



Andrea Grillo
and Elio Calcagno

› War in the Age of Commercial Spacepower: Five Lessons from Ukraine

- › Commercial space architectures and services have become essential to national defence and may be regarded as legitimate targets in warfare, regardless of their providers' formal non-participation in hostilities.
- › Functional innovation in space-enabled services has enabled countries lacking sovereign space assets to derive greater operational value from space than well-established space powers.
- › Non-destructive counterspace operations are a standard feature of contemporary conflict due to the relatively low costs, reversible effects and limited escalation risks. This also favours their growing acceptance and normalisation in grey-zone scenarios.

Since its outbreak in 2022, Russia's large-scale invasion of Ukraine is rightly held as an example of the need to invest in hard deterrence and mass, including with regard to drones, air defences and artillery capabilities. Yet this war was never confined to the conventional battlefield: in fact, Moscow's aggression was marked at its outset by a cyberattack targeting the ground segment of Viasat space systems. Since then, the space domain has remained a core enabler for the effective execution of military operations. No conflict to date has witnessed such extensive use of space and counterspace capabilities by belligerents.¹ Whereas the 1991 Gulf War was framed as the "first space war", shaped by the decisive use of space-based assets, the war in Ukraine is increasingly described by analysts as the first conflict shaped by the pervasive integration of commercial space services into military operations, with some even referring to it as the first "commercial space war".² Notwithstanding the asymmetrical starting conditions – Russia as a long-established space power and Ukraine lacking sovereign orbital assets at the outset of the war – both sides have demonstrated that effective military operations are increasingly dependent upon access to, and integration of, space-enabled information and services. The conflict has underscored the extent to which the space domain

¹ Gurantz, Ron, *Satellites in the Russia-Ukraine War*, Carlisle Barracks, US Army War College Press, 2024, <https://press.armywarcollege.edu/monographs/971>.

² Erwin, Sandra, "On National Security | Drawing Lessons from the First 'Commercial Space War'", in *SpaceNews*, 20 May 2022, <https://spacenews.com/?p=127408>.

Andrea Grillo is Research Fellow for Space and Defence in IAI's "Defence, Security and Space" programme.

✉ a.grillo@iai.it

Elio Calcagno is Senior Research Fellow for Defence and Space in IAI's "Defence, Security and Space" programme.

✉ e.calcagno@iai.it



»» *Russia and Ukraine represent markedly different actors in the space domain*

has become crucial to modern warfare outcomes, and it has also exposed new dynamics of interaction and dependence between governments and private companies.

The onset of the war

Russia and Ukraine represent markedly different actors in the space domain, although both have inherited significant technical expertise from the pioneering Soviet space programme. Throughout the Cold War, Ukraine hosted several critical industrial facilities that produced satellites, launch vehicles and Soviet intercontinental ballistic missiles. Notable among these are KB Pivdenne and the State Enterprise Pivdenmash, which became Ukrainian entities after the dissolution of the Soviet Union, and today continue to contribute to US and European programmes, including the manufacture of propulsion engine blocks for the European launcher Vega.³ However, while Kyiv maintains a relatively advanced space industry that is integrated into Western programmes, it lacked sovereign space assets in orbit when the invasion began.⁴ Indeed, Ukraine relied extensively on foreign technologies and services to support its military operations, even before 2022.⁵

Russia, by contrast, entered the conflict as one of the world's leading space powers and a longstanding member of the international space community. Historically, it played a central role in cooperative ventures, most notably through its contribution to the International Space Station (ISS) programme alongside NASA, the European Space Agency (ESA), the Japan Aerospace Exploration Agency (JAXA) and other Western partners from the 1990s onwards. However, Russia's space sector has increasingly struggled to keep pace with the rapid innovation driven by the United States and China. This relative decline reflects a combination of structural constraints, including limited public funding, persistent corruption, brain drain and the absence of a dynamic private space industry.⁶ Against this backdrop, Moscow has sought to preserve its position of excellence in selected niches, particularly human spaceflight.

Russia has cultivated significant electronic warfare (EW) and cyber capabilities useful also in a counter-space capacity.⁷ Hours before the ground invasion in 2022, one of Moscow's first offensive operations targeted the Ka-Sat satellite network operated by US satellite internet service provider Viasat. Rather than striking assets in orbit, the operation took the form of a cyber denial-of-service (DoS) attack against ground-based internet modems located in Ukrainian territory, on which Kyiv's forces relied on for command, control

³ "Italian Avio S.p.A Buys 10 More Ukrainian Engines", in *Kyiv Post*, 30 April 2021, <https://archive.kyivpost.com/business/italian-avio-s-p-a-buys-10-more-ukrainian-engines.html>.

⁴ Dickey, Robin and Michael P. Gleason, "Space and War in Ukraine: Beyond the Satellites", In *Æther*, Vol. 3, No. 1 (Spring 2024), p. 20-35, <https://csps.aerospace.org/node/587>.

⁵ Marrone, Alessandro (ed.), *Russia-Ukraine War's Strategic Implications*, Rome, IAI, 2024, <https://www.iai.it/en/node/18118>.

⁶ Radin, Andrew et al., *Lessons from the War in Ukraine for Space. Challenges and Opportunities for Future Conflicts*, Santa Monica, RAND, 2025, https://www.rand.org/pubs/research_reports/RRA2950-1.html.

⁷ Cesari, Laetitia and Victoria Samson (eds), *Global Counterspace Capabilities. An Open Source Assessment*, Secure World Foundation, April 2025, <https://www.swfound.org/publications-and-reports/2025-global-counterspace-capabilities-report>.



»» *Beyond Viasat, Ukraine has relied throughout the conflict on other space services provided by foreign private companies*

and communications (C3).⁸ This attack disrupted access to the satellite communications (SATCOM) services provided by Viasat, with Ukrainian sources describing the attack as causing a “huge loss of communications in the very beginning of the war”.⁹

The effects of the cyberattack were not confined to Ukraine. They extended to tens of thousands of Ka-Sat terminals used by other customers across Europe, causing severe and indiscriminate disruptions. In Germany, approximately 5,800 wind turbines operated by Enercon were taken offline as a result of the very same attack,¹⁰ and it is unlikely that either the German company or the government had a clear view of the wider customer base relying on the same service, and thus little ability to anticipate or mitigate the cascading effects of such an attack.

Russian EW and cyber activities have affected a wide range of military functions, from radio communications between soldiers and data links connecting pilots and drones to tracking signals emitted by air-defence radar systems. They have also enabled Moscow to repeatedly disrupt and deny Ukraine’s access to Western satellite-enabled services, primarily through the jamming and spoofing of Global Positioning System (GPS) signals. As a result, in the first months of the war, Russia managed to reduce the operational effectiveness of the numerous precision-guided munitions (PGMs) supplied to Ukraine, mainly by Washington, whose long-range use was already subject to US restrictions. Indeed, the success rate of some systems reportedly fell from 55 per cent to around 6 per cent.¹¹

Ukraine’s innovative use of space-enabled services

Beyond Viasat, Ukraine has relied throughout the conflict on other space services provided by foreign private companies – such as Starlink, OneWeb, SES, Iridium, Eutelsat, Avanti, ICEYE, Planet Labs and BlackSky.¹² By integrating these commercial capabilities, Kyiv has successfully strengthened its command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities, while also combining them with intelligence and data provided by governmental space systems operated by the United States and other European partners.¹³

Satellite communications have, in particular, improved the resilience and

⁸ Vasquez, Christian and Elias Groll, “Satellite Hack on Eve of Ukraine War Was a Coordinated, Multi-Pronged Assault”, in *Cyberscoop*, 10 August 2023, <https://cyberscoop.com/?p=76278>; Calcagno, Elio et al., “Le minacce cyber ed elettromagnetiche alle infrastrutture spaziali”, in *Documenti IAI*, No. 24 | 07 (July 2024), <https://www.iai.it/en/node/18696>.

⁹ Vicens, Aj, “Top Ukrainian Cyber Official Praises Volunteer Hacks on Russian Targets, Offers Updates”, in *Cyberscoop*, 15 March 2022, <https://cyberscoop.com/?p=63163>.

¹⁰ European Space Policy Institute (ESPI), “The War in Ukraine from a Space Cybersecurity Perspective”, in *ESPI Reports*, No. 84 (October 2022), p. 6, <https://www.espi.eu/?p=3021>.

¹¹ Gall, Carlotta, and Vladyslav Golovin, “Some U.S. Weapons Stymied by Russian Jamming in Ukraine”, in *The New York Times*, 25 May 2024, <https://www.nytimes.com/2024/05/25/world/europe/us-weapons-russia-jamming-ukraine.html>.

¹² Marrone, Alessandro (ed.), *Russia-Ukraine War’s Strategic Implications*, cit.; Dickey, Robin and Michael P. Gleason, “Space and War in Ukraine”, cit.

¹³ Burbach, David T., “Early Lessons from the Russia-Ukraine War as a Space Conflict”, in *Airpower after Ukraine*, 30 August 2022, <https://www.atlanticcouncil.org/?p=555878>; Ogden, Theodora et al., “The Role of the Space Domain in the Russia-Ukraine War”, in *CETaS Commentaries*, February 2024, <https://cetas.turing.ac.uk/node/123>.



>> The impact of the space-enabled data and services provided to Ukraine has been significantly amplified by Ukrainian military policies

flexibility of Ukrainian military communications. For instance, they enabled the tele-maintenance of US and NATO weapon systems, allowing Western technicians to support their Ukrainian counterparts remotely.¹⁴ They also supported essential civilian connectivity, including internet access for hospitals and critical infrastructure. At the same time, satellite-based ISR capabilities, especially synthetic aperture radar (SAR) systems, have enhanced Ukraine's ability to accurately locate, track and target Russian forces, as well as to conduct post-strike battle damage assessments with greater precision. Beyond their operational value, these systems have also supported the identification of war crimes, the assessment of deliberate targeting and destruction of food production systems, cultural heritage sites, health facilities and educational infrastructure.¹⁵

The impact of the space-enabled data and services provided to Ukraine has been significantly amplified by Ukrainian military policies, as well as doctrines enabling a flexible approach to information-sharing across all relevant stakeholders capable of extracting operational value from it.¹⁶ The added value of space infrastructure lies not only in the data it produces, but also in how such data is distributed and used by military and government actors. The ability to receive, process and share this data with the right actors at the right time shows that simply possessing space assets is only one part of the equation. Ukraine has been able to leverage advanced software and data-processing solutions to fully exploit the operational advantages of space-enabled information on the battlefield, reducing the time needed to deliver actionable intelligence to soldiers from days to just minutes since the start of the war.¹⁷ For instance, with about 70,000 terminals,¹⁸ Ukrainian forces rely on Starlink connectivity to integrate commercial drones into a real-time kill-chain, using video conferencing tools to stream battlefield footage directly to artillery units for fire correction.¹⁹ Ukrainian forces have thus demonstrated an ability to innovate in the employment of space-based capabilities, often using existing and readily available technologies, showing how functional innovation can be just as important as technological innovation. Furthermore, a more decentralised, distributed and resilient approach to command and control (C2) has allowed them to improve the coordination of ground forces, winning them a relative operational advantage over Russia.

Russia's strategic and operational space posture

The Ukrainians have demonstrated a remarkable capacity for adaptation and innovation, largely driven by their numerical disadvantage and the consequent need to maximise the effectiveness and efficiency of limited resources. This

¹⁴ Tucker, Patrick, "US Soldiers Provide Telemaintenance as Ukrainians MacGyver Their Weapons", in *Defense One*, 18 September 2022, <https://www.defenseone.com/technology/2022/09/us-soldiers-provide-telemaintenance-ukrainians-macgyver-their-weapons/377306>.

¹⁵ Dickey, Robin and Michael P. Gleason, "Space and War in Ukraine", cit.

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ Radin, Andrew et al., *Lessons from the War in Ukraine for Space*, cit.

¹⁹ Skove, Sam, "How Elon Musk's Starlink Is Still Helping Ukraine's Defenders," in *Defense One*, 1 March 2023. <https://www.defenseone.com/technology/2023/03/black-swan-starlinks-unexpected-boon-ukraines-defenders/383514>.



»» **Moscow became over-reliant on Starlink terminals smuggled from neighbouring countries**

approach has not been mirrored by Russia, which instead has remained constrained by the highly rigid decision-making hierarchies typical of a larger and more structured armed forces operating within a strongly centralised and authoritarian state. This limitation is particularly evident in its highly vertical organisation of military communications, characterised by centralised C2 structures, which tend to reduce the overall operational effectiveness of battlefield communications compared to a network-centric approach. In this context and considering an invasion force estimated at up to 190,000 personnel in 2022, deployed across five offensive axes, Russia's constrained bandwidth capacity, together with the limited availability of satellite communication channels and terminals, proved insufficient to ensure the effective operational coordination of deployed forces.²⁰ In fact, Moscow became over-reliant on Starlink terminals smuggled from neighbouring countries to provide units with adequate communications in the field. Yet, starting in February 2026, Moscow's unauthorised use of Starlink has been disrupted. Terminals operating in Ukraine were deactivated, except for those included on a "whitelist" approved by the Ukrainian Defence Ministry, thus severely reducing Russia's access to the internet on the battlefield and hampering its troops' ability to coordinate and conduct operations.²¹

The war has also sped up the longer-term erosion of Russia's space power. Despite retaining many Soviet-era legacy assets, its space programme has progressively declined due to chronic underfunding and corruption, undermining its ability to deploy new satellites.²² For instance, the revisit times of its ISR satellites, both SAR and optical, are insufficient to support effective use in dynamic military operations. Russia's PGM arsenal, which is a highly-valuable asset on the relatively static front in Ukraine, has likewise been limited in number, poorly tested and of reduced effectiveness because it depends on the degraded and unreliable Russian Global Navigation Satellite System (GLONASS).²³ The strain of war in Ukraine combined with Western sanctions has exacerbated these structural weaknesses, diverting even more resources away from innovation. As a result, the relative leadership position inherited from the Soviet space programme has eroded at increasing speed. The decline in demand for Russian Soyuz launch services has contributed to deep cuts in its space programme.²⁴ Moreover, unlike Ukraine, Russia has been unable to officially draw on an extensive network of private space companies in allied states,²⁵ and, like several European countries, it depends to a large extent on public funding to sustain its space sector.

²⁰ Luzin, Pavel, "Russia's Space Satellite Problems and the War in Ukraine", in *Eurasia Daily Monitor*, Vol. 19, No. 76 (24 May 2022), <https://jamestown.org/?p=92811>.

²¹ Adams, Paul, "Musk Cuts Starlink Access for Russian Forces - Giving Ukraine an Edge at the Front", in *BBC News*, 9 February 2026, <https://www.bbc.com/news/articles/c0q3ndj7052o>.

²² Radin, Andrew et al., *Lessons from the War in Ukraine for Space*, cit.

²³ Ibid., p.19.

²⁴ Feldscher, Jacqueline, "Russia Pursues New ASAT Capability amid Declining Space Program", in *Payload Space*, 20 February 2024, <https://payloadspace.com/?p=18452>.

²⁵ The Russian army made unauthorised use of Starlink terminals smuggled into Russia from other countries until SpaceX curtailed access in February 2026. See Kolomychenko, Maria, "How Will the Loss of Starlink and Telegram Impact Russia's Military?", in *Carnegie Politika*, 23 February 2026, <https://carnegieendowment.org/russia-eurasia/politika/2026/02/russia-starlink-telegram-shutdown>.



>> The direct support provided by international commercial suppliers to the Ukrainian Armed Forces and governments has highlighted both benefits and vulnerabilities

Five emerging trends and lessons from the conflict

Over four years of conflict in Ukraine have shed light on the deep and pervasive integration of space assets and services into a large-scale, prolonged and high-intensity multi-domain war. The conflict marks a significant evolution in the role of space in conventional war; not so much in terms of evolving technologies in the face of changing threats, as in terms of how existing instruments have been integrated into kill chains and C4ISR structures. Moreover, the direct support provided by international commercial suppliers to the Ukrainian Armed Forces and governments has highlighted both benefits and vulnerabilities of this increasingly pervasive reality. Five lessons particularly relevant for Europe can be drawn from the Russia-Ukraine war.

First, the conflict has shown that it is not necessary to be a space power in order to benefit from and effectively exploit space-enabled information and data. What proved decisive has been the ability to exploit this vast volume of information through effective processing and distribution systems, thereby minimising the delay between data acquisition and operational utilisation.

At the same time, a similar logic applies to the denial of space-based support to military operations. It is not necessary to be a space power or possess indigenous space capabilities and access to space to undermine adversaries' access to space assets and services.

Second, rather than through kinetic attacks, space infrastructure – including space, ground or link segments – is increasingly targeted through EW and cyber operations, which have significantly lower barriers to entry and overall costs.²⁶ This trend reflects and exploits the growing normalisation and acceptance of non-destructive attacks as a standard feature of contemporary conflict.

Third, the Russian-Ukrainian conflict clearly illustrates the need for those with the financial and technical means to master access to space to avoid excessive dependence on foreign countries or commercial suppliers. While reliance on a plurality of satellite intelligence sources allowed Ukraine to avoid dependence on a single provider, the same was not true for SATCOM.²⁷ The service that Starlink offered to Ukraine at the beginning of the invasion became fundamental, both for military operations and civilian infrastructure. This dependency gave the chief executive officer of a foreign commercial company, Elon Musk, a degree of direct influence over the conflict rarely observed in similar contexts, including the ability to determine when and where the service could be used.²⁸ Foreign companies, subject to limited control by client states, could indeed leverage their position and impose conditions on continued access to essential services. Furthermore, while the initial provision of Starlink to Ukraine without a dedicated contract or government oversight was probably a unique circumstance driven by the extreme urgency dictated by a full-scale invasion, it nevertheless highlighted the importance of developing at least

²⁶ Swope, Clayton et al., "Space Threat Assessment 2025", in *CSIS Reports*, April 2025, <https://www.csis.org/node/115963>.

²⁷ Radin, Andrew et al., *Lessons from the War in Ukraine for Space*, cit.

²⁸ Pollet, Mathieu, "Ukraine Is Stuck with Musk's Starlink for Now", in *Politico EU*, 7 April 2025, <https://www.politico.eu/?p=6334413>.



»» *The Viasat episode highlights a double vulnerability associated with the use of commercial solutions for critical national infrastructure and services*

formal and enforceable agreements with future commercial space partners.²⁹

A similar reflection should extend to the integration of foreign governmental space services into military C4ISR systems. States providing such space systems or services to third countries retain the sovereign right to grant or deny access, based on whether their use is compatible with their own national security interests.

The contrast between Ukraine's excessive, albeit necessary, dependence on the private sector and, conversely, Russia's inability and longstanding reluctance to rely significantly on commercial services also demonstrates how a proper balance between models at the two ends of the spectrum is essential to ensure a country's secure and sustainable access to orbit and cutting-edge space technologies.³⁰

Fourth, the growing dependence of advanced societies on space systems, even outside military contexts, requires a holistic approach to the resilience of critical infrastructures that directly or indirectly rely on them. The Viasat episode highlights a double vulnerability associated with the use of commercial solutions for critical national infrastructure and services. First, it underscores the risk of relying on commercial providers that may lack the security architecture required to meet the operational requirements of the Armed Forces. Second, it highlights the importance of mapping dependencies and end-users' networks associated with a given space service, in order to prevent unintended disruptions to critical infrastructure, as occurred in the case of the German energy network at the dawn of Russia's full-scale invasion.

Finally, for foreign space operators, the Ukraine case also underlines that formal non-participation in a conflict does not itself guarantee protection from being targeted in large-scale offensive operations. Indeed, given the growing reliance on the commercial sector for critical governmental services during conflicts, Russian officials have repeatedly argued that they would consider commercial companies as legitimate targets.³¹ In a world where national security, commercial companies and infrastructure are increasingly interconnected, the line between civilian and military targets becomes harder to draw. In this context, as private companies play an ever-growing role in enabling the strategic capabilities of entire countries, it is also increasingly challenging to discern those capabilities from a complex web of international supplies, dependencies and vulnerabilities.

²⁹ Radin, Andrew et al., *Lessons from the War in Ukraine for Space*, cit., p. 12.

³⁰ Vidal, Florian and Roman Privalov, "Russia in Outer Space: A Shrinking Space Power in the Era of Global Change", in *Space Policy*, Vol. 69 (August 2024), Article 101579, <https://doi.org/10.1016/j.spacepol.2023.101579>.

³¹ Swope, Clayton et al., *Space Threat Assessment 2025*, cit., p. 33.

The Istituto Affari Internazionali (IAI) is a private, independent non-profit think tank, founded in 1965 on the initiative of Altiero Spinelli. IAI seeks to promote awareness of international politics and to contribute to the advancement of European integration and multilateral cooperation. Its focus embraces topics of strategic relevance such as European integration, security and defence, international economics and global governance, energy, climate and Italian foreign policy; as well as the dynamics of cooperation and conflict in key geographical regions such as the Mediterranean and Middle East, Asia, Eurasia, Africa and the Americas. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*AffariInternazionali*), two book series (*Trends and Perspectives in International Politics* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via dei Montecatini, 17
I-00186 Rome, Italy
T +39 06 6976831
www.iai.it



Latest IAI Briefs

Editor: **Lorenzo Biondi** (l.biondi@iai.it)
ISSN 3103-4071 | DOI 10.82088/IAIbrief2653

26 53	Andrea Grillo and Elio Calcagno, <i>War in the Age of Commercial Spacepower: Five Lessons from Ukraine</i>
26 52	Federica Marconi and Ettore Greco, <i>US and European Visions of Global Governance</i>
26 51	Francesca Maremonti, <i>Transatlantic Critical Materials Supply Chains: Rock-Solid?</i>
26 50	Beniamino Irdi, <i>Rethinking European Security When the American Anchor Slips</i>
26 49	Stefan Ristovski, <i>Between Geopolitics and Enlargement: Reconfiguring Pre-Accession Assistance in the Next EU Budget</i>
26 48	Federica Marconi, <i>Breaking the "Walled Garden": The Challenge of Interoperability under the EU's Digital Markets Act</i>
26 47	Matteo Bursi and Ettore Greco, <i>The Digital Euro at a Critical Juncture</i>
26 46	Ayşe Betül Çelik, <i>Women Negotiators' Strategies to Overcome Gender Inequality at the Table</i>
26 45	Anton Peez, <i>The Growing Transatlantic Sanctions Divide</i>
26 44	Alicia García Herrero, <i>China's Building Blocks for an Alternative Monetary System</i>