Proceedings of 5th International Conference CNDGS'2026
ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/10.47459/cndcgs.2026.87**

Protective Measures Concept for Civilian Space Assets

Ondrej BYRTUS[1]*, Tomas DOBROVOLNY[1],

[1]Department of Intelligence Support, University of Defense, Kounicova 65, 662 10 Brno-stred, Czech Republic

*Correspondence: * ondrej.byrtus@unob.cz*

Abstract

This article addresses the issue of protecting civilian space assets that are utilized by states, and particularly by armed forces. It examines the unique characteristics of operating in the space environment, importance of these space assets, the concept of the military use of space, and the strategies applied in the United States to ensure the protection of such assets. The authors propose five protective measures: war risk insurance; physical protection of the ground segment; in-orbit physical protection; deterrence; and threat information sharing.

KEY WORDS: *civilian space assets; national defence; satellites; space environment; infrastructure protection.*

Citation: Byrtus, O., Dobrovolny, T. Protective Measures Concept for Civilian Space Assets. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959, https://doi.org/10.47459/cndcgs.2026.87

1. Introduction

Space-based technologies have evolved from scientific tools into essential infrastructure – the virtual backbone of modern civilization [1]. Their importance spans telecommunications, research, defence, agriculture, finance, crisis response etc [2,3]. Space environment today is being characterized as congested, contested and competitive [4,5].

Civilian satellites play an emerging role in security environment. Partnerships such as that between Finnish Synthetic Aperture Radar satellite producer ICEYE and Germany's Rheinmetall [6], or ICEYE's contracts with the Polish Armed Forces, illustrate this trend [7]. The Russia-Ukraine conflict further proves their significance as Ukraine obtained satellite imagery covering over 40 million km^2 of Russian territory within two weeks. SpaceX's Starlink network underpins Ukraine command and control with impact on targeting, cutting the procedure from 20 minutes to 60 seconds [8]. Such satellites also support crisis management, providing communication, navigation, and situational awareness in all disaster management phases [9,10].

Importance of such satellites is recognized by multiple doctrines and national strategies. The United States *Space Force Doctrine Document 1* notes that national prosperity and security depend on satellites, with over half of United States' infrastructure being reliant on them and promotes integrating commercial space data, products and services (DPS) into space forces' structure [11]. Sweden´s defense and security strategy for space underlines the importance of national satellite building and launching capabilities, including supply chain security [10]. France's National Space Strategy 2025-2040 also highlights dual-use satellite services [12], and Czech Republic's strategic document declares that space assets are vital to its economics, state functionality and defense measures [13].

Given this, civilian satellites have become crucial to national security and thus high-value targets. The Russian Federation has repeatedly stated that the use of (mostly commercial) satellites to support Ukrainian military activities would render them as military targets [14,15]. Threats may arise not only in wartime but also in peacetime, through diverse actors, motives and domains of attack.

These assets are protected by international law or in case of war by law of armed conflict [16]. Military satellites and satellites that are important for national interests are often protected by space command entities, however there is a lack of protection for civilian satellites. Thus, protective measures for the space segment are becoming increasingly important, as the spectrum of actors capable of operating and influencing this domain continues to expand.

2. Methodology and Limitations

This paper employs a qualitative methodology based on analysis and synthesis of publicly available information, academic publications, legal documents, policy papers, and national strategic documents. The paper identifies key trends, risks, dependencies, and existing approaches to the protection of civilian space assets. Based on the findings, authors propose protective measures for the civilian space assets.

Limitations:

- Information on protecting critical national security assets is scarce or too general, which limits in-depth analysis.
- The paper focuses mainly on the United States' approach to civilian actors within the space industry due to its tailored character.

3. Challenging Nature of the Space Environment

This article adopts the now widely used characterization of outer space as congested, contested, and competitive as an analytical framework for describing the contemporary space security environment. This framing was first articulated in the 2011 United States "*National Security Space Strategy*", which identified three mutually reinforcing trends: the increasing congestion of orbit caused by the growth of space objects and debris; the contested character of space resulting from the development of counterspace capabilities; and the increasingly competitive nature of the domain as more state and non-state actors gained access to space-based technologies [17]. This way of framing the contemporary evolution of the space domain is also used, for instance, in the United Kingdom's 2022 Defence Space Strategy [18].NATO's approach to space [5] various space-related reports, news, as well as in scientific papers.

Within the growing trend of deploying satellites into orbit, the risk of "congestion" naturally arises over time. The year 2019 marked a turning point, when SpaceX began utilizing reusable Falcon 9 rockets, thereby drastically reducing the costs of "transportation", to position the Starlink mega constellation [19]. Figure 1 shows the number of objects launched into space annually. According to the source, these figures do not include only satellites, but also probes, landers, crewed spacecraft, and space station flight elements launched into Earth orbit or beyond [20]. Today, the number of active satellites is around 14,200 [21]. It is important to emphasize that active satellites represent only one part of the orbital environment. In addition to functioning spacecraft, orbit is also filled with non-functional satellites, spent rocket stages, mission-related objects, and debris. These objects may travel at speeds of several kilometers per second. Even relatively small fragments can therefore possess enough kinetic energy to damage or destroy parts of a satellite. The greater the number of objects in orbit, the higher the probability of collision, which may then generate additional debris and further increase the risk of collision for other space assets [22].

Another factor contributing to the congestion problem is the conduct of direct-ascent anti-satellite tests. These tests have so far generally been carried out against a state's own satellite, often a non-functional one. Nevertheless, the debris cloud created by such event can spread through the orbital environment and create risks for all actors in space. Although political and diplomatic efforts have been made to limit or delegitimize destructive direct-ascent anti-satellite testing, there is currently no universal binding treaty that specifically prohibits such activities [23]. According to available Space Situational Awareness (SSA) data and statistical models, the orbital environment is estimated to contain approximately [21]:

- 54.000 objects greater than 10 cm (including active payloads),
- 1.2 million objects from 1 cm to 10 cm,
- 140 million objects from 1 mm to 1 cm.

The proliferation of satellites and the growing dependence of states, armed forces, and societies on space-based DPS also contribute to the contested character of space. As space systems become increasingly important for communication, navigation, intelligence, surveillance, reconnaissance, targeting, weather services, and command and control, they also became more attractive targets for actors seeking to weaken one's capabilities [24].

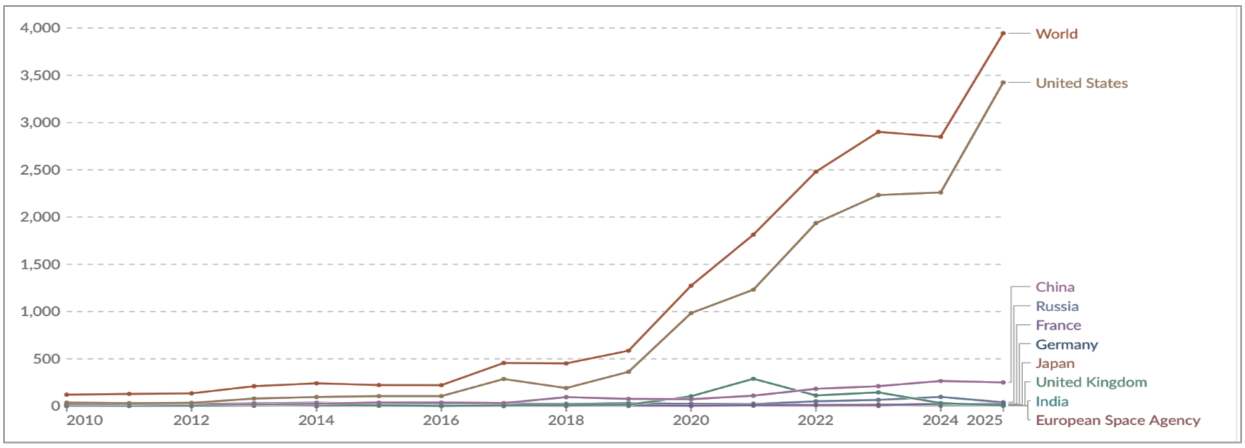

Fig. 1. Number of objects launched into space annually [20]

The contested aspect of space distinguishes it fundamentally from the traditional physical domains of land, sea, and air. Unlike these domains, space lacks defined geographical boundaries, and its systems are omnipresent. The persistent integration of military and civilian infrastructures further complicates this landscape, making the distinction between civilian and military utility blurred. Consequently, the domain is not only contested during open armed conflict but remains a zone of constant friction in peacetime, characterized by cyber operations, electromagnetic interference, and testing of counterspace capabilities [25]. The strategic importance of space is visible in the policies of major space powers such as the United States [11], China [26], and Russia [27]. These states increasingly treat space as an important component of national power [28] as a domain relevant to deterrence, intelligence gathering, military effectiveness, economic development, and international prestige. The designation of space as a "warfighting domain" [29] further illustrates its contested character. Destructive anti-satellite tests conducted by the United States, China, Russia, and India can also be interpreted not only as technical demonstrations, but as strategic signals showing that these states possess capabilities that could be used against space assets in a crisis or conflict. The war in Ukraine illustrates the contested character of space particularly clearly. Civilian satellites from various countries have supported Ukrainian forces by providing DPS that enhance communication, intelligence, command and control, situational awareness, and targeting processes. Their purpose is supportive rather than kinetic: they enable or enhance military activity rather than directly producing effects on the battlefield. Nevertheless, this enabling role complicates the distinction between civilian and military objects. The Russian Federation has repeatedly expressed its position that commercial satellites used to support Ukrainian military activities may be considered military targets [14,30].

The competitive aspect of the space domain can be observed on both civilian and national levels. On the civilian level, private firms compete to provide space-based DPS to customers, including individuals, other private companies, state institutions, and military organizations. Their primary goal is usually to generate profit, recover investment costs, and remain competitive in the market [31]. According to data from 2021, there were more than 10,000 civilian companies operating in the global space sector [32]. However, this figure should be treated as indicative rather than definitive, as the sector expands rapidly. For example, according to data from 2023, approximately 1,590 civilian companies were operating in the space sector in the United Kingdom alone [33]. The services provided by commercial space companies are diverse and may include, among others [34,35]:

- Space data as a service,
  - Automatic Identification System data for Maritime purposes,
  - Earth observation data (Electro-optical, Synthetic Aperture Radar, Multispectral, …),
- Internet access,
- Television broadcasting.
- satellite communications and related services.

This commercial competition increases the availability and flexibility of space-based services. At the same time, it also creates a more complex environment of ownership, dependency, contractual relations, and vulnerabilities. Civilian providers may become important for state functions or military operations even though their assets remain privately owned and primarily commercially operated.

At the national level, competition in space is not primarily about profit generation. It is more closely connected to strategic autonomy, technological capability, access to orbital positions, supply-chain security, and the ability to secure reliable space-based DPS during crises or conflicts. Ambition for limited positions in geostationary orbit (GEO), where orbital slots and frequency coordination is problematic may serve as a national competition example [35]. Such competition can also be observed in the renewed interest in the Moon, Mars, and other celestial bodies. During the 1960s and 1970s, lunar exploration was closely connected to prestige and great-power rivalry [36]. After the successful Moon landings, such ambitions declined for several decades, but in recent years they have again become visible in national space strategies and long-term exploration plans. In this context, competition is not only economic or military, but also symbolic, technological, and political [37].

Taken together, these developments show that space is challenging environment. Orbital congestion increases the risk of collision and complicates the long-term sustainability of space activities. The contested character of space reflects the growing ability and willingness of actors to disrupt, degrade, or threaten space systems. The competitive character of the domain increases the number of actors, assets, services, and dependencies involved. These trends are especially important for civilian satellites, because such assets increasingly provide services relevant to national security while remaining exposed to risks that are difficult for individual operators to manage alone. Space can therefore be understood as a fragile, complex, and strategically significant environment in which the protection of civilian assets requires increasing attention.

4. Space Assets as a Critical Infrastructure and Military Dependence on Civilian Space Assets Providers

Contemporary national security strategies increasingly portray space systems as indispensable enablers of state power, economic prosperity, and societal resilience rather than niche technical assets. Across allied states, official doctrines and strategies converge on several core themes: space-based services underpin critical infrastructure and daily civilian life; modern armed forces and deterrence postures depend on assured access to space support; and autonomous access to, and freedom of action in, space is increasingly framed as a question of national and European sovereignty [5].

Space is also increasingly recognized as part of critical infrastructure. Within the European Union (EU), space is identified as a critical sector under the Critical Entities Resilience (CER) and Network and Information Security 2 (NIS2) Directives. The EU's CER Directive strengthens the physical resilience of critical entities, while the NIS2 Directive strengthens cybersecurity requirements for essential and important sectors. EU member states are required to adapt these directives into their national laws. However, the coverage of the space sector in these instruments is not unlimited. It applies mainly to ground-based infrastructure owned, managed, or operated by member states or private parties that support the provision of space-based services, and to satellites used for telecommunications services [38]. This approach is visible, for example, in France, where space is included among the sectors of critical importance within the technological area of responsibility, providing "*the essential goods and services forming the backbone of French society and its way of life.*" [39] A similar approach can be observed in the United Kingdom, although it is no longer a member of the EU, where space is included within the United Kingdom's Critical National Infrastructure. It refers to infrastructure assets whose loss or compromise could have a major detrimental impact on the availability, integrity, or delivery of essential services, national security, national defense, or the functioning of the state [40] UK also specifies two key components of space infrastructure– ground infrastructure and orbital infrastructure [41] Recognition as critical infrastructure usually implies that the relevant sectors, operators, or services are (usually legally) expected to meet higher standards of security, resilience, continuity planning, and crisis management. These requirements are intended to make essential services more resistant to unexpected adverse events, whether caused by natural hazards, technical failures, cyber incidents, or hostile action. In the case of space systems, however, this recognition remains uneven. Some frameworks focus primarily on terrestrial infrastructure and service continuity, while the protection of satellites themselves may be less clearly defined.

Outside Europe, the United States divides its critical infrastructure into sixteen sectors, but space infrastructure is not explicitly designated as a separate critical infrastructure sector. At the same time, space-related services are indispensable to the functioning of these sectors. All sixteen sectors depend in some way on Position, Navigation, and Timing, while homeland security relies heavily on space systems to provide information and communications for mission success [42]. This illustrates an important point: even if space is not formally listed as an independent critical infrastructure sector, it may still function as a foundational enabler of other critical sectors.

The growing importance, accessibility, and commercialization of the space market have also encouraged armed forces and security institutions to use services provided by a broad range of private actors [43]. According to RAND Corporation, the civilian space services most relevant to military mission requirements include satellite communications, remote sensing, weather data, Position, Navigation, and Timing, and space domain awareness [44]. Cooperation between the civilian space industry and armed forces has therefore created both new opportunities and new risks.

For armed forces, commercially available space services offer flexibility. Whether they serve as the sole source of a given capability or as a supplement to sovereign military systems, civilian providers can offer a wide range of options. Depending on the character and development of an operation, armed forces may require very high-resolution remote sensing with a revisit time of several days, all weather imagery through Synthetic Aperture Radar sensors, or a combination of multiple assets and data sources [44] If procurement, funding, and command arrangements allow military users to request such services in a timely manner, and if civilian providers can respond dynamically, these partnerships may support operational adaptability, possibly enhancing mission command philosophy. For private companies, cooperation with armed forces creates opportunity for lucrative contract and may provide reputational benefits, particularly when their services are seen as contributing to national security or allied defence objectives [45].

At the same time, reliance on civilian space-based DPS creates several risks. One of the significant risks is provider reliability, which can be understood in two ways. The first concerns the resilience of the provider's system [46]. This means the ability to withstand disruption, degradation, or destruction caused by kinetic or non-kinetic threats, including cyberattacks, electronic interference, or physical attrition [47]. The second concerns the provider's commitment. A civilian company is not necessarily bound to support only the state in which it is registered or headquartered. It may provide services to multiple customers, including foreign governments, private actors, or international organizations. As a result, service provision may be affected by contractual obligations or commercial priorities [44]. A civilian provider may also decide to suspend, restrict, or discontinue its services. This may occur because of unwillingness to support a particular military activity, a more profitable contract with another customer, technical limitations, political pressure, or concern that continued support could expose its assets to adversary action. The reported restriction of Starlink services for Ukrainian forces during the Russo-Ukrainian war illustrates this type of vulnerability. According to available reporting, some Ukrainian military functions dependent on the service, including communication, drone operations, and artillery fire adjustment, became significantly more difficult when access was unavailable or limited in certain areas [48]. When civilian space assets directly support military activities, they may be perceived by an adversary as contributing to military action. This raises the question of whether such dual-use assets could become lawful military objectives under the law of armed conflict. Article 52 of Additional Protocol I to the Geneva Conventions defines military objectives as objects: "*which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definitive military advantage.*" [49] If a civilian satellite or related service meets these criteria in a specific operational context, an adversary may argue that it has become a legitimate military target [50].

The military use of the space domain differs from most other operational domains because the relevant assets—particularly satellites—are often privately owned even when they directly support military activities. When armed forces rely on civilian providers for space-based services such as Earth observation, access is commonly procured through service or subscription arrangements. This offers several advantages: it is faster and often more cost-effective than building sovereign capacity, it allows militaries to benefit from rapid technological advances in the commercial market, and it reduces the burden of developing the full Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Interoperability (DOTMLPFI) functional framework required to generate such capabilities independently. However, this arrangement also creates structural tension because those two parties do not bear risk in the same way. Armed forces use these services to advance national security objectives, while commercial providers must protect the financial viability of their business. In a worsening security environment, civilian satellites that support military operations may become targets of adversarial action, whether through disruption, degradation, or destruction. In such case, the military may lose an outsourced sensing capability, but in some circumstances, it may be able to mitigate that loss by switching to another source. For the civilian operator, by contrast, the loss is more acute. Asset may be disabled or destroyed before it has generated sufficient revenue to cover for its costs. The result is not only the loss of a platform, but potentially serious damage to the provider's business model and long-term viability. Unlike most military capabilities, these platforms remain under private ownership even while performing functions of military relevance. Yet because they operate in the space environment, they are inevitably exposed to hostile acts linked to armed conflict. This misalignment between ownership, mission, and risk suggests the need for mechanisms to protect or compensate commercial providers whose assets are endangered because of supporting national security objectives.

5. United States as an Example of a Tailored Approach to the Protection of Civilian Space Assets

The EU's approach to critical infrastructure protection is primarily based on resilience. Critical sectors are treated as essential to social, economic, and governmental continuity, and operators are therefore required to identify risks, adopt technical and organizational safeguards, maintain service continuity, report incidents, and cooperate with competent authorities [51].This form of resilience-building is necessary, but it may be insufficient where civilian actors provide services that are vital to armed forces or other national security institutions and therefore become attractive targets for adversaries. The following section examines the United States as an example of a more tailored approach to the civilian space assets. Although it does not amount to a standing guarantee of direct military defense, it moves beyond general critical-infrastructure resilience.

Recent United States policy suggests that the protection of strategically relevant commercial space companies is pursued primarily through specific risk-reduction measures rather than through a standing guarantee of direct military defense [52,53].The 2024 *DoD Commercial Space Integration Strategy* states that, although military force could be directed to protect and defend civilian assets in appropriate circumstances, the Department's normal protective approach is built around three lines of effort: norms and standards, threat information sharing, and financial protection mechanisms.[52].In that same document, financial protection is defined to include traditional commercial insurance, commercial war-risk insurance, possible United States government-provided insurance, and indemnification, while the strategy also notes that new statutory authority would be required to extend government war-risk insurance to the space domain.[52].This risk-sharing logic is complemented by the 2023 *Space Policy Review and Strategy on Protection of Satellites*, which places the protection of commercial partners within a broader architecture-level approach to space defense. In this understanding, protection concerns not only satellites in orbit, but also ground nodes, networks, electromagnetic spectrum, movement and maneuver, hardening, and cybersecurity [54].At the operational level, United States Space Command's 2025 *Commercial Integration Strategy* translates these principles into practice through its "Inform & Protect" line of effort, under which the command provides threat alerts and mitigation options, uses information-sharing agreements and SSA agreements, supports the *Commercial Space Protection Tri-Seal Framework/Agreement* with National Reconnaissance Office and National Geospatial-Intelligence Agency, and, when directed, protects prioritized commercial space assets to preserve access to critical capabilities throughout conflict.[55,56].Together, these policies indicate that the United States approach protects civilian space companies primarily through resilience, warning, information sharing, contractual assurance, and financial risk-sharing, while reserving direct military defense for selected cases in which those civilian capabilities are tightly linked to national security.

At the same time, external analysis suggests that this approach remains incomplete from the perspective of the civilian actors themselves. Center for Strategic and International Studies argues that commercial satellite operators remain vulnerable because the United States has not clearly established how it would respond to attacks on its civilian satellites and because operators currently lack access to war-risk insurance or comparable financial protection, leaving them to bear the losses themselves [57].Kisiel develops this criticism in legal terms, arguing that indemnification should be treated as a necessary secondary payer because many insurance policies exclude losses caused by war or hostile action and because firms supporting military missions may otherwise be unable to absorb severe financial losses or reconstitute destroyed assets [58] Berkowitz similarly treats civilian space actors as emerging targets rather than neutral market actors and argues that, where the government relies on civilian capabilities for national security purposes, it should move beyond general policy statements toward more practical protection measures, including threat information sharing, provision of government-furnished equipment, selective funding for protective modifications, and possible legislation on indemnification and advanced funding [59]. Taken together, these analyses suggest that the central weakness of the present United States approach lies in the continued uncertainty over how civilian space companies would actually be protected and compensated once they become targets of adversary action. Nonetheless, among the cases examined here, the United States appears to offer the most explicit policy framework dedicated to the protection of civilian or commercial space assets.

6. Proposal of Protective Measures

It should be in the interest of the state to provide protection to civilian providers of space-based DPS. However, it is essential that the state first identifies those providers that are critical and upon whose DPS it is dependent. The authors propose five recommendations through which the state can ensure the protection of these civilian providers: war risk insurance; physical protection of ground segment; in-orbit physical protection; deterrence; and threat information sharing.

For commercial providers of satellite DPS to militaries, one of the principal obstacles may be insurance. Since the nature of this partnership is direct support of military operations, the fact that they inevitably operate over adversary territory, where they may be more easily affected by counterspace capabilities, makes the risk of hostile action against their assets highly likely. Substantial portion of satellite insurance policies exclude coverage for acts of war or cyberattacks [46]. States that identify certain commercial providers as critical to fulfill the missions of their armed forces should therefore provide insurance for their satellites, or alternative (financial) compensation. This insurance would pertain exclusively to risks arising from armed conflict (deliberate kinetic or non-kinetic interference with a satellite system by a third party as a result hostile act, in a manner that partially or wholly impairs the space system's functionality). A key challenge that may arise concerns the attribution of such attacks and the determination of whether a satellite's incapacitation was genuinely attributable to such hostile action. In the case of a kinetic strike on a commercial satellite via a direct ascent anti-satellite missile, or deliberate alternation of an adversary's orbital parameters to induce collision even after evasion maneuvers, attribution is readily feasible (assuming the availability of space situational awareness data). By contrast, this issue may prove considerably more problematic in the context of cyberattacks.

States should implement a tiered physical protection measure for ground stations and associated infrastructure (e.g. communication antennas or launch sites), tailored to three distinct security postures – peacetime baseline (no credible risks, security is conducted by commercial providers sources and consists of routine perimeter security, access controls, and surveillance of the areas); heightened alert (emerging risks, security is reinforced by military personnel); wartime escalation (imminent or ongoing hostile activities, already present military personnel is reinforced by additional manpower and military equipment, in addition increased intelligence, surveillance and reconnaissance activities). Emphasis should be placed on securing remote or isolated sites, which are inherently vulnerable to sabotage or seizing. These protection measures should be executed by dedicated military units, such as territorial defence forces or their equivalents. With this measure, a potential complication arises from the fact that certain companies maintain elements of their space infrastructure network (e.g. satellite dishes) on the territory of other states. It is therefore likely that securing the physical protection of such facilities will necessitate the establishment of bilateral or multilateral agreements between states delineating the modalities of this protection. Several solutions present themselves and for illustrative purposes, consider the following model case. Suppose company Aa, officially headquartered in State A, requires access to a specific site beyond the Arctic Circle on the territory of State B to facilitate more frequent communication between its control center and its satellites. The protection of company Aa's infrastructure on State B's territory could be undertaken by the armed forces of State A, armed forces of State B, or State A could allocate financial resources to company Aa for securing such protection through private security contractors. Another challenge pertains to optical cables employed for near-real-time transmission of information from these remote areas to control centers. Such infrastructure may extend across distances of several thousand kilometers, rendering its persistent physical protection by military presence unreasonable in terms of resource allocation. In this context, the deployment of sensors detecting mechanical or electromagnetic waves, such as sonar or active radar systems, may prove appropriate. Upon detection of a suspicious object in proximity to the infrastructure, a response unit could be dispatched to the specific location. This approach, however, would not preclude inadvertent severance of the cable by a fishing or transport vessel dragging its anchor along the seabed.

Physical protection can also be provided in orbit through patrol satellites. Such protection should be prioritized according to strategic value of the asset. For instance, satellites in low earth orbit (LEO) are mostly in constellations consisting of tens, hundreds or even thousands of assets, meaning their strength lies in redundancy, as the loss or disruption of one satellite may not significantly degrade the overall functionality. For adversary, targeting a single satellite in such constellation may therefore offer limited operational benefit. Furthermore, providing protection in such manner in LEO would necessitate a substantial number of patrolling satellites, rendering the approach truly resource demanding. For such reasons, assigning patrol satellites to protect LEO constellations would be inefficient and difficult to scale. The protection should be focused more on "one of a kind" satellites for instance in GEO. A single GEO communications satellite can provide continuous coverage over a wide geographic area, possibly supporting military units across theaters. For adversary, such satellite presents high value target. Depending on the adversary's objective, he may seek to jam, damage, destroy, conduct rendezvous and proximity operation, or gather intelligence from the satellite via his space assets. For these reasons, patrol satellites should be deployed near selected high-value GEO satellites. Their purpose would be to strengthen local SSA and provide a visible layer of protection. Patrol satellites could monitor the surrounding orbital environment, detect suspicious activities, inspect nearby objects or serve as retaliatory asset. Their presence would also serve as a deterrent by increasing the likelihood of uncovering and attributing adversary activity.

Deterrence represents a highly effective instrument of protection; however, its credibility and implementation must remain firmly within the purview of the state. As a strategic concept, deterrence is not novel. During Cold War, there was a concept embodied in the doctrine of Mutual Assured Destruction between the United States and the Soviet Union. In contemporary security environment, deterrence has evolved into a broader spectrum of measures, including the demonstration of capabilities, forward deployment of forces, declaratory policies, and coordinated signaling through international organizations such as North Atlantic Treaty Organization (NATO). During the 2021 Brussels Summit NATO has explicitly stated that an attack to, from, or within space could lead to the invocation of Article 5 [60]. Nevertheless, deterrence in space requires careful adaptation. The domain introduces unique challenges, including attribution difficulties, dual-use technologies, and an expanded grey zone. Consequently, traditional deterrence models must be tailored to address these complexities, integrating legal, technological, and operational dimensions specific to space. Equally critical is the consistency between declaratory policy and actual behavior. The effectiveness of deterrence hinges on credibility; therefore, states must be prepared to act in response to hostile actions targeting space systems. Failure to uphold stated commitments risks undermining deterrence posture, potentially emboldening adversaries and increasing the likelihood of further aggression.

A further protective measure is the systematic sharing of SSA data and relevant threat warnings with civilian space providers covering the entire space architecture, including the space, ground, and link segments. Such sharing should cover orbital risks, suspicious maneuvers, cyber threats, electromagnetic interference, and threats to ground infrastructure. This type of measure is already reflected in the practice of some actors, particularly in the United States, where commercial space protection frameworks include threat information sharing, and space domain awareness cooperation. To be effective, information sharing should function as a two-way and action-oriented protection mechanism rather than a one-directional flow of warnings from the state to industry. Civilian providers may detect anomalies, cyber incidents, service disruptions, or unusual operational patterns that are relevant to state authorities and intelligence agencies. State-provided warnings should therefore be conducted via secure reporting channels and trigger pre-agreed mitigation procedures. The same mechanism should also support deconfliction. Where security permits, national authorities or armed forces should notify commercial providers about planned activities that may affect their operations, such as electromagnetic warfare activity, satellite maneuvers, launch activity, or exercises affecting ground and link segments. Providers should likewise be able to report planned outages, maneuvers, maintenance, or technical limitations that may affect services used for national security purposes. Such cooperation would reduce the risk of friendly interference, misinterpretation of anomalies, and unintended degradation of commercial capabilities, while still balancing “need to know” with “need to share” concept.

7. Conclusions

In contemporary operational environment, states increasingly rely on privately owned civilian space assets and related services, including data acquisition and processing, satellite operations, and other space-based support functions. As discussed earlier in this article, civilian companies provide national actors, including the military and other government agencies, with vital capabilities such as satellite communications and Earth observation. Because these functions are strategically important to the state, the companies that provide them may constitute valuable targets for potential adversaries. It is therefore reasonable to assume that the protection or support of civilian providers of space-related services is in national interest.

This interest should not be limited to general declarations of resilience or to the expectation that private operators will absorb strategic risk on their own. Civilian space providers may remain commercial entities, but once their services become essential for national defence, crisis response, or continuity of state functions, their protection becomes a shared responsibility. The state should therefore be able to identify those civilian providers on which national defence is critically dependent and establish mechanisms that reduce their exposure to hostile action, disruption, or unacceptable financial loss. Protective measures should be understood as a layered approach rather than isolated instruments. War-risk insurance or other financial compensation can reduce the economic burden placed on civilian providers. Physical protection of the ground segment can strengthen vulnerable terrestrial infrastructure. In-orbit protective capabilities may be suitable for selected high-value assets, particularly where redundancy is limited. Deterrence can raise the political and military costs of hostile action, while threat information sharing can improve warning, attribution, mitigation, and coordination between public authorities and private operators.

The protection of civilian space assets will not eliminate the vulnerability of space systems, nor can every satellite or supporting infrastructure be defended in the same way. However, the absence of a clear protection framework creates a strategic gap between state dependence and private ownership. As the military and civilian use of space continue to converge, this gap is likely to become more significant. States that rely on civilian space-based DPS should therefore move from ad hoc cooperation toward structured protection mechanisms. Such mechanisms would improve the resilience of national security functions while also making cooperation with civilian space providers more sustainable in periods of crisis or armed conflict.

Acknowledgements. The authors respectfully thank leaders and participants of "Land Operations Leadership - LANDOPS" project, which focuses on the decision support for commanders, conducting land operations. Their support, ideas and partial inputs enriched content of this paper.

References

1. Why *Go to Space*. Online. NASA. Available at: https://www.nasa.gov/humans-in-space/why-go-to-space/ (accessed on 2 February 2026).
2. MARIAPPAN, Amrith and CRASSIDIS, John L., 2023. *Kessler’s syndrome: a challenge to humanity*. Frontiers in Space Technologies. 2023, vol. 4.

3. *UK Space Agency blog: Satellites – the power behind our modern world*. Online. 2023. Available at: https://shorturl.at/Vl40Z (accessed on 2 February 2026).
4. *U.S. Space Force: Ensuring Readiness in a Contested Space Domain*. Online. 2025 Available at: https://shorturl.at/6M15P (accessed on 2 February 2026).
5. NATO. *NATO's approach to space*. Online. 2025. Available at: https://shorturl.at/7AbuL (accessed on 2 February 2026).
6. *Rheinmetall and ICEYE plan to establish a joint venture – satellite production and other space solutions in the new Rheinmetall Space Cluster*. Online. 2025. Available at: https://shorturl.at/UQCWI (accessed on 3 February 2026).
7. *Poland acquires SAR satellites from ICEYE to strengthen defence capabilities*. Online. 2025. Available at: https://shorturl.at/bq8Ww (accessed on 2 February 2026).
8. GURANTZ, Ron. *Satellites in the Russia-Ukraine War*. Carlisle: Strategic Studies Institute and U.S. Army War College Press, August 2024. ISBN 1-58487-857-6.
9. *International Charter Space and Major Disasters. Online.* Available at: https://shorturl.at/RkGVL (accessed on 2 February 2026).
10. GOVERNMENT OFFICES OF SWEDEN, Ministry of Defence. *The role of space in a new security situation: Sweden's defence and security strategy for space*. Stockholm: Government Offices of Sweden, 2025.
11. *Space Force Doctrine Document 1, The Space Force*. Space Training and Readiness Command, 3 April 2025.
12. *National space strategy 2025–2040*. Paris: Secrétariat général de la défense et de la sécurité nationale (SGDSN), 2025.
13. *Security Strategy of the Czech Republic 2023*. Prague: Ministry of Foreign Affairs of the Czech Republic, 2023. ISBN 978-80-7441-100-7.
14. *'We Have Not Passed the Point of No Return', Disarmament Committee Told, Weighing Chance Outer Space Could Become Next Battlefield*. Online. United Nations. 26 October 2022. Available at: https://press.un.org/en/2022/gadis3698.doc.htm (accessed on 4 February 2026).
15. *Russia warns United States: use of SpaceX for spying makes its satellites a target. Online. Reuters. March 20, 2024. Available at:* https://shorturl.at/ZrTFD (accessed on 4 February 2026).
16. UN GENERAL ASSEMBLY. *Preliminary Recommendations On Possible Norms, Rules And Principles Of Responsible Behaviours Relating To Threats By States To Space Systems*. 2023. A/AC.294/2023/WP.7.
17. United States Department of Defense; Office of the Director of National Intelligence. National Security Space Strategy: Unclassified Summary; U.S. Government: Washington, DC, USA, 2011
18. United Kingdom Ministry of Defence. Defence Space Strategy: Operationalising the Space Domain; Ministry of Defence: London, UK, 2022.
19. MELECHIN, Petr. *Vše o konstelaci Starlink*. Online. ElonX. 2019. Available at: https://www.elonx.cz/vse-o-konstelaci-starlink/ (accessed on 5 February 2026).
20. *Annual number of objects launched into space*. Online. Our World in Data. January 8, 2026. Available at: https://shorturl.at/oOJPT (accessed on 7 February 2026).
21. European Space Agency. Space Environment Statistics. Online. ESA: Darmstadt, Germany, 2026 Available at: https://sdup.esoc.esa.int/discosweb/statistics/ (accessed on 15 April 2026).
22. GROWCOOT, Matt. *Satellite Takes Selfie to Show it Was Hit by Space Debris*. Online. PetaPixel. 9 November 2024. Available at: https://shorturl.at/jONFg (accessed on 7 February 2026).
23. United Nations. *Destructive direct-ascent anti-satellite missile testing*. A/C.1/77/L.62. General Assembly, Seventy-seventh session, 13 October 2022. New York: United Nations, 2022.
24. Pollpeter, K. *China's Role in Making Outer Space More Congested, Contested, and Competitive*. China Aerospace Studies Institute. Montgomery, AL, USA, 2021.
25. TIBALDO, Francesco. *The War In Ukraine And The U.S. New Strategic Posture In Outer Space*. The Defence Horizon Journal. 2025.
26. U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *2025 Report to Congress of the U.S.-China Economic and Security Review Commission*. Washington, DC: U.S. Government Publishing Office, 2025.
27. LUZIN, Pavel. *Russia's Space Program After 2024*. Philadelphia: Foreign Policy Research Institute, Eurasia Program, July 2024.
28. HADLEY, Greg. *Space 'Underpins All Instruments of National Power,' Raymond Says*. Online. Air and Space Forces Magazine. 2022. Available at: https://shorturl.at/oMiiD (accessed on 20 February 2026).
29. Dolman, Everett C. *Space Is a Warfighting Domain*. Æther: A Journal of Strategy & Airpower, vol. 1, no. 1, Spring 2022, pp. 82–90.
30. *Global Counterspace Capabilities: An Open Source Assessment*. 4. Secure World Foundation, 2025
31. RAKHSITHA, Sayyam Sonegara a SHREYA R, Sonia Kumawat. PROFIT MAXIMIZATION PRINCIPLES FOR BUSINESS GROWTH IN THE MODERN WORLD. Online. *International Journal of Development Research*. Year 2023, Vol. 13, 04. ISSN 2230-9926.
32. *SpaceTech Industry in Figures*. Online. SpaceTech Analytics. Available at: https://shorturl.at/QXvht (accessed on 20 February 2026).
33. *Executive summary: Expanding frontiers*. Online. GOV.UK. 16 May 2023. Available at: https://shorturl.at/ryc7P (accessed on 23 February 2026).
34. *SPACE DATA AS A SERVICE*. Online. AAC CLYDE SPACE. Available at: https://shorturl.at/hsCOx (accessed on 20 February 2026).
35. FINCH, Michael J. Limited Space: Allocating the Geostationary Orbit. Online. *Northwestern Journal of International Law & Business*. 1986, no. 7.

36. WILKINSON, Freddie. The History of the Space Race. Online. National Geographic Education. Last updated 20 January 2026. Available at: https://shorturl.at/PwI7p (accessed on 23 February 2026).
37. NASH, Elias. *Why Humans Haven't Gone Back To The Moon Since 1972*.Online. SCIENCING. 2025. Available at: https://shorturl.at/PNUKd (accessed on 23 February 2026).
38. European Commission; High Representative of the Union for Foreign Affairs and Security Policy. EU Space Strategy for Security and Defence Online. European Union: Brussels, Belgium, 2023. Available at: https://shorturl.at/WVxAF (accessed on 3 May 2026).
39. General Secretariat for Defence and National Security (SGDSN). *The Critical Infrastructure Protection in France: Objectives and Challenges*. SGDSN: Paris, France, 2017.
40. National Protective Security Authority. Critical National Infrastructure. Online. NPSA: London, UK, 2026. Available at: https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure (accessed on 3 May 2026).
41. National Protective Security Authority. Critical National Infrastructure. Online. NPSA: London, UK, 2026. Available at: https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure (accessed on 3 May 2026).
42. Cybersecurity and Infrastructure Security Agency. Space Systems and Services. Online. CISA: Washington, DC, USA, 2024. Available at: https://www.cisa.gov/space-systems (accessed on 5 May 2026).
43. North Atlantic Treaty Organization. NATO Commercial Space Strategy. Online. NATO: Brussels, Belgium, 2025. Available at: https://shorturl.at/MlcXy (accessed on 7 May 2026).
44. WONG, Jonathan P.; et al. *Leveraging Commercial Space Services: Opportunities and Risks for the Department of the Air Force*. Santa Monica, CA: RAND Corporation, 2023. ISBN 978-1-9774-1129-7.
45. RAJWANI, Tazeeb; et al. *Corporate military activities and key frontiers in international business research*. Journal of World Business, 2026, vol. 61. https://doi.org/10.1016/j.jwb.2025.101693.
46. KIM, Yool, et al. *Operational and Policy Implications of Integrating Commercial Space Services into U.S. Department of Defense Operations*. Santa Monica, CA: RAND Corporation, 2025. ISBN 978-1-9774-1487-8
47. STENSBERG, Luke. *Small Satellites with Large Exposure: How Does New Space Fare in Cyberspace?* Joint Air Power Competence Centre (JAPCC), Journal Edition 38, October 2024. Available at: https://www.japcc.org/articles/small-satellites-with-large-exposure/ (accessed on 19 May 2026)
48. ROULETTE, Joey; et al. *Musk ordered shutdown of Starlink satellite service as Ukraine retook territory from Russia.* Reuters, 25 July 2025. Available at: https://shorturl.at/kYfXR (accessed on 20 May 2026).
49. INTERNATIONAL COMMITTEE OF THE RED CROSS. Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I) [treaty]. Adopted 8 June 1977. Entry into force: 7 December 1978. Geneva: ICRC.
50. BERRANG, Svenja. *How would IHL apply to hostilities in outer space?* Humanitarian Law & Policy Blog. Online. 2 November 2023. International Committee of the Red Cross. Available at: https://blogs.icrc.org/law-and-policy/2023/11/02/how-would-ihl-apply-to-hostilities-in-outer-space/ (accessed 24 February 2026).
51. EUROPEAN UNION. *Making critical entities more resilient: Summary of Directive (EU) 2022/2557*. Online. EUR-Lex, 2023 (last updated 19 February 2024). Available at: https://shorturl.at/VWYbt. (accessed on 20 May 2026).
52. UNITED STATES. Department of Defense. *Commercial Space Integration Strategy*. Washington, D.C.: Department of Defense, 2024
53. Deputy Pentagon Press Secretary Sabrina Singh, press briefing, 2 April 2024. Available at: https://shorturl.at/d4l4N (accessed on 20 May 2026).
54. Department of Defense, *Space Policy Review and Strategy on Protection of Satellites*. *Online.* 2023. Available at: https://spacenews.com/dod-submits-congressionally-mandated-space-policy-report/ (accessed on 20 May 2026).
55. UNITED STATES SPACE COMMAND. *Commercial Integration Strategy*. Peterson SFB (CO): Department of Defense, United States Space Command, 2025.
56. NATIONAL RECONNAISSANCE OFFICE. *Tri-Seal Commercial Space Protection Framework*. Online. 31 August 2023. Available at: https://shorturl.at/lbJjs (accessed on 23 May 2026).
57. SWOPE, Clayton. *How Can the U.S. Government Safeguard Commercial Satellites from Threats?*. Washington, D.C.: Center for Strategic and International Studies (CSIS), August 2025.
58. KISIEL, Edwin Charles. *Indemnification for Commercial Space Services Vendors.* Public Contract Law Journal. Online. 21 August 2024. American Bar Association. Available at: https://shorturl.at/zylXE (accessed on 26 May 2026).
59. BERKOWITZ, Marc. Countering threats to US commercial space systems. *The Space Review*. Online. 16 December 2024. Available at: https://www.thespacereview.com/article/4910/1 (accessed on 26 May 2026).
60. NORTH ATLANTIC TREATY ORGANIZATION (NATO). Brussels Summit Communiqué. *NATO*. Online. 14 June 2021. Available at: https://shorturl.at/jurcG (accessed on 29 May 2026).