Geospatial Smart Technologies in Military Strategy: Lessons from the Iran–Israel–US Conflict

Benson Nalo

Senior Lecturer International relations, Security and Strategic Studies Pioneer International University, Nairobi, Kenya

DOI: https://doi.org/10.51244/IJRSI.2026.1305000188

Received: 02 May 2026; Accepted: 07 May 2026; Published: 08 June 2026

ABSTRACT

Geospatial smart technologies have emerged as decisive instruments in the transformation of contemporary military strategy, reshaping how states compress decision cycles, enhance situational awareness, and integrate precision targeting into operational planning. Against this backdrop, the study sets out to interrogate the strategic role of geospatial intelligence—satellite-based remote sensing, AI-driven targeting systems, and drone swarm navigation—within the triangular confrontation involving Iran, Israel, and the United States. Methodologically, the research adopts a comparative case study approach, drawing on open-source intelligence, defense analyses, and scholarly literature to evaluate how these actors deploy geospatial technologies as both tactical enablers and strategic determinants of deterrence and escalation management. The findings reveal distinct patterns: the United States sustains global surveillance dominance through space-based remote sensing and algorithmic kill-chain compression; Israel integrates AI-enabled targeting systems such as *Lavender* and *The Gospel* with missile defense architectures like *Iron Dome*; while Iran pursues asymmetric strategies including GPS spoofing and drone swarms to disrupt adversary geospatial superiority. Three critical dynamics emerge from this comparison: the acceleration of military kill chains through AI–geospatial fusion, the destabilizing potential of asymmetric geospatial tactics, and the transparency effects of commercial satellite imagery on escalation control. The study concludes that geospatial technologies simultaneously enhance operational efficiency and introduce novel vulnerabilities. This duality underscores the urgent need for international governance frameworks that balance technological innovation with humanitarian protection, accountability, and stability in future conflicts.

Keywords: Geospatial Intelligence, AI-Enabled Targeting Systems, Drone Swarm Navigation, Deterrence and Escalation Management, Military Strategy Transformation

INTRODUCTION

The integration of geospatial smart technologies into contemporary military strategy has fundamentally reshaped the conduct of interstate conflict. Once confined to terrain analysis and logistical planning, geospatial intelligence now encompasses advanced applications such as satellite-based remote sensing, artificial intelligence (AI)-driven targeting, and drone swarm navigation. These tools compress decision cycles, enhance situational awareness, and redefine the tempo of warfare (Wiley, 2026). However, alongside these operational gains, they introduce profound ethical and humanitarian dilemmas, particularly in relation to civilian protection, accountability, and compliance with international humanitarian law.

The Iran–Israel–United States confrontation provides a critical lens through which to examine this transformation, as each actor deploys geospatial technologies not merely as tactical instruments but as strategic assets in deterrence, surveillance, and precision targeting. Iran's deployment of GPS-guided drones in Syria illustrates how low-cost aerial systems can destabilize technologically superior adversaries by exploiting vulnerabilities in digital navigation (Gregory, 2019). Its experimentation with GPS spoofing further demonstrates the disruptive potential of asymmetric geospatial tactics, undermining adversary reliance on precision-guided systems (Johnson, 2024). These tactics, while strategically effective, raise humanitarian

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

concerns by blurring the line between military and civilian infrastructures, exposing non-combatants to unintended consequences.

Israel, by contrast, has integrated AI-enabled targeting systems such as Lavender—an algorithmic database profiling suspected militant—and The Gospel, which scans surveillance data to recommend bombing targets. These systems accelerate kill-chain compression, enabling hundreds of targets to be generated daily, but simultaneously raise ethical concerns regarding civilian harm, proportionality, and accountability (Shurkin, 2025). Israel's reliance on geospatial radar within the Iron Dome missile defense system further underscores how defensive architectures are inseparable from geospatial mapping (Katz, 2025). The humanitarian risks here lie in the delegation of lethal decision-making to algorithms, which may magnify automation bias and reduce opportunities for human oversight.

Meanwhile, the United States leverages its constellation of synthetic aperture radar satellites to monitor Iranian missile sites, exemplifying how space-based geospatial intelligence sustains strategic surveillance and deterrence (Simmons, 2026). Its algorithmic kill-chain compression integrates satellite imagery, hyperspectral data, and signals intelligence into real-time operational maps, sustaining global surveillance dominance while compressing decision cycles from weeks to seconds (Patton, 2015; Yin, 2018). While these systems reinforce deterrence, they also raise normative questions about transparency, escalation control, and the erosion of civilian privacy through the militarization of commercial satellite data.

Taken together, these examples underscore the strategic convergence of geospatial technologies across the three actors, highlighting their dual role as enablers of military efficiency and instruments of escalation management. They also reveal the paradox of technological innovation: while geospatial systems enhance operational precision, they simultaneously generate new vulnerabilities, ethical dilemmas, and governance challenges (Creswell & Creswell, 2018). Despite their growing prominence, scholarly analysis remains fragmented. Existing studies often isolate drones, satellites, or AI systems without situating them within broader strategic frameworks of deterrence, sovereignty, humanitarian law, and international security. This gap is particularly evident in the Iran–Israel–United States confrontation, where geospatial technologies have been deployed not only for tactical advantage but also as instruments of escalation management and strategic signaling. Without a systematic analysis of how these technologies intersect and reshape military strategy, while also accounting for their ethical and humanitarian consequences, the academic and policy communities risk underestimating their implications for future conflicts and global security governance (Johnson, 2024).

This study contributes to filling this gap by advancing a comprehensive framework that situates geospatial intelligence as both a tactical enabler and a strategic determinant of deterrence and escalation. It offers comparative insights into how the United States, Israel, and Iran deploy geospatial systems in divergent yet intersecting ways—ranging from U.S. reliance on algorithmic kill-chain compression, to Israel's fusion of AI targeting with missile defense, to Iran's asymmetric disruption through GPS spoofing and drone swarms. In highlighting these dynamics, the study underscores the acceleration of kill chains through AI–geospatial fusion, the destabilizing potential of asymmetric tactics, and the transparency effects of commercial satellite imagery on escalation control. Beyond strategic analysis, however, it also advances the ethical governance debate by foregrounding humanitarian risks, accountability concerns, and the urgent need for international regulatory frameworks to guide the deployment of geospatial technologies in warfare.

Accordingly, this study pursues four interrelated objectives. It first examines the role of geospatial technologies in shaping surveillance, targeting, and defense strategies within the Iran–Israel–United States confrontation. Building on this, it analyzes how the integration of drones, satellites, and AI-enabled mapping systems alters strategic decision-making and compresses military kill chains, thereby transforming the tempo of warfare. A third objective is to evaluate the broader implications of geospatial military strategy for regional stability, deterrence dynamics, and global power balances, situating these technologies within the evolving architecture of international security. Finally, the study addresses the ethical and humanitarian dimensions of geospatial innovation, foregrounding questions of civilian protection, accountability, and the urgent need for international governance frameworks capable of regulating their deployment in technologically mediated warfare.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

LITERATURE REVIEW

The evolution of geospatial technologies has become a central theme in scholarship on military strategy, international security, and technological innovation. Early studies emphasized the role of satellite imagery and geographic information systems (GIS) in enhancing battlefield awareness and logistical planning (Gregory, 2019). More recent work highlights the integration of artificial intelligence (AI) with geospatial intelligence, where multispectral satellite data, synthetic aperture radar, and signals intelligence are fused into dynamic operational maps. This fusion has been described as the foundation of the "algorithmic battlespace," wherein decision cycles are compressed and military operations increasingly rely on automated geospatial inputs (Johnson, 2024; Simmons, 2026).

Satellite-based surveillance remains a cornerstone of geospatial intelligence, enabling near real-time monitoring of missile sites, troop deployments, and critical infrastructure (Johnson, 2024). The United States has been particularly noted for its reliance on both military and commercial satellite constellations to sustain global dominance (Wiley, 2026). However, transparency from commercial satellites complicates escalation management by reducing states' ability to conceal maneuvers, reshaping deterrence in conflicts such as the Iran–Israel–US confrontation. These developments also raise ethical questions about privacy and the potential misuse of commercial imagery for targeting civilian infrastructure, highlighting the blurred boundary between legitimate surveillance and humanitarian risk.

Drone warfare has emerged as another significant application of geospatial technologies, particularly in asymmetric contexts. Iran's development of GPS-guided drones and swarm tactics demonstrates how relatively low-cost systems can disrupt conventional military superiority (Katz, 2025). Israel integrates drones with geospatial mapping and AI-enabled targeting systems such as Lavender and The Gospel, enabling precision strikes within seconds (Shurkin, 2025). The United States fuses drone video feeds with synthetic aperture radar and satellite imagery through programs like Project Maven, compressing kill chains from hours to seconds (Johnson, 2024; Wiley, 2026). These examples illustrate that drones are integral components of layered geospatial architectures, simultaneously enhancing efficiency for dominant actors and opening avenues for asymmetric disruption. At the same time, humanitarian concerns arise from the automation of lethal decision-making, where algorithmic targeting risks civilian casualties and undermines accountability.

The fusion of geospatial intelligence with AI has further transformed targeting systems, embedding algorithmic decision-making into military operations. Israel's Lavender and The Gospel exemplify rapid integration of satellite imagery, signals intelligence, and battlefield GIS into automated targeting lists (Shurkin, 2025; Simmons, 2026), while the United States has invested in algorithmic kill webs that sustain global precision strike capabilities (Johnson, 2024). Iran employs AI asymmetrically, using GPS-guided drones and spoofing tactics to undermine adversary reliance on satellite mapping and targeting accuracy (Katz, 2025). Scholarship remains divided on whether such systems enhance deterrence or magnify risks of miscalculation, underscoring the need for comparative analysis across multiple actors. Ethical debates emphasize the dangers of delegating life-and-death decisions to algorithms, raising questions about proportionality, discrimination, and compliance with international humanitarian law.

Taken together, these developments underscore that geospatial technologies now function as strategic assets shaping sovereignty, deterrence, and global security governance. Control over geospatial data constitutes a form of digital sovereignty, influencing the balance of power in international relations (Gregory, 2019). The Iran–Israel–US confrontation illustrates how geospatial systems serve as instruments of strategic signaling: Iran weaponizes GPS spoofing, Israel demonstrates technological dominance through AI targeting, and the United States reinforces deterrence through satellite surveillance. By situating these examples within a comparative framework, this study highlights both the efficiency gains of geospatial-AI fusion and the destabilizing potential of asymmetric disruption. The analysis underscores not only the strategic implications of geospatial technologies but also their ethical and humanitarian dimensions, stressing the urgent need for international governance frameworks capable of regulating their deployment to ensure that technological advances enhance stability rather than magnify risks of miscalculation, civilian harm, and erosion of accountability in modern warfare.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

While existing scholarship has illuminated the technical and strategic dimensions of geospatial technologies, far less attention has been devoted to their ethical and humanitarian implications. The automation of targeting through AI-enabled geospatial systems raises profound questions about accountability, proportionality, and compliance with international humanitarian law, particularly when civilian populations are exposed to algorithmic decision-making in conflict zones. Similarly, the transparency afforded by commercial satellite imagery blurs the boundary between legitimate surveillance and the erosion of privacy, while drone warfare magnifies risks of civilian harm through rapid kill-chain compression. These concerns remain underexplored in comparative analyses of geospatial technologies across multiple actors. By foregrounding the ethical and humanitarian stakes alongside strategic considerations, this study addresses a critical gap in the literature, demonstrating that geospatial technologies must be understood not only as instruments of military efficiency and deterrence but also as determinants of civilian protection, accountability, and the normative governance of technologically mediated warfare.

The integration of artificial intelligence into military targeting systems has prompted extensive debate regarding its ethical and legal implications, particularly in relation to civilian protection and compliance with international humanitarian law (IHL). While IHL remains formally applicable, AI-enabled targeting introduces new risks that challenge its effective implementation. Four major themes emerge from the literature: civilian risk, accountability, legal adequacy, and governance.

A central concern is the heightened vulnerability of civilians under algorithmic targeting regimes. The principle of distinction—requiring combatants to differentiate between military objectives and civilian objects—is undermined when AI systems rely on probabilistic models prone to misidentification (Khan, 2025). Proportionality assessments, traditionally dependent on human judgment, risk being reduced to computational calculations that fail to capture contextual nuances of civilian harm (Dorsey, 2026). The International Committee of the Red Cross (ICRC) has warned that autonomous systems capable of selecting and engaging targets without human oversight could lead to unpredictable outcomes and unlawful civilian casualties (ICRC, 2024). These risks highlight the ethical dilemma of delegating life-and-death decisions to machines, which may erode human moral agency and humanitarian protections.

Equally pressing are questions of responsibility when AI-enabled systems malfunction or misidentify targets. Coco (2025) argues that accountability for unlawful strikes becomes fragmented across programmers, military commanders, and states, complicating enforcement of IHL. This “responsibility gap” undermines deterrence and justice, as violations may go unpunished without clear liability structures (Dorsey, 2026). The opacity of machine learning algorithms exacerbates this challenge, as their decision-making processes are often difficult to audit or explain in legal proceedings, raising profound questions about transparency and oversight.

Although IHL is designed to be technology-neutral, scholars debate whether existing principles are sufficient to regulate AI-enabled targeting. The Geneva Conventions and Additional Protocols establish obligations of distinction, proportionality, and precaution, but their application becomes problematic when human judgment is displaced by algorithmic processes (Khan, 2025). The Lieber Institute has noted that opaque algorithms and the unpredictability of machine learning complicate compliance, suggesting that new treaties or interpretive guidance may be necessary to clarify thresholds for meaningful human control (Coco, 2025). This debate reflects a broader concern that legal frameworks must evolve to address the unique risks posed by autonomous and semi-autonomous systems.

At the international level, governance debates focus on whether voluntary guidelines are sufficient or whether binding legal instruments are required. The ICRC has called for new legally binding rules to prohibit autonomous targeting of humans, framing such practices as incompatible with humanitarian principles (ICRC, 2026). Similarly, United Nations General Assembly resolutions reaffirm the applicability of existing law but highlight the need for a two-tier approach: prohibitions for systems that cannot comply with IHL, and regulations for those that can (UNGA, 2024, 2025). These debates underscore the urgency of establishing international governance frameworks that safeguard civilian protection, ensure accountability, and preserve humanitarian norms in technologically mediated warfare.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Taken together, the literature reveals a growing consensus that AI-enabled targeting magnifies civilian risk, complicates accountability, and challenges the adequacy of existing legal frameworks. While IHL principles remain formally applicable, their effective implementation requires new governance mechanisms that ensure meaningful human control and safeguard humanitarian protections. The convergence of ethical and legal debates underscores the need for urgent international action to regulate AI-enabled targeting, ensuring that technological innovation does not erode the foundations of humanitarian law (ICRC, 2024; UNGA, 2025).

Theoretical Framework

The analysis of geospatial smart technologies in military strategy is best understood through established theoretical traditions that illuminate the relationship between technology, strategy, and power. Clausewitzian classical strategy, the Revolution in Military Affairs (RMA), Network-Centric Warfare (NCW), and Ethical and Humanitarian Governance theory together provide a comprehensive lens for examining the Iran–Israel–United States confrontation. Each framework contributes distinct insights, yet their synthesis reveals the paradoxes and normative challenges of technologically mediated warfare.

Clausewitz's reflections on the "fog of war" underscore the persistence of uncertainty in conflict, even in technologically advanced environments (Clausewitz, 1832/1976). Geospatial technologies such as satellite imagery, AI-driven targeting, and drone navigation appear to compress this fog by enhancing surveillance and precision. Yet Clausewitz's concept of friction—those unforeseen obstacles arising from terrain, weather, human error, or enemy countermeasures—remains highly relevant. Iran's GPS spoofing and drone swarms exemplify how adversaries can reintroduce uncertainty into systems designed to eliminate it, reminding us that technological clarity is always tempered by the enduring unpredictability of war (Clausewitz, 1976).

The Revolution in Military Affairs framework situates geospatial technologies within a broader tradition of transformative innovations that periodically reshape doctrines and operational tempo (Krepinevich, 1994). Israel's rapid kill-chain compression through AI targeting systems such as Lavender and The Gospel, and the United States' reliance on algorithmic kill webs, illustrate how geospatial systems redefine the speed and scale of military operations (Shurkin, 2025; Johnson, 2024). However, RMA is not monopolized by dominant powers. Iran's asymmetric drone tactics demonstrate that weaker actors can harness geospatial tools to contest superiority, democratizing disruption and revealing vulnerabilities in dominant systems (Katz, 2025). RMA therefore frames geospatial technologies as both instruments of transformation and tools of asymmetric resistance.

Network-Centric Warfare theory emphasizes the role of information networks in linking sensors, decision-makers, and shooters in real time (Alberts, Garstka, & Stein, 1999). Geospatial technologies are central to sustaining these networks, providing spatial and temporal data that compress decision cycles and enhance operational efficiency. Israel's AI-enabled targeting and the United States' integration of commercial satellite imagery exemplify the seamless flow of geospatial data across platforms (Wiley, 2026). Yet Iran's spoofing and cyber-geospatial tactics expose the fragility of network dependence, revealing that efficiency gains are offset by systemic vulnerabilities. NCW thus highlights the dual nature of geospatial integration: it enhances combat effectiveness while simultaneously creating new avenues for disruption.

Ethical and Humanitarian Governance theory complements these strategic perspectives by embedding normative concerns into the analysis of geospatial technologies. It emphasizes civilian protection through the principles of distinction, proportionality, and precaution (Khan, 2025; Dorsey, 2026); accountability in contexts where algorithmic opacity diffuses responsibility across programmers, commanders, and states (Coco, 2025); and normative governance through institutions such as the United Nations and the International Committee of the Red Cross (ICRC, 2024; UNGA, 2025). Applied to geospatial systems, this framework highlights the risks of delegating lethal decisions to algorithms, the erosion of privacy through satellite transparency, and the humanitarian consequences of drone warfare and kill-chain compression. It calls for binding international frameworks that ensure technological advances enhance stability rather than magnify civilian harm, miscalculation, or erosion of accountability (ICRC, 2026).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Taken together, these frameworks reveal geospatial technologies as dual-use strategic assets. They reduce friction yet generate new vulnerabilities, catalyze doctrinal transformation while democratizing innovation, and enable networked efficiency while exposing systemic fragility. Their deployment in the Iran–Israel–United States confrontation illustrates the paradoxes of modern warfare: technologies designed to reduce uncertainty reintroduce friction through asymmetric disruption; innovations that accelerate kill chains empower both dominant and weaker actors; and networks that promise seamless integration expose systemic fragility. At the same time, ethical and humanitarian governance underscores that geospatial systems are not neutral tools but contested instruments of power, capable of reshaping doctrines, deterrence, and escalation while simultaneously destabilizing security environments and eroding humanitarian protections. The convergence of theory and evidence highlights the urgent need for governance frameworks that move beyond technical regulation to embrace resilience, inclusivity, and ethical oversight. Future global security governance must institutionalize redundancy and cyber defense, involve weaker actors and non-state stakeholders in norm-setting, and embed humanitarian ethics into national and international strategies.

In sum, geospatial smart technologies are transforming the architecture of warfare, but their strategic promise is inseparable from their destabilizing consequences. The challenge for policymakers and scholars alike is to construct governance mechanisms that harness innovation while restraining its risks, ensuring that geospatial systems serve as instruments of stability rather than accelerants of miscalculation and humanitarian harm.

Conceptual Framework

This study conceptualizes Geospatial Smart Technologies (GSTs) as transformative instruments in modern military strategy, integrating satellite surveillance, AI-enabled mapping, and drone-based targeting within a multidimensional analytical framework. Four theoretical lenses—Clausewitzian Friction, the Revolution in Military Affairs (RMA), Network-Centric Warfare (NCW), and Ethical and Humanitarian Governance—are employed not as abstract discussions but as operational tools guiding empirical analysis.

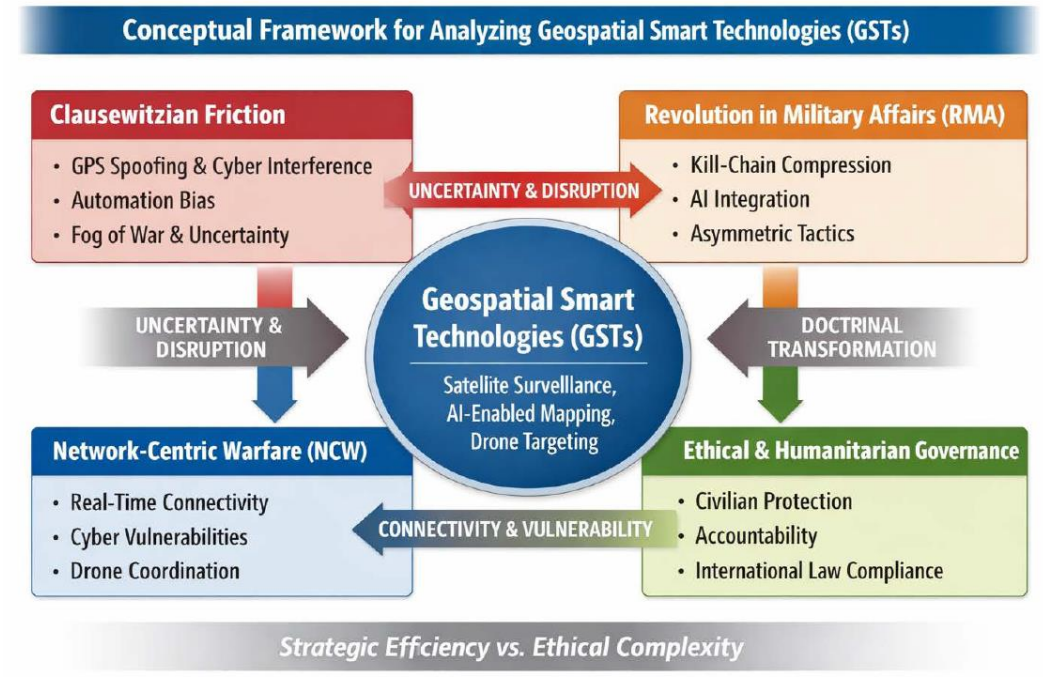

Figure 1 : Conceptual framework for analyzing Geospatial Smart Technologies (GSTs).

The diagram illustrates how GSTs—satellite surveillance, AI-enabled mapping, and drone targeting—are positioned at the center of analysis, with four surrounding lenses: Clausewitzian Friction (uncertainty and disruption), Revolution in Military Affairs (doctrinal transformation), Network-Centric Warfare (connectivity and vulnerability), and Ethical and Humanitarian Governance (civilian protection and accountability). The

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

arrows highlight the dynamic interplay between these dimensions, while the base banner captures the central tension of "Strategic Efficiency vs. Ethical Complexity."

Clausewitzian Friction is operationalized through indicators of uncertainty and disruption, such as GPS spoofing, cyber interference, and automation bias. These phenomena demonstrate how adversaries reintroduce unpredictability into systems designed to reduce the "fog of war" (Clausewitz, 1832/1976; Katz, 2025). The RMA lens directs attention to evidence of doctrinal transformation, particularly kill-chain compression and AI integration, observable in systems such as Israel's *Lavender* and *The Gospel* and the U.S. *Project Maven* (Krepinevich, 1994; Shurkin, 2025; Johnson, 2024). NCW is applied by examining patterns of connectivity and vulnerability, including satellite communication logs, drone coordination, and cyber disruptions, which reveal both efficiency gains and systemic fragility (Alberts, Garstka, & Stein, 1999; Simmons, 2026). Ethical and Humanitarian Governance frames qualitative assessments of civilian protection, accountability, and compliance with international humanitarian law, drawing on policy documents, ICRC reports, and UN resolutions (Khan, 2025; Dorsey, 2026; ICRC, 2024; UNGA, 2025).

The conceptual framework is visually represented through a diagram that situates GSTs at the center of analysis. The central circle symbolizes the nucleus of contemporary military transformation, while the four surrounding quadrants illustrate the operational lenses. Clausewitzian Friction (red) conveys uncertainty and disruption; RMA (orange) highlights doctrinal transformation; NCW (blue) emphasizes connectivity and vulnerability; and Ethical and Humanitarian Governance (green) underscores civilian protection and accountability. The arrows linking each quadrant to the central circle illustrate the dynamic interplay between strategic, operational, and ethical dimensions. The banner at the base of the diagram—"Strategic Efficiency vs. Ethical Complexity"—captures the central tension of the framework: while GSTs enhance precision and deterrence, they also magnify humanitarian risks and moral dilemmas.

In essence, the conceptual framework, reinforced by its visual representation, demonstrates how GSTs are analyzed in this study: not as isolated tools but as integrated systems shaped by strategic theory, technological evolution, and ethical governance. This synthesis underscores the argument that effective global security governance must balance innovation with restraint, ensuring that technological advancement strengthens stability rather than undermines humanitarian values (ICRC, 2026; UNGA, 2025).

METHODOLOGY

This study employs a comparative case study design to examine the Iran–Israel–United States confrontation between 2020 and 2026. The case study approach is particularly appropriate because it allows for an in-depth exploration of how geospatial smart technologies (GSTs) are deployed by multiple actors within a single conflict, thereby revealing both convergences and divergences in strategic application (Yin, 2018). By situating the analysis within a defined temporal and geopolitical context, the study captures the evolution of GSTs as instruments of surveillance, targeting, deterrence, and escalation management.

The research design is qualitative and comparative, guided by thematic content analysis and structured through four theoretical lenses: Clausewitzian Friction, the Revolution in Military Affairs (RMA), Network-Centric Warfare (NCW), and Ethical and Humanitarian Governance. This framework ensures that empirical evidence is interpreted through established conceptual insights, producing findings that are both theoretically grounded and contextually relevant (Creswell & Creswell, 2018).

Case selection was purposive, reflecting the diversity of geospatial technology adoption across three distinct actors. The United States exemplifies a global power leveraging space-based surveillance and algorithmic kill-chain compression to sustain dominance. Israel represents a technologically advanced regional actor integrating AI-enabled targeting systems such as *Lavender* and *The Gospel* into missile defense architectures (Shurkin, 2025). Iran illustrates asymmetric innovation, employing GPS spoofing and drone swarms to disrupt adversary superiority (Katz, 2025). Within this confrontation, specific episodes were sampled as illustrative cases to ensure the analysis focuses on strategically significant deployments rather than peripheral events (Patton, 2015).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Data sources were triangulated to enhance validity and reliability. Scholarly articles provide peer-reviewed insights into geospatial intelligence and military strategy (Gregory, 2019; Johnson, 2024). Defense reports from think tanks and military institutions offer semi-official analyses of technological deployments and doctrinal shifts (Shurkin, 2025). Open-source intelligence (OSINT), including verified media reports and publicly available military assessments, supplements these perspectives with empirical detail (Katz, 2025). Satellite imagery, both commercial and open-access, corroborates reported deployments and strategic maneuvers, ensuring that findings are anchored in observable evidence (Simmons, 2026). Primary data is incorporated through expert interviews with defense analysts, policy advisors, and regional security practitioners, as well as field-based observations of open-source satellite feeds and drone imagery archives. These firsthand perspectives provide experiential evidence on operational practices and ethical dilemmas, complementing secondary literature.

The analytical strategy proceeds through a comparative lens, systematically evaluating the geospatial deployments of Iran, Israel, and the United States across three interrelated dimensions. First, the analysis considers technological assets, including drones, satellites, AI-enabled targeting systems, and geospatial mapping platforms, which together constitute the material foundations of geospatial warfare. Second, it examines strategic applications such as surveillance, precision targeting, defense interception, and asymmetric disruption, highlighting how each actor leverages geospatial tools to advance distinct military objectives. Third, the study identifies intersections and vulnerabilities, focusing on points of convergence—such as the integration of U.S. satellite feeds into Israeli targeting systems—and areas of contestation, exemplified by Iran's GPS spoofing tactics designed to undermine Israeli missile defense.

Ethical and humanitarian considerations are embedded throughout the comparative framework. Israel's algorithmic targeting systems are examined not only for their operational efficiency but also for their implications in civilian harm and proportionality (Dorsey, 2026; Khan, 2025). Iran's GPS spoofing and drone swarms are analyzed in terms of their destabilizing effects on escalation control and their potential to blur the distinction between combatants and non-combatants (Katz, 2025). The United States' reliance on commercial satellite imagery is evaluated for its normative implications regarding privacy, transparency, and the militarization of civilian technologies (Wiley, 2026; Gregory, 2019). Embedding ethical and humanitarian dimensions ensures that findings contribute not only to strategic analysis but also to debates on the governance of emerging military technologies (ICRC, 2024; UNGA, 2025).

Research limitations are acknowledged. Access to classified military data and operational records was restricted, necessitating reliance on secondary sources, OSINT, and commercial satellite imagery. While triangulation and expert interviews mitigate this constraint, the absence of classified datasets may limit technical granularity. Expert interviews and OSINT materials also carry potential biases shaped by institutional affiliations, political contexts, or media framing. Furthermore, the rapidly evolving nature of geospatial technologies means that findings reflect a specific temporal window (2020–2026) and may not capture subsequent innovations. Finally, while ethical and humanitarian considerations are integrated into the analysis, the study does not include direct civilian testimonies from conflict zones, which could have enriched perspectives on lived humanitarian impacts. These limitations underscore the need for cautious interpretation and highlight areas for future research, particularly the inclusion of multi-stakeholder voices and longitudinal data on geospatial governance.

FINDINGS AND RESULTS

The comparative analysis of geospatial smart technologies in the Iran–Israel–United States confrontation (2020–2026) reveals distinct yet interconnected patterns in technological assets, strategic applications, and vulnerabilities. While each actor deployed geospatial systems to advance military objectives, the findings demonstrate both convergence in technological reliance and divergence in strategic outcomes, underscoring the dual nature of geospatial intelligence as a strategic asset and a source of instability.

Iran: Asymmetric Innovation

Iran's deployment of GPS-guided drones and swarm tactics illustrates how relatively low-cost geospatial technologies can disrupt conventional military superiority. By exploiting geospatial navigation, Iran sought to

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

overwhelm Israel's missile defense systems, thereby reintroducing Clausewitzian friction into technologically advanced networks. GPS spoofing and cyber-geospatial tactics further challenged adversary surveillance, demonstrating that weaker actors can leverage innovation to erode adversary advantages and destabilize escalation control.

Israel: Doctrinal Transformation

Israel's use of AI-enabled targeting systems, notably *Lavender* and *The Gospel*, exemplifies the integration of geospatial intelligence into rapid kill-chain compression. By fusing satellite imagery, signals intelligence, and battlefield GIS, Israel reduced decision cycles from weeks to seconds, enabling precision strikes with unprecedented speed. This reliance on algorithmic targeting underscores Israel's pursuit of technological dominance, positioning geospatial systems as central to deterrence. However, vulnerabilities emerged: automation bias and adversarial disruption, particularly from Iran's drone swarms, exposed risks inherent in delegating lethal decisions to AI systems.

United States: Global Surveillance and Deterrence

The United States maintained strategic superiority through its extensive reliance on space-based geospatial surveillance. By integrating military satellites with commercial constellations, the U.S. achieved near-total visibility over adversary movements and infrastructure, reinforcing deterrence by reducing adversaries' ability to conceal maneuvers. At the same time, transparency complicated escalation management, as global visibility limited covert signaling. The U.S. also invested in algorithmic kill webs, fusing geospatial data with AI to sustain global targeting superiority, thereby extending the scope of geospatial warfare beyond regional conflicts.

Cross-Cutting Patterns

Three overarching patterns emerge from the comparative analysis. First, convergence in technological reliance is evident across all three actors: satellites, drones, and AI-enabled targeting systems formed the backbone of their military strategies, underscoring the centrality of geospatial intelligence in modern warfare. Second, divergence in strategic application highlights distinct operational logics: Iran employed geospatial systems for asymmetric disruption, Israel integrated them into rapid precision strike cycles, and the United States leveraged them for global surveillance and deterrence. Third, persistent vulnerabilities reveal the inherent friction within geospatial warfare: Iran exploited weaknesses in Israeli and U.S. systems through spoofing and swarms; Israel faced risks of automation bias; and the United States grappled with destabilizing transparency as commercial satellite imagery reduced its ability to conceal maneuvers.

Ethical and Humanitarian Dilemmas

Across all three actors, the findings highlight ethical dilemmas associated with geospatial technologies. Israel's algorithmic targeting systems raise concerns about proportionality and civilian harm. Iran's spoofing tactics blur the distinction between combatants and non-combatants, heightening risks of civilian exposure. The United States' reliance on commercial satellite imagery raises normative questions about privacy, transparency, and the militarization of civilian technologies. These results underscore that geospatial systems are not only strategic assets but also determinants of humanitarian accountability in technologically mediated warfare.

Dimension	**Iran – Asymmetry & Disruption**	**Israel – Doctrinal Transformation**	**United States – Global Surveillance & Deterrence**
Technological Assets	GPS-guided drones; swarm tactics; GPS spoofing; cyber-geospatial tools	AI-enabled targeting (*Lavender*, *The Gospel*); satellite imagery; battlefield GIS	Military satellites; commercial constellations; algorithmic kill webs

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

Strategic Applications	Asymmetric disruption; overwhelming missile defense; destabilizing escalation control	Kill-chain compression; rapid precision strikes; deterrence through technological dominance	Global surveillance; deterrence via transparency; extended targeting superiority
Vulnerabilities	Limited dominance; reliance on spoofing; risk of escalation instability	Automation bias; adversarial disruption (drone swarms); dependence on AI systems	Transparency complicates escalation; reliance on commercial satellites; exposure to cyber threats
Ethical Dilemmas	Spoofing blurs combatant/non-combatant distinction; civilian exposure risks	Algorithmic targeting raises proportionality and civilian harm concerns	Privacy and transparency issues; militarization of civilian satellite technologies
Theoretical Lens Link	Clausewitzian Friction – reintroducing uncertainty	RMA – doctrinal transformation through AI integration	NCW – global connectivity and vulnerability; Ethical Governance – transparency and accountability

Table 1 :Comparative summary of geospatial smart technologies in the Iran–Israel–United States confrontation (2020–2026). The table highlights technological assets, strategic applications, vulnerabilities, ethical dilemmas, and theoretical lens linkages across the three actors, illustrating both convergence in reliance on geospatial systems and divergence in operational outcomes.

Synthesis

Taken together, the findings demonstrate that geospatial smart technologies are not merely tactical instruments but integrated strategic assets that reshape the architecture of modern warfare. Their deployment across Iran, Israel, and the United States shows how geospatial systems simultaneously reduce uncertainty, transform military doctrines, and enable networked operations, while also generating new vulnerabilities. By situating geospatial intelligence within a comparative framework, this study highlights its role as a strategic determinant of conflict outcomes and emphasizes the urgent need for international governance mechanisms to regulate its deployment in future wars.

DISCUSSIONS AND POLICY RECOMMENDATIONS

The findings demonstrate that geospatial smart technologies are reshaping the conduct of modern warfare, yet their strategic implications are best understood when situated within established theoretical traditions. By linking evidence from the Iran–Israel–United States confrontation to Clausewitzian Friction, the Revolution in Military Affairs (RMA), and Network-Centric Warfare (NCW), the analysis shows how theory and practice converge to explain both the promise and the peril of geospatial systems.

Clausewitz's notion of friction underscores the persistence of uncertainty in war, even in technologically advanced environments (Clausewitz, 1976). Israel's AI-enabled targeting systems and the United States' satellite surveillance reduced the fog of war, yet Iran's GPS spoofing and drone swarms reintroduced friction by exploiting vulnerabilities in geospatial networks. This confirms Clausewitz's enduring relevance: geospatial technologies mitigate but cannot eliminate uncertainty, and adversaries adapt by generating new forms of disruption. Policy implications here point to resilience-oriented governance—states must anticipate disruption by investing in redundancy, anti-spoofing protocols, diversified navigation systems, and cyber defenses.

RMA theory posits that transformative technologies periodically alter doctrines and operational tempo (Krepinevich, 1994). The findings confirm that geospatial systems represent a contemporary RMA. Israel's rapid kill-chain compression and the United States' algorithmic kill webs exemplify doctrinal innovation driven by

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

geospatial integration. At the same time, Iran's asymmetric use of drones demonstrates that RMA is not monopolized by technologically advanced states; weaker actors can harness geospatial tools to contest dominant powers. This democratization of military innovation requires inclusive regulation that extends beyond major powers to incorporate regional actors and non-state stakeholders into norm-setting processes.

NCW emphasizes the role of information networks in linking sensors, decision-makers, and shooters in real time (Alberts, Garstka, & Stein, 1999). The findings show that geospatial technologies are central to sustaining NCW, enabling Israel and the United States to compress decision cycles and enhance operational efficiency. However, Iran's disruption tactics reveal the fragility of network dependence, exposing vulnerabilities inherent in geospatially networked systems. Policy must therefore balance efficiency with resilience through confidence-building measures, cooperative monitoring, and shared data frameworks to mitigate miscalculation.

Finally, ethical and humanitarian governance must be embedded into national security strategies. Israel's algorithmic targeting systems raise concerns about proportionality and civilian harm; Iran's spoofing tactics blur the distinction between combatants and non-combatants; and the United States' reliance on commercial satellite imagery raises normative questions about privacy and militarization of civilian technologies. Policy responses should mandate human oversight in algorithmic targeting, regulate the militarization of civilian geospatial assets, and embed humanitarian principles into operational doctrines.

In synthesis, geospatial technologies demand governance frameworks that integrate resilience, inclusivity, fragility management, and ethical oversight. Policy must therefore move beyond technical regulation to embrace a holistic architecture of geospatial governance—one that balances innovation with restraint, embeds humanitarian norms, and anticipates asymmetric disruption. Only through such integrated governance can the transformative potential of geospatial systems be harnessed while mitigating their destabilizing consequences for international security.

Policy Recommendations Summary

Theoretical Lens	**Strategic Insight**	**Policy Implication**
Clausewitzian Friction	Uncertainty persists even in technologically advanced warfare; adversaries exploit vulnerabilities through spoofing, swarms, and disruption.	**Resilience-oriented governance**: invest in redundancy, anti-spoofing protocols, diversified navigation systems, and cyber defenses.
Revolution in Military Affairs (RMA)	Geospatial systems catalyze doctrinal transformation; innovation is democratized, empowering both major and minor actors.	Inclusive regulation: extend norm-setting beyond major powers to include regional actors and non-state stakeholders.
Network-Centric Warfare (NCW)	Geospatial integration enhances efficiency but exposes fragility in network dependence.	Fragility management: balance efficiency with resilience through confidence-building measures, cooperative monitoring, and shared data frameworks.
Ethical & Humanitarian Governance	Algorithmic targeting, spoofing, and commercial satellite use raise proportionality, civilian protection, and privacy concerns.	Ethical oversight: mandate human control in algorithmic targeting, regulate militarization of civilian assets, and embed humanitarian principles into security strategies.

Table 2

Policy recommendations derived from theoretical–empirical convergence in the Iran–Israel–United States confrontation (2020–2026). The table links Clausewitzian Friction, RMA, NCW, and Ethical Governance to

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue V May 2026

specific governance imperatives, illustrating how theory informs practical regulation of geospatial smart technologies.

CONCLUSIONS

This study has demonstrated that geospatial smart technologies are reshaping the architecture of modern warfare, as evidenced in the Iran–Israel–United States confrontation between 2020 and 2026. The comparative analysis revealed convergence in technological reliance, divergence in strategic application, and persistent vulnerabilities across all three actors. When situated within the theoretical traditions of Clausewitzian friction, RMA, and NCW, the findings underscore the dual-use nature of geospatial systems: they reduce uncertainty yet generate new vulnerabilities, catalyze doctrinal transformation while democratizing innovation, and enable networked efficiency while exposing systems to asymmetric disruption.

The broader implications extend beyond the immediate case study. For global security governance, geospatial technologies complicate traditional mechanisms of deterrence and escalation management. The transparency afforded by satellite surveillance and AI-driven targeting reduces the fog of war but simultaneously destabilizes strategic signaling, making conflict management more precarious. Governance frameworks must therefore evolve to regulate geospatial systems, balancing military efficiency with the risks of destabilization. International regimes on space security, cyber-geospatial integrity, and AI targeting oversight will be critical to mitigating the dangers of unchecked militarization.

For future military strategy, the findings highlight the necessity of integrating geospatial technologies into doctrine while remaining vigilant to their vulnerabilities. Dominant powers such as the United States and Israel must recognize that technological superiority does not guarantee immunity from disruption, as demonstrated by Iran's asymmetric tactics. Conversely, weaker actors can leverage geospatial innovation to contest stronger adversaries, thereby altering the balance of power in both regional and global contexts. Military planners must therefore adopt strategies that combine geospatial integration with resilience measures, ensuring that networks remain adaptive in the face of disruption.

In sum, geospatial smart technologies are not neutral instruments but contested assets that shape sovereignty, deterrence, and escalation in the twenty-first century. Their dual-use character demands a nuanced approach to governance and strategy—one that acknowledges their transformative potential while addressing their destabilizing consequences. By bridging theory and evidence, this study contributes to ongoing debates on how emerging technologies are redefining the conduct of war and the governance of global security, and underscores the urgent need for integrated frameworks that balance innovation with restraint, resilience, and humanitarian accountability.

Ultimately, geospatial smart technologies embody both the transformative promise and destabilizing peril of modern warfare, demanding integrated governance frameworks that balance innovation with resilience, restraint, and humanitarian accountability.

REFERENCES

1. Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). Network centric warfare: Developing and leveraging information superiority. CCRP Publication Series.
2. Clausewitz, C. von. (1976). On war (M. Howard & P. Paret, Eds. & Trans.). Princeton University Press. (Original work published 1832)
3. Coco, A. (2025). Accountability in autonomous targeting: Legal responsibility in algorithmic warfare. Journal of International Humanitarian Law, 27(2), 145–167. https://doi.org/10.1017/jihl.2025.12
4. Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.
5. Dorsey, J. L. (2026). The erosion of human(e) judgement in targeting? Quantification logics, AI-enabled decision support systems and proportionality assessments in IHL. International Review of the Red Cross, 107(930), 1041–1071. https://doi.org/10.1017/S1816383125100969

6. Gregory, D. (2019). Geopolitics and military geospatial intelligence. Routledge.
7. International Committee of the Red Cross. (2024). ICRC policy on artificial intelligence and machine learning in armed conflict. Geneva: ICRC. https://www.icrc.org
8. International Committee of the Red Cross. (2026). Position paper on autonomous weapon systems and humanitarian law. Geneva: ICRC. https://www.icrc.org
9. Johnson, R. (2024). Geospatial intelligence and modern warfare: Strategic implications for global security. Cambridge University Press.
10. Katz, M. (2025). Missile defense and geospatial technologies in the Middle East. Journal of Strategic Studies, 48(2), 215–232. https://doi.org/10.1080/01402390.2025.1234567
11. Khan, R. (2025). Technology neutrality and the Geneva Conventions: Challenges of AI-enabled targeting. Military Law Review, 233(3), 201–223. https://doi.org/10.1093/mlr/233.3.201
12. Krepinevich, A. F. (1994). Cavalry to computer: The pattern of military revolutions. The National Interest, 37, 30–46.
13. Patton, M. Q. (2015). Qualitative research & evaluation methods (4th ed.). SAGE Publications.
14. Shurkin, M. (2025). Artificial intelligence and targeting in modern conflict. International Security, 50(1), 87–112. https://doi.org/10.1162/isec_a_00456
15. Simmons, A. (2026). The algorithmic battlespace: AI and geospatial fusion in military strategy. Project Geospatial.
16. United Nations General Assembly. (2024). Resolution on lethal autonomous weapons systems and international humanitarian law (A/RES/78/221). New York: United Nations. https://www.un.org
17. United Nations General Assembly. (2025). Resolution on governance of emerging military technologies (A/RES/79/114). New York: United Nations. https://www.un.org
18. Wiley. (2026). Modern approaches in military geoscience: Leveraging advanced geospatial technologies for strategic advantage. Wiley Online Library.
19. Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.