blurring the lines between military actors and civilians. However, as Caton (2020) anticipated, IoT vulnerabilities became a weak point when this sensor infrastructure was targeted by cyber attacks. On the cognitive dimension, the battle for the narrative of truth through social media creates a psychological reality that is often more decisive than the facts on the ground, confirming Conde & Whiskeyman's (2025) thesis on cognitive warfare as the primary operational domain.

4. 2. Operation "Salt Typhoon": Espionage on a Humanitarian Scale

This operation, linked to Chinese intelligence, reveals the paradox of contemporary digital security: technology designed for human connectivity becomes a tool for mass surveillance. The personal data of billions of individuals, their locations, communications, preferences is collected to build psychographic-geospatial maps that enable personalized influence. This case is not only about technical system breaches, but about the erosion of privacy as a fundamental human right in an interconnected digital ecosystem. As Bilgin (2025) reminds us, the absence of a global governance framework leaves individuals vulnerable in a borderless landscape that should empower them.

4. 3. Maritime Disputes: Sovereignty in the Blue Domain

In the South China Sea, integrated underwater sensors, satellites, and drones create a continuous maritime domain awareness system, but at the same time, it becomes a field of cyber contestation. Here, GEOINT-cyber integration is not only about data collection but also about shaping contested narratives of sovereignty. As in the analysis by Conde & Whiskeyman (2025), historical claims built through information operations become strategic weapons, transforming international waters into a claimed psychological space.

Table 5. The Human Dimension in GEOINT-Cyber Integration

Case Study	Impact on Individuals	Impact on the Community	Ethical Dilemma	Humanitarian Implications
Ukraina	Citizens become unprotected sensors	Digital solidarity vs. collective vulnerability	The obligation to protect civilian actors	Privacy vs. national survival
"Salt Typhoon"	Personal data as an intelligence commodity	Group profile for target influence	Consent in mass data collection	Individual autonomy in a monitored ecosystem
Maritime Dispute	Fishermen as subjects of supervision	Coastal communities in geopolitical narratives	Access to resources vs. national security	Traditional rights vs. modern digital claims

Processed: by researcher, 2026

4. 4. The Human Narrative in Technology

Behind the sensors, algorithms, and command-and-control systems, the integration of GEOINT and cyber ultimately touches on universal human experiences: the need for security, the desire for privacy, and the right to self-determination. The Ukraine conflict teaches us that community resilience can be a stronger strategic asset than cutting-edge technology. The "Salt Typhoon" case warns us that personal data is not just a point in a database, but a digital trace of human identity that deserves protection. Maritime disputes remind us that behind claims of sovereignty are communities whose livelihoods and cultures are connected to the sea.

The integration of GEOINT-cyber between 2016-2025 is not merely a technological development, but a shift in the relationship between humans, technology, and security. As articulated in the four journals, the future will be determined not only by who has the most sophisticated systems, but by who can balance technological superiority with the protection of human dignity in an increasingly complex digital ecosystem. The success of integration will be measured not only in operational excellence, but in its ability to protect rather than sacrifice the human values that form the foundation of the society it seeks to protect.

5. Challenges and Recommendations for Geoint-Cyber Integration: Building an Effective and Principled Operational Framework

One of the main challenges is the fundamental tension between national security needs and the protection of civil rights. Effective intelligence filtering systems, as described by Bilgin (2025), often conflict with the principles of transparency and democratic accountability. At the technical level, Caton's (2020) predictions about the vulnerability of IoT devices have proven accurate, but an excessive regulatory response risks limiting innovation and public access to beneficial technologies. These challenges are compounded by the legal ambiguities highlighted by Brantly (2015), where the difficulty of distinguishing between cyber espionage and cyber attacks creates operational uncertainty and increases the risk of conflict escalation. The cognitive dimension identified by Conde and Whiskeyman (2025) adds an additional layer of complexity. Influence operations and cognitive manipulation exist in a poorly mapped legal and ethical gray area, creating new challenges in developing appropriate doctrines and operational procedures.

Based on an in-depth analysis of these four perspectives, this study proposes four areas of policy recommendations that are interrelated and mutually reinforcing.

- 1) First, in the dimension of digital governance, it is necessary to develop mechanisms that are resilient while still respecting fundamental rights. This includes standards for digital twins that protect individual privacy while enabling effective operational simulations.



Intelligence filtering mechanisms need to be designed with an adequate level of transparency to maintain public accountability, recognizing that sustainable national security requires social legitimacy.

- 2) Second, in the technical regulation dimension, IoT security standards need to be developed with consideration for the balance between security and affordability. The principle of "security by design" should be mandatory, accompanied by public education programs on basic digital security practices. This approach recognizes that the protection of national systems begins with securing the individual devices of citizens.
- 3) Third, the development of a clear legal framework is necessary to reduce operational ambiguity. Independently verifiable attribution protocols will increase certainty in responding to cyber incidents. Proportional response guidelines, based on parameters such as the scale and effect of the incident, can help prevent unnecessary escalation. Legal protection for humanitarian operations also needs to be guaranteed in an increasingly complex cyber conflict environment.
- 4) Fourth, the operational ethics dimension requires special attention. Clear restrictions are needed for operations targeting civilian cognition, with the principle of informed consent in data collection for cognitive profiling. Exceptions to this principle should be strictly limited and closely monitored.

The evaluation of the success of cyber-GEOINT integration should not be limited to technical parameters alone. More holistic metrics are needed that reflect the balance between security and other values important to society. A national digital resilience index, for example, could measure not only technical capabilities but also social resilience and the legal framework protecting digital rights. Regular humanitarian impact audits of security systems and policies could help identify and address unintended consequences before they develop into more serious problems.

The principle of caution needs to be applied in the adoption of new technologies, with careful consideration of long-term implications. Continuous professional education and training are essential to build human capacity that understands not only the technical aspects but also the legal and ethical dimensions of multidomain operations. This approach recognizes that true security is not achieved by sacrificing the values it seeks to protect, but by deeply integrating them into security systems and policies.





CONCLUSION

Based on a review of developments over the past decade (2016–2025), it can be concluded that the integration of Geospatial Intelligence (GEOINT) and the cyber domain has become a critical foundation in addressing modern security threats. This combination forms an operational framework that not only connects the physical and digital worlds, but also enters the cognitive dimension of humans. GEOINT strengthens the cyber intelligence cycle by providing real geographical context to abstract cyber data. The presence of GEOINT transforms a series of logs and codes into actionable spatial narratives, from tracking the origin of attacks to mapping their impact on physical infrastructure. This integration enables a more targeted and location-based response.

The main technologies driving this integration are the Internet of Things (IoT), artificial intelligence (AI), and simulation platforms such as digital twins. IoT devices function as geospatial sensors as well as points of cyber vulnerability. Meanwhile, analytical approaches such as epidemiological models and Cognitive Intelligence (COGINT) enable threat tracking not only technically, but also at the psychological and social levels. The toughest challenges lie outside the technical realm, namely the clash between national security and civil rights, legal ambiguity, and ethical dilemmas in information operations. Experiences from the Ukraine conflict, Operation Salt Typhoon, and maritime disputes show that the success of integration is no longer measured solely by technological sophistication, but by the ability to maintain a balance between defense and the protection of human dignity.

As explained, GEOINT-cyber integration reflects a paradigm shift: superiority in modern warfare will belong to those who are able to harmonize technological capabilities with social resilience, regulatory clarity, and a commitment to human values. The future of national security will be largely determined by our ability to not only master technology, but also keep it centered on humanity.

REFERENCE

- Ai, C., Zaheer, Q., Qiu, S., Atta, Z., Malik, M., Hu, W., & Shah, S. M. A. H. (2025). Cybersecurity in infrastructure management. In *Smart Infrastructure Management*. <https://doi.org/10.1016/B978-0-443-34017-8.00007-7>
- Bilgin, A. (2025). Military Intelligence and Digital Ecosystem Governance SSRN. <https://doi.org/10.2139/ssrn.5423054>
- Brantly, A. F. (2016). Aesop's wolves: the deceptive appearance of espionage and attacks in cyberspace. *Intelligence and National Security*, 31(5), 674–685.



- <https://doi.org/10.1080/02684527.2015.1077620>
- Caton, J. (2020). Dancing on the Razor's Edge: A Foundational Review of IoT Exploitation and Defense through the Lens of TECHINT Collection. *International Journal of Intelligence and CounterIntelligence*, 33(3), 540–555. <https://doi.org/10.1080/08850607.2020.1720007>
- Clarke, K. C. (2019). Geospatial Intelligence. In *International Encyclopedia of Human Geography Second Edition*. <https://doi.org/10.1016/B978-0-08-102295-5.10550-5>
- Conde, J., & Whiskeyman, A. (2025). The Emergence of Cognitive Intelligence (COGINT) as a New Military Intelligence Collection Discipline. *International Journal of Intelligence and CounterIntelligence*, 1–27. <https://doi.org/10.1080/08850607.2025.2571497>
- Dawson, M. (2015). A brief review of new threats and countermeasures in digital crime and cyber terrorism. In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*. <https://doi.org/10.4018/978-1-4666-8345-7.ch001>
- Dawson, M. (2018). A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism. In *Cyber Security and Threats* (pp. 173–180). IGI Global. <https://doi.org/10.4018/978-1-5225-5634-3.ch010>
- Dong, Y., Werling, B., Cao, Z., & Li, G. (2024). Implementation of an in-field IoT system for precision irrigation management. *Frontiers in Water*, 6. <https://doi.org/10.3389/frwa.2024.1353597>
- Eslam, H., & Tiwari, G. (2025). Cyberspace: Reimagining Cybersecurity and Its Impact on State Sovereignty. In *Studies in Computational Intelligence* (Vol. 1181). https://doi.org/10.1007/978-3-031-80557-8_4
- Fundoni, M., Porcu, L., & Melis, G. (2023). Systematic literature review: Main procedures and guidelines for interpreting the results. In *Researching and Analysing Business Research Methods in Practice*. <https://doi.org/10.4324/9781003107774-5>
- García-Peñalvo, F. J. (2022). Developing robust state-of-the-art reports: Systematic Literature Reviews | Desarrollo de estados de la cuestión robustos: Revisiones Sistemáticas de Literatura. *Education in the Knowledge Society*, 23, E28600. <https://doi.org/10.14201/eks.28600>
- Ileri, K. (2025). IoT-Based Smart Farming: Benefits, Attacks, and Security Solutions. *Ichora 2025 2025 7th International Congress on Human Computer Interaction Optimization and Robotic Applications Proceedings*. <https://doi.org/10.1109/ICHORA65333.2025.11017038>
- Okano, M. T., Lopes, W. A. C., Fong, C. K., Fernandes, J. C. L., & Ruggero, S. M. (2026). Technological Convergence of Operational Technology (OT) and Information Technology (IT) in the Digital Industry: Conceptual Analysis of OT, Highlighting Its Convergences and Differences with IT.



- In IFIP Advances in Information and Communication Technology: Vol. 766 IFIPAI. https://doi.org/10.1007/978-3-032-03538-7_3
- Rugge, F. (2018). "Mind Hacking": Information warfare in the cyber age | "Mind Hacking": La guerra informativa nell'era cyber. *Notizie Di Politeia*, 34(132), 108–117.
- Shekhawat, V., Khare, P., & Hoang, K. L. (2025). Cyber warfare and blurring lines between state and non-state actors. In *Technology Geopolitics and the Transformation of International Political Economy*. <https://doi.org/10.4018/979-8-3373-1727-4.ch004>
- Sin, S., & Washburn, R. (2022). When the levee breaks: A global trend of cyber-physical and cyber-operational attacks against critical infrastructure and future implications on the great power competition. In *Great Power Competition* (Vol. 3). https://doi.org/10.1007/978-3-031-04586-8_7
- Siroli, G. P. (2018). Considerations on the Cyber Domain as the New Worldwide Battlefield. *International Spectator*, 53(2), 111–123. <https://doi.org/10.1080/03932729.2018.1453583>
- Smyth, S. M. (2018). Warfare of the Future. In *Advanced Sciences and Technologies for Security Applications*. https://doi.org/10.1007/978-3-319-74107-9_13
- Stanik, J., & Kiedrowicz, M. (2025). INTEGRATION OF NATIONAL CYBERSECURITY STANDARDS INTO THE GEOGRAPHIC INFORMATION SYSTEMS IN THE CONTEXT OF CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT. *Geographic Information Systems Odyssey Journal*, 5(1), 111–121. <https://doi.org/10.57599/gisoj.2025.5.1.111>
- Stefanov, M., & Berchev, D. (2025). Integration Processes in the Military Education System. *Environment Technology Resources Proceedings of the 16th International Scientific and Practical Conference*, 5, 277–284. <https://doi.org/10.17770/etr2025vol5.8466>
- Tsetsos, K. (2025). Preparing Civilian Infrastructure for Potential Cyber and Hybrid Attacks. In *Co Evolution of Technology and Warfare Reshaping the Battlefield*. <https://doi.org/10.4324/9781003520160-9>
- Veerasamy, N., Moolla, Y., & Dawood, Z. (2022). Application of Geospatial Data in Cyber Security. *European Conference on Information Warfare and Security Eccws*, 2022-June, 305–313.

