

The MILITARISATION OF GEOSPATIAL DATA

The Security Risks of Commercial Satellite Imagery in Wartime



By: **Professor Wael Saleh** (Director at TRENDS Research & Advisory - France and Canada)

Commercial satellite imagery is now an integral component of contemporary warfare, as demonstrated by the recent conflict involving the United States, Israel, and Iran. Imagery captured from space is no longer a neutral visual record of events unfolding on the ground. Instead, it has evolved into a strategic resource capable of serving a wide range of purposes, including verification, documentation, accountability, intelligence collection, geospatial intelligence (GEOINT), battle damage assessment, military planning support, media narrative construction, and even indirect participation in targeting chains. »

» The importance of this transformation lies in the fact that commercial satellite imagery exists in a grey zone between civilian and military domains, between market-driven services and national security imperatives, and between public knowledge and operationally sensitive information. On one hand, it provides journalists, researchers, and civil society organisations with unprecedented capabilities to monitor armed conflicts. On the other, it enables states, adversaries, non-state actors, and geospatial intelligence networks to access information that may possess direct or indirect military value.

This creates a fundamental paradox. The same technologies that enhance transparency and commercial innovation can, during times of war, become sources of security vulnerability. Likewise, tools that support accountability and public oversight may also contribute to target identification, operational planning, or the assessment of military strikes. The rise of commercial Earth-observation companies such as Planet Labs, Maxar/Vantor, ICEYE, and Black-Sky has shifted a portion of space-based observation capabilities from the exclusive domain of sovereign states to a global marketplace for geospatial data. The proliferation of small satellites, increasing image resolution, faster delivery cycles, and advances in artificial intelligence-driven analysis have expanded the scope of this transformation. Consequently, the challenge is no longer limited to the imagery itself. It now encompasses the entire ecosystem that converts imagery into actionable knowledge. A satellite captures the image; a ground station receives it; cloud infrastructure stores it; digital platforms distribute it; algorithms analyse it; and users interpret it. At the end of this chain, the resulting information may influence political decisions, military operations, or media narratives.

Objectives of the Study

This study seeks to analyse the security and strategic risks associated with commercial satellite imagery during armed conflicts. It examines the implications of such imagery for national security, its potential role in supporting military targeting and intelligence-



» Commercial satellite imagery falls into a grey area between civilian and military, between the market and national security, and between public knowledge and operational information.

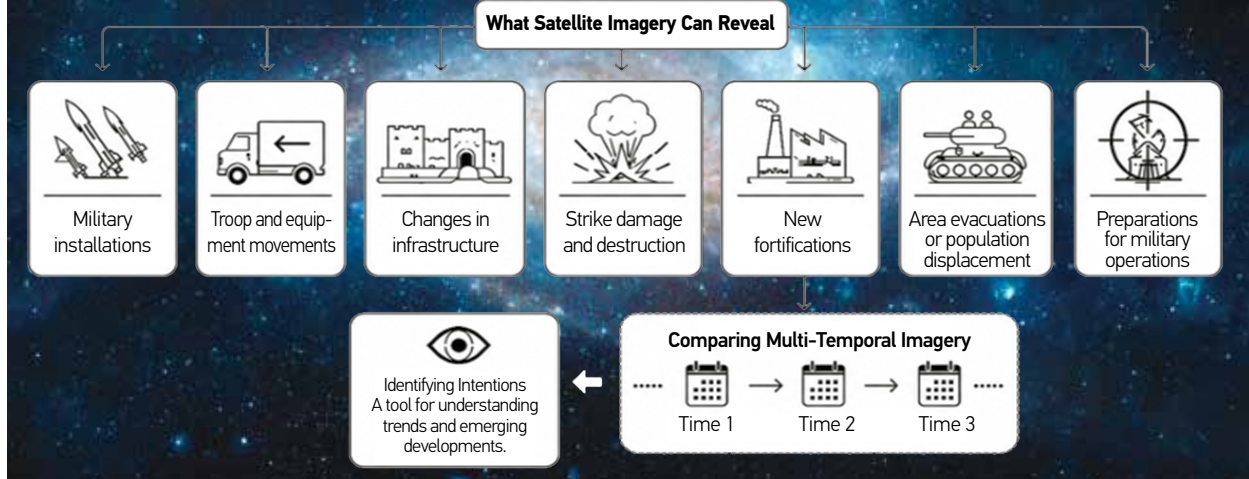
gathering activities, and the legal and regulatory challenges surrounding the control and dissemination of geospatial data. The analysis is particularly relevant given the rapid expansion of commercial actors in the space sector, their integration into licensing and regulatory frameworks, and their growing interaction with the principles of international humanitarian law and space law. The study argues that commercial satellite imagery can no longer be viewed merely as a commercial service or a civilian observation tool. Rather, it has become part of a broader phenomenon that may be described as “geospatial warfare.” In this emerging environment, the ability to access, analyse, interpret, restrict, and strategically release geospatial imagery and video has become an important factor in shaping power balances, influencing narratives, managing escalation, and determining whether actors are exposed to or shielded from accountability.

Commercial Satellite Imagery and the Militarisation of Geospatial Data

The importance of commercial satellite imagery extends far beyond its visual content. Increasingly, such imagery has become part of a broader intel-

ligence architecture. High-resolution images—particularly those approaching near-real-time availability—can reveal military installations, troop movements, infrastructure modifications, strike effects, newly constructed fortifications, population evacuations, and preparations for military operations. When multiple images are compared over time, satellite imagery becomes more than a tool for describing reality; it becomes a mechanism for identifying intentions and forecasting behaviour. Modern military targeting does not rely on a single source of information. Instead, it is built upon integrated data ecosystems. Commercial satellite imagery may constitute one component of these systems, alongside aircraft and maritime tracking data, publicly available videos, unmanned aerial vehicle imagery, field intelligence, open-source information, and automated analytical tools. When combined, these elements transform imagery from a visual record into operationally relevant intelligence. This distinction is particularly important from both legal and strategic perspectives. An image released publicly several days after a military strike differs significantly from imagery provided in near real time to a belligerent actor for the purpose of supporting a specific

Commercial Satellite Imagery: From Visual Observation to Actionable Intelligence



operation. The timing, precision, intended audience, and operational integration of the imagery all influence its strategic significance.

The issue becomes even more consequential with the growing integration of artificial intelligence into geospatial analysis. Advanced algorithms for change detection, pattern recognition, and optical and radar image analysis are capable of dramatically reducing the time required to transform raw imagery into operational conclusions. As a result, the challenge is no longer solely about access to imagery but also about the speed with which that imagery can be converted into militarily useful knowledge. This capability enables the production of sophisticated intelligence products that merge commercial satellite imagery with open-source intelligence, aircraft and vessel tracking data, and other publicly available information streams. In doing so, commercial imagery increasingly becomes part of what can be described as geospatial warfare—a form of competition defined not merely by control of territory, but by control of information about that territory.

In such an environment, power is measured by the ability to access geo-

spatial information, analyse it, restrict it, manipulate it, and deny it to adversaries. Geospatial data becomes the connective tissue linking reconnaissance, command and control, communications, targeting, battle damage assessment, and information operations.

Moreover, this transformation is not limited to major powers. The availability of imagery through commercial markets allows relatively weaker actors to compensate for certain intelligence deficiencies. Although they may lack sovereign satellite constellations or advanced intelligence infrastructures, they can often obtain valuable geospatial information through intermediaries, commercial platforms, third-party networks, or private service providers. In doing so, commercial imagery contributes to a reconfiguration of power relationships by granting actors visibility that would previously have been beyond their reach. Yet these new capabilities come with high costs and vulnerabilities. States that rely heavily on commercial imagery, communications networks, cloud services, or privately owned analytical platforms may become dependent on decisions made by commercial providers. Such dependencies expose governments and military organisations to corporate policies,

regulatory restrictions, political pressure from host governments, shifting access conditions, and potential legal or technical disruptions. Accordingly, reliance on commercial infrastructure represents both an operational opportunity and a source of strategic vulnerability.

Private Companies and Critical Commercial Infrastructure in Modern Warfare

Private companies operating in the fields of space technology, communications, cloud computing, and artificial intelligence are no longer merely external service providers. In many contemporary conflicts, they have become integral components of the critical infrastructure that underpins military operations. Commercial satellites provide persistent observation, satellite communication networks enable connectivity, cloud platforms store and process vast volumes of data, artificial intelligence accelerates analysis, and geospatial firms transform raw information into actionable maps, reports, and intelligence products.

This evolution has placed private companies in an unprecedented position. They are neither states nor military forces, yet they can sig- ➤



» Images are now being used to reinforce political narratives, deny responsibility, exaggerate losses, conceal damages, or steer public opinion towards a particular interpretation.

» nificantly influence a military's ability to observe, communicate, and operate. They are not humanitarian organisations, yet their services can empower journalists, researchers, and human rights groups to document violations and increase transparency. Nor are they necessarily parties to a conflict, yet their decisions—whether to release, delay, restrict, or withhold data and services—can directly affect the conduct of military operations.

At the heart of this transformation lies the challenge of strategic interdependence. When the services of a private company become essential to the operations of a state or a belligerent actor, what begins as a commercial relationship can evolve into a strategic one. Companies may be compelled to modify their services, respond to government pressure, comply with regulatory requirements, or navigate legal and reputational risks. In all cases, the availability—or disruption—of their services can become a factor in the broader calculations of war.

This reality has given rise to a new form of hybrid competition. Military advantage is no longer determined solely by control of traditional military

platforms. Increasingly, it depends on control of the networks that enable those platforms to function: communications, navigation, data storage, analytics, and information distribution. Actors capable of disrupting, degrading, restricting, or manipulating these networks may achieve significant strategic effects without engaging in direct military confrontation. The issue becomes even more sensitive when commercial providers maintain defence or government contracts. A company that supplies satellite imagery to universities, researchers, or media organisations may simultaneously provide services to military or intelligence agencies. Such dual roles raise important questions regarding neutrality, transparency, conflicts of interest, and the extent to which commercial decision-making can remain independent in times of conflict.

More fundamentally, they raise a broader question: can commercial actors whose services have operational military significance remain entirely outside the legal and political framework of war?

The growing integration of private companies into military ecosystems

does not automatically make them parties to a conflict. It does, however, complicate their legal and ethical position. The closer a company's services move towards supporting a specific military operation, the greater the need to assess both the nature of the service and the context in which it is used. Conversely, when those services remain within the realm of public dissemination, post-conflict documentation, research, or broad situational awareness, they remain more closely aligned with legitimate civilian activity. For this reason, the decisive factor is not the existence of the imagery or service itself, but rather its function, timing, intended audience, and degree of integration into military action. A publicly available image released for general awareness is fundamentally different from a tailored intelligence product delivered to support a specific operational objective.

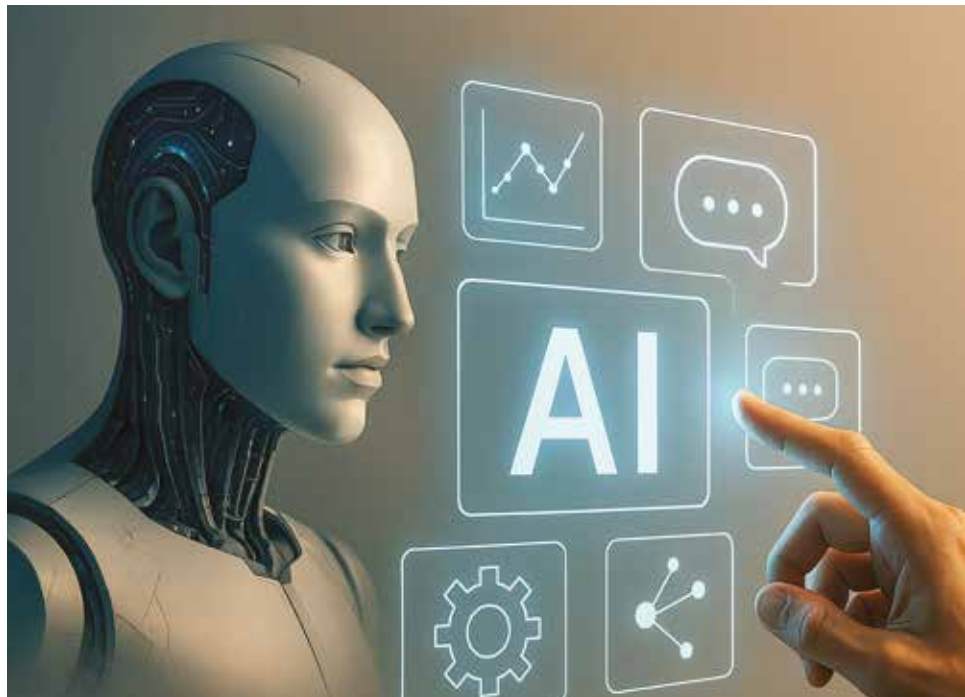
In this sense, commercial companies have emerged as intermediary actors in contemporary warfare. They operate at the intersection of state authority and market forces, security and transparency, civilian services and military support, commercial interests and public responsibility. This unique po-

sition makes them part of the broader equation of modern conflict—even when they do not seek such a role. As a result, their decisions increasingly carry consequences that extend far beyond the boundaries of a commercial contract or a technical service, influencing not only the flow of information but, in some cases, the conduct and outcomes of war itself.

The Crisis of Trust in Commercial Satellite Imagery: Another Dimension of the Militarisation of Geospatial Data

While commercial satellite imagery has significantly enhanced the ability to uncover facts on the battlefield, it has also become a central element in the contest over truth itself. Satellite images are increasingly employed to reinforce political narratives, deny responsibility, amplify perceived losses, conceal damage, or influence public opinion towards a preferred interpretation of events. In the age of artificial intelligence, the challenge extends far beyond the misinterpretation of authentic imagery. It now includes the creation of highly convincing synthetic images and the manipulation of genuine ones in ways that are often difficult to detect in real time.

The influence of commercial satellite imagery stems largely from its appearance of objectivity. Captured from space and seemingly detached from human bias, such imagery often carries an inherent sense of credibility. Yet this perception can be deceptive. Images do not speak for themselves; they require selection, framing, annotation, contextualisation, comparison, and interpretation. The actor presenting the image frequently shapes the narrative through which it is understood. Consequently, the struggle is no longer centred solely on the image itself, but increasingly on the interpretation that accompanies it. Even authentic imagery can become a tool of misinformation when removed from its original context, attributed to the wrong location or time, or linked to unsupported conclusions. Likewise, manipulated or AI-generated imagery can spread rapidly across digital platforms before experts have the opportunity to verify its authenticity. The resulting harm extends beyond the circulation of false



» Artificial intelligence threatens not only to generate fabricated imagery but also to produce flawed interpretations of authentic data.

information. It erodes confidence in visual evidence more broadly, making it increasingly difficult to distinguish fact from fabrication.

This creates a particularly troubling paradox. As artificial intelligence becomes more capable of generating realistic imagery, it also becomes easier for those accused of misconduct or violations to dismiss authentic evidence as fake. Claims of manipulation can serve as a convenient political defence, regardless of the validity of the underlying evidence. In this way, visual disinformation produces two mutually reinforcing effects: the creation of false imagery and the erosion of trust in genuine imagery.

Addressing this challenge requires the development of more rigorous standards and methodologies for visual verification. High-resolution imagery or a reputable provider can no longer be viewed as sufficient guarantees of credibility. Verification must encompass the image's source, acquisition date, metadata, chain of custody, geospatial consistency, correlation with other sources, and the possibility of manipulation or synthetic generation. Technical expertise must also be com-

bined with operational awareness and political and military context, as imagery without context can easily lead to incomplete or misleading conclusions.

Artificial intelligence presents another layer of risk. Beyond generating fabricated imagery, it can also produce flawed interpretations of authentic data. Algorithms may incorrectly identify locations, patterns, or changes, and these inaccuracies can subsequently influence intelligence assessments, political decisions, or military planning. As a result, algorithmic accountability has become inseparable from the credibility of the imagery itself, while the integrity of the entire data chain has become as important as the reliability of the visual evidence.

From Imagery to Targeting: Legal and Ethical Challenges

Commercial satellite imagery raises a fundamental legal and ethical question: when does imagery remain a legitimate civilian activity, and when does it begin to contribute to hostilities? International humanitarian law distinguishes between civilians and combatants, as well as between civilian infrastructure and military objectives. Yet these distinctions





» Commercial satellite imagery raises an important legal question: when does an image remain a legitimate civilian activity and when does it approach participation in hostilities?

» become increasingly difficult to apply when civilian companies provide imagery or analytical services that may support military operations.

Not all commercial satellite imagery constitutes military assistance. Publicly available imagery, post-strike documentation, humanitarian assessments, and journalistic investigations generally remain within the sphere of legitimate civilian activity. However, the provision of recent, tailored imagery to a belligerent party for the purpose of facilitating a specific strike or enhancing targeting accuracy enters a far more complex legal domain. In such circumstances, the imagery may become integrated into the conduct of hostilities or the direct preparation for them.

This distinction highlights the difference between imagery as documentation and imagery as an operational service. A satellite image released publicly days after an event differs fundamentally from imagery commissioned for a specific location, collected at a specific time, analysed for a specific client, and delivered in support of an ongoing military operation. The greater the degree of customisation, immediacy, and operational relevance, the closer commercial support moves towards the

legal debate surrounding direct participation in hostilities.

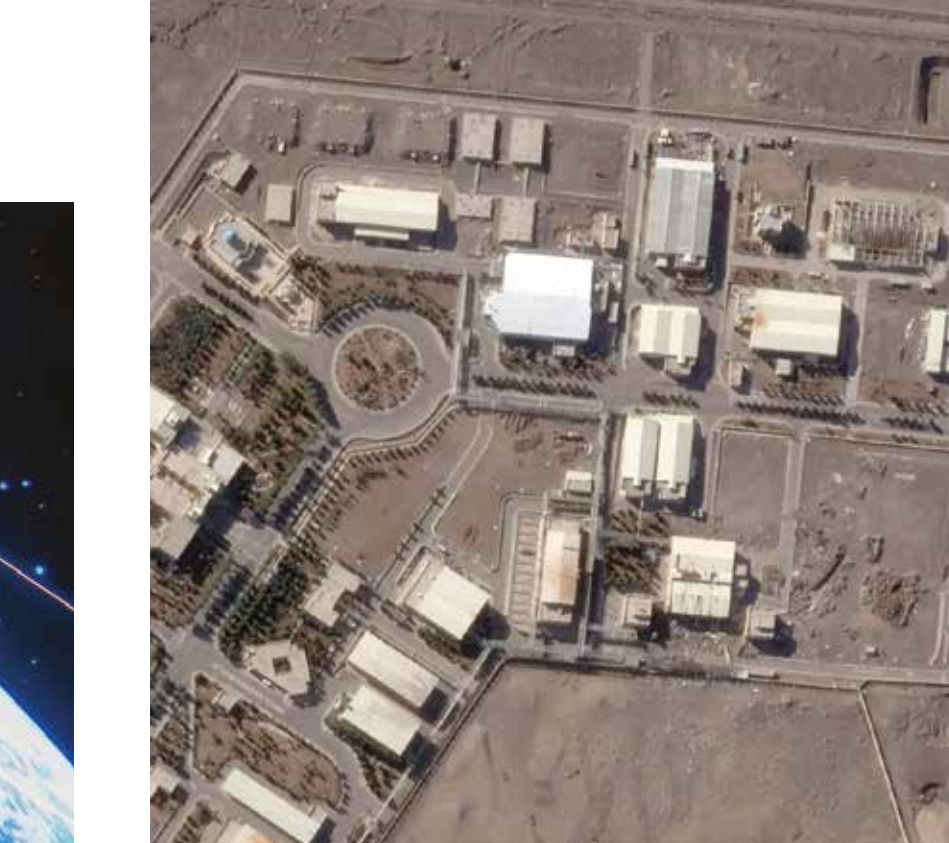
The issue extends beyond individuals to encompass infrastructure and technical systems. Employees of commercial firms generally retain civilian status, yet questions may arise regarding ground stations, processing centres, satellites, cloud networks, or data interfaces if they make an effective contribution to military operations and their disruption would provide a definite military advantage. Nevertheless, this does not mean that every satellite, server, or commercial facility automatically becomes a lawful military objective simply because it possesses some military utility.

The challenge lies in the inherently dual-use nature of commercial systems. The same infrastructure may simultaneously serve businesses, journalists, researchers, humanitarian organisations, civilian agencies, and military users. Any military action directed against such systems must therefore comply with the principles of distinction, proportionality, and precaution. Disrupting a commercial network may affect civilian populations, humanitarian activities, and the international community's ability to monitor and verify the consequences of conflict.

Potential military value alone cannot serve as a blanket justification for targeting commercial infrastructure.

An equally significant concern is the risk of misclassification. Treating all forms of commercial support as military threats could dangerously expand the range of potential targets and undermine civilian protections. Conversely, assuming that all commercial activity remains protected regardless of its operational role could enable private companies to become instruments of warfare without adequate accountability. The key consideration, therefore, is not the commercial nature of the service itself, but its function, timing, intended user, and operational context.

In this regard, contemporary conflicts may not necessarily require entirely new legal frameworks as much as they require a more precise application of existing principles. The critical questions are not whether imagery is commercial or military in origin, but how it was used, who received it, when it was provided, whether it was publicly available or specially commissioned, and whether it contributed to general situational awareness or directly supported a specific hostile act. These factors ultimately determine the legal and



» The future of wars will be determined by who owns the image, who controls its flow, who can interpret it, when it is seen, and when it is hidden.

ethical implications associated with commercial satellite imagery.

A framework of responsible governance should rest on three complementary pillars. First, commercial providers must establish clear standards governing access, dissemination, and delivery timelines. Second, governments must maintain robust licensing and oversight mechanisms for private-sector actors operating in this increasingly strategic domain. Third, the international community must work towards more consistent norms and regulatory frameworks capable of preventing geospatial data from becoming an unrestricted instrument of military targeting.

Conclusion

The future of warfare will be shaped not only by who possesses the most advanced weapons, but also by who controls the image, manages its flow, interprets its meaning, and decides when it is revealed—or withheld. In an era defined by the convergence of commercial satellites, artificial intelligence, digital platforms, and cloud computing, the struggle for visibility has become inseparable from the struggle for power, influence, and truth. The central challenge is neither to prohibit commercial satellite imagery nor to

permit its unrestricted use. Rather, it is to establish a framework of responsible governance capable of distinguishing between commercial, humanitarian, and military-operational applications; between post-strike documentation and real-time targeting support; and between transparency that promotes accountability and transparency that creates security vulnerabilities.

Achieving this balance requires clearer responsibilities for commercial providers, more effective oversight by states, and more stable international norms governing the use of geospatial data during armed conflict.

Ultimately, the militarisation of geospatial data imposes a new responsibility on governments, private companies, journalists, researchers, and international organisations alike: to preserve the right to observe without transforming it into an instrument of harm, and to safeguard security without allowing it to become a justification for obscuring the truth. Between these two imperatives lies one of the defining ethical challenges of modern warfare, where managing the relationship between imagery, analysis, targeting, and accountability has become essential to protecting both human life and objective truth. ■



Treating commercial support as a military threat could dangerously expand the range of civilian targets, while assuming that commercial activities are always protected could allow private companies to become instruments of warfare without adequate accountability.

Managing the relationship between imagery, analysis, targeting, and accountability has become essential to protecting both human life and objective truth.

Sources and references:

- Paul Zgheib, Deterrence by Disruption, *Small Wars Journal*, 12.31.2025.
- Dustin J. Nicholson, How the Weak Can Beat the Strong in War at Sea, *Naval War College*, vol 57, No. 3, 2022.
- Tim Migaki, Fleet-in-Being: Can an inferior naval fleet defeat a larger one?, *fair wind and following seas*, July 18, 2021.
- John B. Hattendorf, The Idea of a «Fleet in Being» in Historical Perspective, *Naval War College Review*, Vol. 67, No. 1, 2014.
- Norman Friedman and S.C.M. Paine, Review Essay—«Spoiling Victory: How Weaker Fleets Win»: Deterrence and Denial: The Power of Fleets in Being, *Naval War College Review*, Vol. 79, No. 1, 2026.
- John D. Willingham, Kenneth Walls Jr, and Timothy Jones, *Frogmen and Fast Boats: The Future of Irregular Warfare in the Maritime Domain*, *inter populum the journal of irregular warfare and special operations*, December 15, 2025.
- Brian Glyn Williams, How the Ukrainians - with no navy - defeated Russia's Black Sea Fleet, the conversation, July 19, 2024.
- Simon Shuster, The Drone Wars: How Ukraine Beat Russia in the Battle of the Black Sea, *TIME*, Aug 26, 2024.