Research Paper

International Security Programme

May 2025

Securing the space-based assets of NATO members from cyberattacks

A framework to strengthen cybersecurity in outer space

Julia Cournoyer

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

Summary

- The increasing reliance on space-based assets for military and civilian functions has heightened the need to protect these systems from cyberthreats. Satellites play a crucial role in secure communications, navigation, intelligence and early warning systems, making them indispensable to NATO's defence and deterrence posture. However, space-based assets face a growing array of threats, including cyberattacks, which can disrupt critical functions, compromise operations and undermine global security.
- This paper examines the vulnerabilities of the space-based systems of NATO's key members to cyberattacks, outlining a structured framework for enhancing their security. It builds on previous Chatham House research and consultations with experts to identify major cybersecurity challenges in the space domain, and it offers a roadmap for strengthening NATO's resilience. By analysing trends in space security, emerging threats and NATO's evolving space policy, the paper highlights the need for a more coordinated approach to securing space-based assets.
- This paper assumes that NATO will remain a functional and cohesive organization, continuing to play a central role in collective security and space defence. However, NATO's ability to implement an effective space cybersecurity strategy is increasingly shaped by shifting transatlantic defence priorities, evolving national security policies and a growing reliance on private sector space infrastructure. As defence commitments among NATO members continue to evolve, ensuring the long-term stability of space security cooperation within the alliance will be critical for sustaining collective deterrence and operational resilience.
- NATO has taken significant steps to integrate space into its defence strategy, recognizing it as an operational domain alongside air, land, sea and cyber in 2019. However, protecting space-based assets requires a more coordinated and proactive cybersecurity strategy. This paper proposes a three-tiered framework – based on mitigation, adaptation and resilience – for strengthening NATO's space cybersecurity posture.
- In this framework, mitigation focuses on implementing immediate technical and policy measures to reduce vulnerabilities, such as encryption, intrusion detection and secure procurement standards. Adaptation involves developing long-term strategies to adjust to evolving cyberthreats, including training programmes, strategic foresight and interoperability between NATO members. Resilience ensures that space-based systems can withstand and recover from cyberattacks by prioritizing redundancy (e.g. back-up systems), robust infrastructure and alternative navigation systems.

— This paper also explores key trends shaping the space security landscape, including the commercialization of space, the increasing role of private sector actors in military operations and the development of emerging technologies such as artificial intelligence (AI) and quantum computing. This research underscores the need for NATO to engage more closely with commercial providers, to strengthen cyber practices across its members and to develop common standards for cybersecurity in the space domain.

— By adopting this structured framework approach, NATO can enhance its ability to secure critical space-based assets against cyberthreats. The protection of these assets is not only a technical necessity but a strategic imperative that will determine NATO's ability to deter threats, respond to crises and maintain its operational advantage in an increasingly contested space environment.

01 Introduction

Space-based assets underpin NATO's ability to deliver collective defence, crisis management and operational coordination. As cyber and space domains become increasingly intertwined, a unified, cyber-resilient strategy is vital to ensure NATO is able to fulfil its mission.

NATO's ability to coordinate defence and deterrence efforts has long been a cornerstone of transatlantic security. However, as the alliance faces new challenges both externally and internally, cohesion and strategic stability cannot be taken for granted. Among key member states, shifting geopolitical priorities and evolving national policies have introduced new complications for NATO's long-term endurance, raising questions about its future role, collective defence commitments and ability to operate as a unified security actor. These shifts in member state priorities and policies have significant implications for NATO's ability to protect critical space-based assets, which underpin much of its operational capability.

Space is critical to NATO's ability to fulfil its mission of collective defence and crisis management. Satellites and space-based assets provide essential capabilities, including secure communication, navigation, early warning systems, intelligence and surveillance. These capabilities underpin NATO's ability to coordinate multinational operations, monitor threats and ensure readiness in response to new challenges. At the 2021 NATO summit in Brussels, NATO members also acknowledged that attacks to, from, or within space pose a significant threat to the alliance's security and could trigger an Article 5 response. With space increasingly contested, NATO must secure these systems to maintain its operational edge and safeguard its interests.

This paper assumes that NATO will remain functional despite mounting pressures on its unity and strategic direction. However, if political divergences among member states widen or if long-standing security commitments are reassessed, NATO's ability to coordinate joint security efforts, particularly in space, may be affected. Securing NATO's space assets remains imperative regardless of broader political changes or challenges but the degree to which the recommendations made throughout the paper remain viable will ultimately depend on the alliance's ability to sustain cohesion and strategic alignment in an increasingly complex security environment.

NATO and the space security challenge

In the last two decades, countries within and beyond NATO have come to rely heavily on space-based technologies for military, economic and civilian purposes. From satellite communications to global positioning systems (GPS), these technologies underpin modern life and are integral to national defence and security. However, as space becomes increasingly contested – and as a result congested – the resilience and protection of these critical assets are of paramount importance.

Space-based systems face a wide range of emerging threats. These include physical kinetic threats, such as anti-satellite (ASAT) weapons, cyberattacks and non-deliberate hazards like space debris and space weather. These threats have the ability to disrupt communications, compromise operations and fundamentally undermine global security. This paper focuses specifically on the cybersecurity of satellites and space-based assets.

In the last two decades, countries within and beyond NATO have come to rely heavily on space-based technologies for military, economic and civilian purposes.

Russia's invasion of Ukraine illustrated the strategic vulnerabilities of space-based systems in modern warfare. On 24 February 2022, the day of the full-scale invasion, a cyberattack targeted Viasat's KA-SAT satellite network, disrupting internet services for tens of thousands of people across Ukraine and Europe. Rather than directly attacking the satellite itself, the hackers compromised ground-based infrastructure, specifically modems used to connect to the satellite, causing widespread connectivity failures.[1] The attack was intended to undermine Ukrainian command and control, and also had spillover effects on civilian infrastructure.[2] Additionally, a few months later, US cybersecurity authorities and NATO members issued a joint warning that Russian state-backed cybercriminal groups were preparing cyberattacks on critical infrastructure.[3] This attack is part of a broader trend of increasing cyberattacks on satellites and critical infrastructure.[4]

NATO declared space as an operational domain in 2019. That declaration led to a fundamental change in the way in which the alliance conducts its missions and operations. It has also had implications for NATO's security, defence and deterrence policy. It is expected that acknowledging space as a domain of operations will expand NATO's collective defence arrangements and will place outer space security

1 Viasat (2022), 'KA-SAT Network cyber attack overview', 30 March 2022, https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview.
2 Cyberpeace Institute (2022), 'Case Study: Viasat', June 2022, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.
3 Cybersecurity and Infrastructure Security Agency (2022), 'Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', 9 May 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.
4 Kaczmarek, S. (2024), 'We Need Cybersecurity in Space to Protect Satellites', 5 February 2024, Opinion, *Scientific American*, https://www.scientificamerican.com/article/we-need-cybersecurity-in-space-to-protect-satellites.

at the centre of NATO's defence and deterrence portfolio. NATO's 2022 Strategic Concept also underlined the vital role of space for the alliance's deterrence and defence posture.[5]

However, NATO's ability to protect its space-based assets is inextricably linked to its political cohesion and strategic unity, both of which appear less certain at the time of writing. President Donald Trump has cast doubt on the US commitment to NATO, by calling into question whether he would defend NATO members if they do not meet defence spending commitments.[6] While there have been no concrete changes to the US posture in NATO, if US backing for NATO were to diminish significantly or be withdrawn altogether, this would severely compromise the alliance's ability to coordinate intelligence sharing, collective defence and space-based operations. Certain capabilities such as intra-NATO intelligence sharing and coordinated space operations are contingent on a functional and cohesive alliance.

Cyberthreats can target multiple components of NATO's space-based assets system, including satellites themselves, the ground infrastructure that controls them and the transmission links that carry data between them. Rather than target a single point of vulnerability, cyberattacks can exploit weaknesses across this entire network.

NATO members, or companies based on their territories, own more than half of the operational satellites that are in orbit.[7] However, only a handful of countries within NATO have the means to provide space support to NATO operations. In the future, more countries will gain access to advanced space equipment as these technologies become more readily available.

A previous Chatham House study analysed the role of space technology in NATO missions and operations, examining NATO's space capabilities, including position, navigation and timing (PNT), intelligence, surveillance and reconnaissance (ISR), missile defence, communications, space situational awareness and environmental monitoring.[8] That study highlighted possible cyber risks and identified potential impacts from the loss of capabilities due to cyberattacks. Several recommendations included potential capability needs for NATO, with a specific focus on doctrine, organization, training, materiel, leadership, personnel, facilities and interoperability (DOTMLPF-I) approaches.[9]

This research paper aims to highlight mitigation, adaptation and resilience measures that NATO and its key members can implement through improved coordination to protect space assets from cyberattacks. This three-tiered framework of measures should be considered when establishing future cybersecurity standards and guidelines within the alliance.

---

5 NATO (2022), *NATO 2022 Strategic Concept*, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.
6 *Guardian* (2025), 'Trump casts doubt on willingness to defend Nato allies "if they don't pay"', 7 March 2025, https://www.theguardian.com/us-news/2025/mar/07/donald-trump-nato-alliance-us-security-support.
7 NATO (2020), 'NATO's approach to space', 27 April 2020, https://www.nato.int/cps/en/natohq/topics_175419.htm.
8 Unal, B. (2019), *Cybersecurity of NATO's Space-based Strategic Assets*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/publication/cybersecurity-nato-s-space-based-strategic-assets.
9 Ibid.

Chapter 2 of the paper highlights existing trends and developments in space technology. Chapter 3 gives an overview of the development of NATO's outer space policy and the national space policies of key members. Chapter 4 introduces a three-tiered framework for tackling cyberthreats in space. The paper concludes with further recommendations and areas for future research, offering a roadmap for strengthening NATO's space cybersecurity posture.

The space–cyber nexus

The interconnectedness of space and cyber domains has become increasingly apparent in modern conflict, as illustrated by the role of cyberattacks in Russia's invasion of Ukraine. Space-based systems are critical in military operations, enabling secure command and control, navigation, precise targeting, intelligence gathering and early warning of threats. Satellites also provide essential communications for coordinating forces, guiding weapons systems and monitoring adversary movements. Space-based assets are foundational to NATO's operations and their compromise could destabilize military readiness, crisis response and broader alliance cohesion.

NATO's 2022 Strategic Concept highlighted the vital role of space in its deterrence and defence posture, reflecting a shared understanding among member states of the risks posed by cyberthreats to space systems. To address these risks, NATO has taken concrete steps to strengthen its space and cyber capabilities. The establishment of the NATO Space Centre at Allied Air Command in Ramstein, Germany, and ongoing efforts to integrate space considerations into collective defence strategies illustrate NATO's proactive approach. These initiatives align closely with the national policies of member states, outlined in this paper, many of which prioritize space and cyber resilience as key elements of their security strategies. This shared commitment underscores the urgency of securing these assets to ensure NATO's operational edge and collective security.

Cyberattacks on space-based assets may affect the way in which NATO conducts its operations. Depending on the type of space-dependent capability that the adversary chooses to attack and the type of attack (e.g. spoofing, software infiltration and signal jamming), the consequences may vary. Loss of PNT signals, for instance, may impact how warships and guided missiles function.[10] Losing communication systems or receiving spoofed data may oblige military forces to adapt to the new operating environment in a quicker manner.

10 For more analysis on possible consequences of losing space-dependent capabilities, see Unal (2019), *Cybersecurity of NATO's Space-based Strategic Assets*, pp. 17–18.

02
Trends and recent developments in space technology

Evolving trends in space technology present both opportunities and risks for NATO's member states. Commercialization, emerging technologies and cost reductions increase access to space, but also amplify cyber risks to space-based assets.

National and international infrastructure is increasingly dependent on outer space services and products, for example: financial transactions; sea, land and air navigation; military manoeuvres on the battlefield; Earth observation from orbit for emergency/disaster monitoring and atmospheric composition; and internet and phone communications. Moreover, strategic weapons systems depend on space assets for command, control, communication and consultations, early warning systems for surveillance and reconnaissance, and missile defence.

Military use of outer space is not a new phenomenon, but several key trends help further our understanding of how space technology has evolved in this domain. These are:

— **Commercialization:** Outer space is no longer an area that is out of reach for commercial actors. Rather, investments by the private sector have significantly reduced the barriers to accessing space, particularly through advances in satellite launches and communication technologies. The role of commercial operators has been prominent during Russia's invasion of Ukraine, where US-based companies like SpaceX have provided critical satellite internet services through Starlink, enabling Ukrainian forces to maintain secure communications despite disruptions to traditional infrastructure. Commercialization is also expanding into areas such as sensors, satellite constellations and space-based data services, which are

increasingly integrated into national and allied security frameworks. The reliance on space assets is likely to increase even further in the future, especially as space technology becomes more commercialized, leading more countries to invest in this sector. This shift is exemplified by the US Department of Defense's release of its 2024 Commercial Space Integration Strategy, which aims to incorporate commercial space solutions into national security architectures.[11] The US Space Force has similarly pivoted to a new model for integrating commercial space solutions, to 'focus on stronger partnerships with commercial partners and allied nations'.[12] The growing reliance on commercial space-based assets underscores the need for robust partnerships between defence organizations and private operators to ensure the security and resilience of these systems.

- **Financial cost calculation:** The commercialization of space has also drastically reduced the financial barriers to entry, enabling more actors to invest in the space domain. In particular, several private initiatives have lowered the costs to launch into outer space. The price of heavy launches to low Earth orbit (LEO), for example, has fallen by 95 per cent in large part due to efficiencies introduced by the private sector.[13] This reduction has facilitated the proliferation of small satellites, like CubeSats and mega satellite constellations, including Starlink and Amazon's Project Kuiper.
- **New manufacturing methods:** Space-based additive manufacturing – for example, in-space 3D printing – reduces the weight needed to be sent into space, allowing for easier launches with reduced amounts of fuel used.[14]
- **Use of emerging technologies in space exploration:** Advancements in other technology areas also open new ways to explore outer space. For instance, AI-enabled applications provide necessary information to space exploration rovers, enabling them to land safely in challenging space conditions.[15]
- **Dual-use elements:** Dual-use technologies and assets in outer space, which serve both civilian and military purposes, blur the line between peaceful and potentially disruptive applications. For instance, service-oriented space infrastructure, including global navigation satellite systems (GNSS) and communication satellites, serve both civilian needs – enabling services like safe navigation and internet access – and military functions – supporting defence and security operations on Earth.[16] This duality can complicate how international legal and regulatory frameworks for outer space security are established.[17] In addition to dual-use capabilities, emerging dual-purpose technologies introduce

---

11 U.S. Department of Defense (2024), *Commercial Space Integration Strategy*, https://media.defense.gov/2024/Apr/02/2003427610/-1/-1/1/2024-DOD-COMMERCIAL-SPACE-INTEGRATION-STRATEGY.PDF.
12 United States Space Force (2024), *U.S. Space Force Commercial Space Strategy*, 8 April 2024, https://csps.aerospace.org/sites/default/files/2024-04/USSF_Commercial_Space_Strategy_April%202024.pdf.
13 Daehnick, C., Gang, J. and Rozenkopf, I. (2023), 'Space launch: Are we heading for oversupply or a shortfall?', 17 April 2023, McKinsey & Company, https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/space-launch-are-we-heading-for-oversupply-or-a-shortfall.
14 Inside Metal Additive Manufacturing (2024), 'Impact of Additive Manufacturing on Space Exploration', 18 March 2024, https://insidemetaladditivemanufacturing.com/2024/03/18/impact-of-additive-manufacturing-on-space-exploration.
15 An example of this is the successful landing of NASA's Perseverance Rover, which collected samples from Martian rocks and soil. See NASA (2020), 'Mars 2020/Perseverance', mars.nasa.gov/mars2020.
16 Azcárate Ortega, A. (2023), 'Not a Rose by Any Other Name: Dual-Use and Dual-Purpose Space Systems', 5 June 2023, https://www.lawfaremedia.org/article/not-a-rose-by-any-other-name-dual-use-and-dual-purpose-space-systems.
17 Ibid.

> further complexities. Activities like satellite servicing, in-orbit servicing and manufacturing (ISAM), debris removal and space logistics are inherently ambiguous in their applications. While these technologies can advance sustainability and resilience in outer space by repairing or refuelling satellites and clearing debris, they could also be repurposed for harmful actions, including disabling or interfering with other satellites.[18]

These trends present both opportunities for and risks to the defence posture of NATO and members more generally, as modern warfighting strategies increasingly depend on secure access to and use of outer space. However, the growing development of counterspace capabilities by other actors poses a direct threat to these systems, with the potential to disrupt NATO's security and defence posture in the long run. Understanding security implications at an earlier stage and laying out necessary risk-mitigation measures is fundamental to shaping NATO's best practices and guidelines in the space domain.

18 Azcárate Ortega, A. (2022), 'Address as part of UNIDIR to Open-Ended Working Group on 'Reducing space threats through norms, rules and principles of responsible behaviours', Topic 3: Current and future space-to-space threats by States to space systems', 14 September 2022, Geneva, https://documents.unoda.org/wp-content/uploads/2022/09/Azcarate-Ortega-Almudena-OEWG-dual-use-presentation-FINAL.pdf.

03
The evolution of the space policies of NATO and its key members

NATO and its key members recognize space as vital to security, with national policies shaping the alliance's approach to the space–cyber nexus. Growing reliance on civilian systems and emerging technologies increases vulnerabilities, making cyberattacks an escalating threat to critical space infrastructure.

NATO

In May 2018, the North Atlantic Council (NAC) adopted the policy of NATO space support in operations. A year later, in June 2019, the members formulated the new NATO space policy at a defence ministers' meeting in Brussels.[19] That new policy led to the declaration of space as a fifth domain of operations in November 2019.[20]

19 NATO (2019), 'NATO Defence Ministers approve new space policy, discuss readiness and mission in Afghanistan', 27 June 2019, https://www.nato.int/cps/en/natohq/news_167181.htm.
20 NATO (2020), 'NATO's approach to space', 27 April 2020, https://www.nato.int/cps/en/natohq/topics_175419.htm.

Through its space policy, NATO integrates considerations around outer space into its three core tasks of collective security, crisis management and cooperative security.[21] It engages in consultations across the alliance to reach a common understanding on opportunities, risks, challenges and vulnerabilities in line with the intergovernmental deliberations on responsible behaviours in outer space.[22]

Other developments have mainstreamed outer space across the alliance. One was the establishment of the NATO Space Centre at Allied Air Command in Ramstein, Germany, in October 2020. The centre works with national space agencies to develop interoperable space products and services across the alliance, for use in satellite imagery, PNT and early warning.[23] Another was the establishment in July 2023 of the NATO Space Centre of Excellence (CoE) in Toulouse, France – a known hub for the space industry – to focus on space-related development, education and training for the alliance.[24] The CoE provides knowledge and analysis around 'space domain awareness',[25] operational space support and space domain coordination.[26] The centre aims to be fully operational by 2026.

NATO's task also involves raising awareness and leveraging the value of the space domain across the alliance.

NATO's task also involves raising awareness and leveraging the value of the space domain across the alliance. In this regard, the NATO Bilateral Strategic Command (Bi-SC) working group focuses on empowering members that possess fewer capabilities to become significant space actors. This has been achieved in the cyber domain with Estonia leading the cybersecurity field. A similar cooperative approach is being explored for addressing challenges in Arctic communications, with initiatives like Northlink where 13 members are exploring the development of a 'secure, resilient, and reliable multinational Arctic satellite communications capability'.[27]

Additionally, as part of implementing its overarching space policy, NATO launched the Alliance Persistent Surveillance from Space (APSS) initiative in February 2023. Rather than creating NATO-owned and operated space assets, APSS uses existing and future space assets from allied countries, integrating them into

---

21 NATO (2022), 'NATO's Overarching Space Policy', 17 January 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm.
22 Ibid.
23 NATO (n.d.), 'NATO Space Centre', https://shape.nato.int/about/aco-capabilities2/nato-space-centre.
24 NATO Allied Command Transformation (2023), 'Lift-off, NATO Launches New Space Centre of Excellence', 17 July 2023, https://www.act.nato.int/article/space-newest-coe; Ministère de l'Europe et des Affaires étrangères (2021), 'Defence – Establishment of the NATO space centre of excellence in Toulouse – Communiqué issued by the Ministry for the Armed Forces (05 Feb. 2021)', https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/article/defence-establishment-of-the-nato-space-centre-of-excellence-in-toulouse; NATO (2023), 'One more step for NATO's Space Centre of Excellence', 20 January 2023, https://www.act.nato.int/articles/nato-space-coe-mou.
25 The term 'space domain awareness' is a new NATO lexicon, indicating situational awareness. While situational awareness keeps the focus on specific missions and tasks, space domain awareness expands the focus to the safety and security in the overall space environment.
26 NATO (2023), 'One more step for NATO's Space Centre of Excellence'.
27 NATO (2024), 'NATO launches five new multinational cooperation initiatives that enhance deterrence and defence', 17 October 2024, https://www.nato.int/cps/en/natohq/news_229664.htm.

a NATO virtual constellation known as 'Aquila'.[28] This initiative addresses gaps in NATO's access to specific intelligence products from outer space when needed. APSS aims to ensure that these intelligence products are available within a specific time frame. This initiative highlights the growing need to ensure the cybersecurity of space-based assets to protect both the assets themselves and the valuable data they provide. At present, APSS is a voluntary commitment from 18 NATO nations.[29] Cyberattacks on space systems can compromise not just the assets themselves, but also the critical data they provide, posing risks to NATO's operational effectiveness.

The alliance has also developed a NATO Intelligence, Surveillance and Reconnaissance Force (NISRF) to address capability gaps (tactics, techniques, procedures) in ground surveillance.

A mechanism for assisting partners in the space domain has not yet been established but existing cooperative security arrangements – for instance, the Defence and Related Security Capability Building (DCB) initiative – could be used for partner states to request assistance from NATO. DCB packages launched so far cover support to Georgia, Tunisia, Iraq, Jordan and Moldova; a package is also provided for UN peacekeeping purposes in Uganda.[30]

At the technical level, work is ongoing to improve diversity in the space segment by developing numerous satellite platforms and multiplying service providers. NATO is working on providing multiple reinforced anchors and ground stations to protect the ground segment. NATO is also protecting its systems from cyberthreats through data encryption and by securing transmission links and bearer services.[31]

The national space policies of NATO's key members

In parallel with NATO's efforts, key NATO members (the US, UK, France, Canada, etc.) have adopted specific outer space policies and doctrines that reflect their national priorities and capabilities. There are clear convergences between members in how they perceive outer space security, such as the recognition of space as a critical domain for security and defence. Yet, there is no unified position on the optimal strategies for addressing outer space threats. This divergence is particularly evident when comparing NATO's cautious approach, which avoids framing space as a warfighting domain, to the more assertive policies of some members including the US, which emphasize counterspace capabilities.[32]

This divergence in approach stems from varying national priorities, capabilities and perceptions of the threats posed in outer space. Moreover, the evolving outer space landscape, including the proliferation of commercial actors, space debris

---

28 NATO (2023), 'Alliance Persistent Surveillance from Space (APSS)', Factsheet, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230215-factsheet-apss.pdf.
29 Ibid.
30 NATO (2020), 'Defence and Related Security Capability Building Initiative', 23 March 2020, https://www.nato.int/cps/en/natohq/topics_132756.htm.
31 Bearer services transmit information signals between network interfaces.
32 For a more detailed discussion of why these divergent approaches exist, see Erickson, S. and Azcárate Ortega, A. (2023), 'To Space Security and Beyond: Exploring Space Security, Safety, and Sustainability Governance and Implementation Efforts', Geneva: UNIDIR, https://doi.org/10.37559/WMD/23/Space/06.

and emerging technologies, has made it increasingly challenging for NATO members to arrive at a unified one-size-fits-all approach. Broader geopolitics – such as shifting transatlantic security dynamics and changing US defence policies – could further shape NATO's ability to coordinate space security efforts in the coming years.

United States

In 2019, in his first term, President Trump announced the formation of the US Space Force, within the US Armed Forces, and the US Space Command. These were part of the Department of Defense's initiative to achieve and maintain 'space superiority',[33] and were thus criticized by other countries like Russia and China. The Biden administration issued a new framework for space policy, changing the rhetoric from superiority to US 'leadership in space exploration and space science'. The same terminology, referring to the need to maintain space superiority, continues to be used by leading representatives of the US military. It is also a focus of the US chief of space operations' approach to maintaining space superiority, as outlined in March 2024.[34]

The US issued a National Space Policy in 2020 that emphasized the need to 'ensure space systems and their supporting infrastructure […] are designed, developed, and operated using risk-based, cybersecurity-informed engineering'.[35] This policy also expressed the intention to collaborate with industry and other space system operators to develop 'best practices and mitigations'.[36] In the same year, the Department of Defense issued a Space Policy Directive on Cybersecurity Principles for Space Systems, setting clear cybersecurity standards for space systems at all stages of their life cycle.

Building on this, in 2022, the US released a specific Department of Defense Space Policy that 'recognizes space as a priority domain of national military power'. The US also issued the Memorandum on Space Policy Directive-5 on Cybersecurity Principles for Space Systems, effective September 2020.[37] This directive sets out clear definitions and cybersecurity principles and practices that can be integrated into space systems before they are launched.

Furthermore, the US also has extensive international collaboration with Australia, Canada, France, Germany, New Zealand and the UK under the Combined Space Operations initiative. This collaboration involves sharing intelligence and information with each other and increasing interoperability of space infrastructure

---

33 U.S. Department of Defense (2020), 'Defence Space Strategy, Summary', June 2020, https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/2020_DEFENSE_SPACE_STRATEGY_SUMMARY.PDF, p. 1.
34 See Clark, J. (2024), 'Space Force General Outlines U.S. Approach to Maintaining Space Superiority', 28 March 2024, DoD News, https://www.defense.gov/News/News-Stories/Article/Article/3723145/space-force-general-outlines-us-approach-to-maintaining-space-superiority.
35 Archived Trump administration website (2020), 'National Space Policy of the United States of America', https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf.
36 Ibid.
37 Archived Trump administration website (2020), 'Memorandum on Space Policy Directive-5–Cybersecurity Principles for Space Systems', Presidential Memoranda, 4 September 2020, https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems.

among partner nations.[38] The US also extended its operational plan to protect outer space, known as Operation Olympic Defender, to include participation of NATO members.[39] The US is part of NATO's APSS initiative.[40]

However, as the second Trump administration continues to reassess US defence commitments and burden-sharing expectations within NATO, the long-term trajectory of the country's space security partnerships is in question. The increasing reliance of the US and other militaries on commercial satellite networks, particularly Starlink, has introduced new dynamics into transatlantic space security. Starlink's critical role in military operations, including its use in Ukraine, has raised concerns about the implications of privately owned infrastructure in shaping national security outcomes. Although Washington remains a leader in military space policy, its strategic priorities and willingness to extend full-spectrum space security guarantees to NATO partners may evolve in response to broader geopolitical considerations.

United Kingdom

The UK has increasingly positioned itself as a key player in the space domain and published its first national space strategy in September 2021, setting out its defence capability priority areas as satellite communications, Earth observation, ISR, command and control operations, space control for defensive purposes, PNT capabilities, orbital launch capability, in-orbit servicing and manufacturing, and space domain awareness.[41] This strategy set the UK's commitment to invest at £5 billion over 10 years in the military satellite communications sector and £1.4 billion in new technologies and capabilities.

The UK sees great value in an integrated approach between civilian and military space policy actors.[42] To this end, UK Space Command, formed in April 2021, is structured as a joint operation between the UK military forces and civil service. The space command has several duties, including monitoring threats (through the UK Space Operations Centre) and providing ballistic missile early warning and space surveillance capability through RAF Fylingdales. The military-grade space sensor at RAF Fylingdales provides services not only to the UK but also to the US.

The UK also set its Defence Space Strategy in February 2022, categorizing threats in terms of their impact, ranging from non-kinetic to kinetic effects.[43] The strategy mentions cyberthreats as having 'the potential to deny, disrupt or deceive satellites

---

38 U.S. Department of Defense (2022), 'DoD and Partners Release Combined Space Operations Vision 2031', 22 February 2022, https://www.defense.gov/News/Releases/Release/Article/2941594/dod-and-partners-release-combined-space-operations-vision-2031.
39 Hitchens, T. (2020), ' "Major Milestone" As Allies Join SPACECOM's War Plan', 21 May 2020, *Breaking Defence*, https://breakingdefense.com/2020/05/major-milestone-as-allies-join-spacecoms-war-plan.
40 NATO (2023), '16 Allies, Finland and Sweden launch largest space project in NATO's history', 15 February 2023, https://www.nato.int/cps/en/natohq/news_211793.htm.
41 UK Government (2022), *National space strategy*, Policy Paper, updated 1 February 2022, https://www.gov.uk/government/publications/national-space-strategy/national-space-strategy.
42 UK Cabinet Office (2021), 'Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy', 2 July 2021, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.
43 UK Ministry of Defence (2022), 'Defence Space Strategy: Operationalizing the Space Domain', p. 10, https://www.gov.uk/government/publications/defence-space-strategy-operationalising-the-space-domain.

data'.[44] The UK's focus on space security is also closely tied to its collaboration with international partners, and the UK is a participant in NATO's APSS initiative and contributes to the Combined Space Operations partnership alongside the US, Canada, Australia and other members. The UK's National Cyber Force also works to address the growing cyberthreats to space-based assets, among other critical national infrastructure, underscoring the intersection of cyber and space security in the country's defence priorities.[45]

France

France is a leading European power in space. In 2019, it published its Space Defence Strategy, recognizing a broad spectrum of threats in outer space, including anti-satellite tests, cyberattacks, electromagnetic jamming, directed energy weapons and unfriendly proximity operations.[46] The same strategy states that 'cyber-attacks on the software parts of the different segments of space capability are among the most likely threats' and notes the difficulty of attributing these threats.[47] In its space policy, France identified one of its main objectives as ensuring strategic autonomy by developing space capabilities and being able to monitor activity in all orbits through enhanced space situational awareness.[48] Through this capability, France would be able to 'detect and attribute unfriendly or hostile acts'.[49]

In its space policy, France identified one of its main objectives as ensuring strategic autonomy by developing space capabilities and being able to monitor activity in all orbits through enhanced space situational awareness.

In 2019, President Emmanuel Macron also announced the creation of a space command attached to the French Air Force.[50] This led to rebranding the French Air Force as the French Air and Space Force in 2020. Lastly, in order to better collaborate with the space industry, France established a national space innovation laboratory (LISA) within the Ministry of Armed Forces.[51]

---

44 Ibid., p. 11.
45 National Cyber Force (2023), *The National Cyber Force: Responsible Cyber Power in Practice*, https://assets.publishing.service.gov.uk/media/642a8886fbe620000c17dabe/Responsible_Cyber_Power_in_Practice.pdf.
46 The French Ministry for the Armed Forces (2019), *Space Defence Strategy*, Report of the 'space' working group, p. 23, https://cd-geneve.delegfrance.org/IMG/pdf/space_defence_strategy_2019_france.pdf?2194/80ea1f07a5171e4ee796a52752c9bce695d34acb.
47 Ibid.
48 Mission Permanente de la France auprès des Nations Unies à New York (2022), United Nations Disarmament Commission – 2022 Session, Working Group II – 'Espace: Présentation de la politique spatiale de la France' [National Presentation by France] (13 April), https://www.un.org/disarmament/institutions/disarmament-commission/session-2022.
49 The French Ministry for the Armed Forces (2019), *Space Defence Strategy*, p. 9.
50 Ibid.
51 Mission Permanente de la France auprès des Nations Unies à New York (2022), 'Espace: Présentation de la politique spatiale de la France' [National Presentation by France], p. 5.

French space defence strategy outlines the importance of partnership, particularly with the US on space situational awareness, with India on civilian satellite launches,[52] with Japan on space surveillance, and with Canada and Australia on finding new avenues of cooperation.[53] France also is a participant in NATO's APSS but the country has openly acknowledged the need to prepare for potential conflict in space, unlike NATO which avoids framing space as a 'warfighting domain'. France's strategy also acknowledges the growing threats to space security, including space debris, cyberattacks and the development of counterspace capabilities by adversaries.

Canada

Canada's approach to space is guided by its new defence policy, 'Our North, Strong and Free: Renewed Vision for Canada's Defence' published in April 2024, which emphasizes the critical importance of space in safeguarding national security and detecting, deterring and defeating threats.[54] This strategy also highlights the importance of resilience in the space domain, calling for forces that can operate across cyber and space domains that are 'digitalized and networked for the information age'.[55]

In July 2022, Canada established its 3 Canadian Space Division (3 CSD), which is the Air Force's main agency for delivering the space initiatives outlined in Canada's defence policy. This space division will 'streamline, focus, and improve how space-based capabilities support critical CAF requirements such as communications, command and control, navigation, weather and situational awareness'.[56] Canada's previous defence policy from 2017 also outlined a framework for the country to ensure consistent, long-term financial support for various space defence initiatives. This encompassed improving situational awareness, enhancing Earth observation capabilities, and bolstering satellite communications infrastructure.[57] That policy also emphasized the importance of space-based assets for modern militaries and highlighted the potential vulnerabilities and risks to satellites, without explicitly mentioning the cyberthreats to these assets.[58]

---

52 France and India have a long history of partnership (from the 1960s onwards) in the area of peaceful uses of outer space. France also set a bilateral strategic dialogue with India on space in 2022. See Madhusudan, H. (2022), 'How the India and France Space Strategic Dialogue can Address Multi-Dimensional Concerns in 2020s', *The Space Review*, 23 May 2022, https://www.thespacereview.com/article/4389/1.
53 The French Ministry for the Armed Forces (2019), *Space Defence Strategy*, pp. 34–35.
54 Government of Canada (2024), *Our North, Strong and Free: A Renewed Vision for Canada's Defence*, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.
55 Ibid.
56 Government of Canada (2022), 'Establishment of 3 Canadian Space Division', 22 July 2022, https://www.canada.ca/en/department-national-defence/news/2022/07/establishment-of-3-canadian-space-division.html.
57 Government of Canada (2017), *Strong, Secure, Engaged: Canada's Defence Policy*, https://www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf.
58 Ibid., p. 57.

Protecting the alliance's space–cyber nexus

Changes to national-level space policy also affect NATO's security, defence and deterrence strategy. Having realized the need for a multifaceted and integrated domain of operations, NATO and key members (such as the US and the UK), have prioritized the integration of cyber and space capabilities alongside traditional physical domains. The multi-domain operations concept in essence is different from simply joining up the core physical domains (air, land and maritime). It calls for integration across all domains (including cyber and space) to a level whereby each domain can access near real-time information from other domains at all times.

In practice, multi-domain operations come with certain challenges, some of which are related to information and data security. For instance, if real-time information is transmitted through a cloud-based single operating environment then that would raise questions around protection of this environment from cyberattacks given that a single point of failure might cause cascading impacts across domains. Therefore, dependency on a single cloud server to collect and diffuse data – even though such networks may have military-grade cybersecurity solutions – may pose mission-critical risks. Another challenge is to overcome classification barriers across land, sea and maritime domains both within NATO and within each ally country as this would be integral to near real-time information sharing.

Having realized the need for a multifaceted and integrated domain of operations, NATO and key members (such as the US and the UK), have prioritized the integration of cyber and space capabilities alongside traditional physical domains.

NATO and its members may also require new capabilities to successfully execute multi-domain operations. In order to achieve multi-domain autonomy in air, land and maritime domains, the alliance is said to require more than 50 satellites to be operational at all times.[59] Such a level of readiness requires partnership and cooperation across the members. These operations will likely require significant processing power, with artificial intelligence (AI), machine learning and automation solutions. They will also benefit from advancements in quantum technologies, including quantum computing, advanced sensors and quantum communications (such as encryption) technologies, to assist in understanding the environment in which NATO forces are operating.

In the operational space, NATO forces are also dependent on civilian and commercial sectors: 90 per cent of military transport is accomplished using civilian assets chartered or requisitioned from the commercial sector; more than 70 per cent

59 Information shared in an event held under the Chatham House Rule.

of satellite communications used for defence purposes are provided by the commercial sector; and 75 per cent of host-nation support to NATO operations is sourced from local commercial infrastructure and services.[60]

This dependence introduces additional vulnerabilities, as civilian-operated systems may not always adhere to military-grade security standards. This is particularly concerning in the context of multi-domain operations, where the seamless integration of data across domains is essential for mission success. A breach in a civilian-operated system could cascade across NATO's operations, affecting real-time communication, situational awareness and decision-making.

At the same time, the weaponization of space presents escalating risks to both Earth-based critical infrastructure and the peaceful uses of outer space. Despite the potential long-term consequences for orbital sustainability, states continue to invest in military and dual-purpose counterspace capabilities. These include technologies developed for benign purposes, such as rendezvous and proximity operations (RPO) or on-orbit servicing (OOS), which can be repurposed into aggressive tools like anti-satellite (ASAT) weapons.[61] Such dual-purpose systems blur the line between their intended functions and their potential use as offensive tools. Counterspace capabilities can be categorized as follows: a) capabilities with kinetic physical effects such as ASAT, including direct-ascent ASAT and co-orbital ASAT weapons; b) capabilities with non-kinetic but physical effects,[62] such as lasers and high-powered microwave (HPM) weapons; c) electronic means that target the electromagnetic spectrum, such as jamming capability; and d) cyber means that could result in either short-term or permanent effects, depending on the targeted system and intention of the adversary.[63] The expansion of counterspace capabilities by states has exacerbated vulnerabilities in the space domain while heightening the risk of unintended escalation.

Cyberattacks, in particular, offer a degree of flexibility and deniability, due to the lengthy and often disputed process of attribution. Cyberattacks are also typically lower cost and more accessible compared to developing and deploying sophisticated kinetic counterspace weapons that require overt physical destruction. Offensive cyber operations can disable, disrupt or manipulate satellites and their supporting infrastructure.

This potential for impact and the scope for deniability make cyberattacks a preferred tool for a broader range of actors, including states with limited resources, which are seeking to disrupt space-based systems without the more overt consequences of kinetic actions. Kinetic and non-kinetic physical capabilities, such as ASAT weapons or high-powered lasers, often carry the risk of unintended or unnecessary escalation that a state may not be willing to take at that point in time.

---

60 NATO (2024), 'Resilience, civil preparedness and Article 3', 13 November 2024, https://www.nato.int/cps/bu/natohq/topics_132722.htm.
61 Azcárate Ortega, A. (2023), 'Not a Rose by Any Other Name: Dual-Use and Dual-Purpose Space Systems'.
62 These capabilities can cause physical impact without having physical contact with the source.
63 For a detailed explanation of this classification, see Swope, C. et al. (2024), 'Space Threat Assessment 2024', https://www.csis.org/analysis/space-threat-assessment-2024.

04
A three-tiered approach to protect critical assets

The proposed framework of mitigation, adaptation and resilience offers NATO a strategic method to protect space systems from cyberattacks, combining technical defences, proactive planning, and recovery capabilities for sustained operational strength.

Protecting NATO's space-based assets from cyberattacks requires a holistic approach: one that ensures operational continuity while preparing for evolving challenges. This paper builds upon existing cybersecurity and resilience models to propose a three-tiered framework – based on mitigation, adaptation and resilience – as a structured method for addressing both immediate and long-term threats to critical systems.

While elements of this approach are reflected in NATO's broader cybersecurity and other defence strategies, its application to space-based assets is underexplored.[64] This framework offers a new way of conceptualizing NATO's space cybersecurity posture, integrating insights from cybersecurity best practices, resilience theory and NATO's own ongoing efforts to enhance its space and cyber capabilities. By focusing on these three tiers, this paper provides a roadmap for NATO and its members to develop more coordinated and forward-looking strategies for securing space infrastructure against cyberthreats.

64 Mitigation and adaptation, for example, are central components of NATO's Climate Change and Security Action Plan; see NATO (2023), *NATO Climate Change and Security Action Plan: A Compendium of Best Practice*, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230710-climate-change-best-practices.pdf.

The three tiers each play a vital role in this framework. Mitigation measures are fundamental for implementing 'quick fixes' in order to limit or minimize the impact of threats. As these are often technical and operationally focused, they are among the most feasible for near-term implementation across the alliance.

There is a direct relationship between mitigation and adaptation: if threats cannot be mitigated or prevented, the military needs to learn how to adapt to new realities within the changing security environment.

Adaptation, by contrast, requires a long-term commitment to innovation and flexibility. It involves the development of new strategies, training programmes and technologies to adjust to an evolving threat landscape. There is a direct relationship between mitigation and adaptation: if threats cannot be mitigated or prevented, the military needs to learn how to adapt to new realities within the changing security environment.

The third tier is resilience. Resilience measures that are focused on long-term solutions will enable a system not only to recover from shocks but also to adapt and evolve towards a new more sustainable state. Resilience involves integrating lessons learned into operational practices and fostering a culture of preparedness across the alliance. Resilience measures often require significant investment and coordination, but their long-term benefits are critical for NATO's ability to maintain its operational edge in an increasingly contested space environment.

Mitigation measures

Mitigation measures aim to minimize the impact of cyberattacks on critical infrastructure by implementing initiatives that limit vulnerabilities and reduce potential damage. For space-based assets, these strategies focus on proactively addressing risks and enhancing the security of systems at every stage of their life cycle, from design and development to operation and decommissioning.

Traditional security approaches to protecting critical assets and systems against cyberattacks are also relevant for securing space assets. These approaches include establishing defence layers throughout critical systems or securing systems throughout their life cycle, and should be part of any mitigation strategy.

Measures to mitigate cyberattacks on space-based assets could include leveraging cryptography techniques, harnessing AI and machine-learning techniques, addressing cryptographic limitations, prioritizing investment in post-quantum cryptography, and enhancing interference and intrusion detection.

The cryptography methods for securing data and communications are constantly advancing in response to new and evolving cyberthreats. As a result, adopting the latest encryption techniques has become standard practice for safeguarding both

information and operational technologies. These techniques should be approved by NATO agencies prior to their use. Other than providing end-to-end encryption methods and authentication of the user's identity across critical systems, it is fundamental to make use of cryptographic algorithms to provide encryption between satellite communication anchor stations and terminals. Establishing the necessary requirements for 'payload telemetry encryption' across NATO members' capabilities (e.g. in Earth observation, communications) would strengthen these systems.[65]

AI and machine-learning techniques could also be used for 'cryptographic problems'[66] – for instance, to detect intrusions or discover vulnerabilities in real time. While NATO members should harness the positive applications of AI-enabled techniques, they should also make sure that those techniques and technologies adhere to the NATO principles of responsible use of AI, adopted in October 2021.[67]

While cryptography techniques are valuable for securing data, they come with limitations, including the possibility of developers employing algorithms containing unidentified problems, or users selecting weak cryptographic private keys, all of which can potentially result in vulnerabilities and easier decryption.[68] Using pseudorandom binary codes would make it harder for the intruder to predict the cryptographic algorithm or the key to access sensitive information.[69] These techniques should be part of transmission security.[70]

It is also fundamental to roll out policies around quantum key distribution (a form of encryption that uses quantum properties) and to prioritize investment in post-quantum cryptography today to safeguard critical national infrastructure within the alliance against potential vulnerabilities, particularly as the threat that quantum computers pose to current cryptography increases.[71] The US's Cybersecurity and Infrastructure Security Agency (CISA) has released a 'Post-Quantum Cryptography Roadmap' that outlines actionable guidelines for organizations, such as carrying out an inventory of current cryptographic technologies, creating acquisition policies on post-quantum cryptography, and educating the workforce about changes ahead.[72]

---

65 For more information, see The Consultative Committee for Space Data Systems (2011), 'Space Missions Key Management Concept', Informational Report, CCSDS 350.6-G-1, Green Book, https://public.ccsds.org/Pubs/350x6g1.pdf.
66 Federal Office for Information Security (n.d.), 'Applications of Artificial Intelligence in Cryptography', https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/KI-in-der-Kryptografie/ki-in-der-kryptografie_node.html.
67 NATO (2021), *Summary of the NATO Artificial Intelligence Strategy*, https://www.nato.int/cps/en/natohq/official_texts_187617.htm.
68 IEEE Cyber Security (2015), 'Use Cryptography Correctly', 13 November 2015, https://cybersecurity.ieee.org/blog/2015/11/13/use-cryptography-correctly.
69 Committee on National Security Systems (2012), 'National Information Assurance Policy for Space Systems Used to Support National Security Missions', 28 November 2012, CNSSP No. 12, p. 3, https://www.hsdl.org/?view&did=726945.
70 Rouse, M. (2013), 'Transmission Security (TRANSEC)', 29 August 2013, https://www.techopedia.com/definition/25857/transmission-security-transec.
71 National Cyber Security Centre (2024), *Next steps in preparing for post-quantum cryptography*, Paper, 14 August 2024, https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography.
72 U.S. Department of Homeland Security (2021), 'Preparing For Post-Quantum Cryptography', https://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf.

States should also invest in technical capabilities to separate random errors from genuine threats. Reliable interference or intrusion detection capabilities – for instance, warnings on spoofing incidents – could provide protection against sophisticated cyberattacks.

The alliance should establish smart procurement requirements for integrated capabilities and have a directory of accredited providers that offer mature cybersecurity products and services. Additionally, information assurance requirements should be incorporated throughout the entire life cycle of space systems.[73]

Adaptation measures

While mitigation strategies aim to resist attacks and, if possible, prevent them and minimize their impact on a system, adaptation strategies involve accepting the inevitability of an attack and its effects, as well as adjusting to the new operating environment. As observed in cyberattacks on other critical national infrastructure, adaptation is a key part of coping with such a threat.

In biology, adaptation is a 'process of change by which an organism or species becomes better suited to its environment'.[74] It has been increasingly used in systems engineering and social sciences. For instance, adaptation has been part of the debate around climate, especially regarding the processes of adjusting to the effects of climate change.[75]

Both reactive and proactive adaptation measures are key in strengthening NATO forces and their response to cyberattacks. Reactive adaptation requires adapting to the operating environment when an adversary neutralizes NATO's space services and products. Reactive adaptation happens on the ground due to an unexpected change. Military forces may need to adapt to a new operating environment for multiple reasons, including situations where GNSS is disrupted, instances where there is insufficient or excessive information inundating early warning systems, or when allied forces become aware of a reliance on spoofed data.

Proactive adaptation happens gradually, and it relies on future-looking capabilities (such as strategic foresight). Examples of proactive adaptation may include conducting training and teaching operators to switch between high-tech and low-tech environments.

---

73 Committee on National Security Systems (2012), 'National Information Assurance Policy for Space Systems Used to Support National Security Missions', p. 6.
74 Oxford Learner's Dictionaries (n.d.), 'adaptation', https://www.oxfordlearnersdictionaries.com/definition/english/adaptation.
75 The European Union has been calling for 'smarter, faster, and systemic' adaptation to climate change. See European Commission (2021), 'Forging Climate Resilient Europe – the New EU Strategy on Adaptation to Climate Change', 24 February 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:82:FIN.

Resilience measures

From protecting critical national infrastructure to societal and individual awareness against disinformation campaigns, resilience has a key preventative role in NATO's defence. One key outcome of the Brussels NATO summit in 2021 was to 'adopt a more integrated and better coordinated approach' to resilience.[76] Resilience is not a new concept within NATO. Article 3 of the Washington Treaty provides the basis for each NATO ally to be resilient, requiring that 'separately and jointly, by means of continuous and effective self-help and mutual aid [the members] will maintain and develop their individual and collective capacity to resist armed attack'.[77]

At the Warsaw Summit in 2016, allied leaders committed to enhancing resilience, indicating the need to reinforce civilian infrastructure and boost resources that are fundamental to supporting military operations.[78] The framework noted seven baseline requirements:

- assured continuity of government and critical government services;
- resilient energy supplies;
- ability to deal effectively with the uncontrolled movement of people;
- resilient food and water resources;
- ability to deal with mass casualties;
- resilient communication systems; and
- resilient transportation systems.[79]

An unidentified theme across the seven baseline requirements is the dependency of critical infrastructure on space-based assets. The government sector in each NATO state, for instance, requires both cables and satellites to have secure and encrypted communication channels between capitals and their permanent missions in sensitive regions and across members. The energy sector relies on space data for monitoring oil and gas pipelines, the grid, power stations and wind turbines, among other things. The continuous functioning of the energy sector is critical for national and economic security. Earth observation services are essential for monitoring the uncontrolled movement of people, such as migrants and internally displaced persons, as well as for forecasting floods, and monitoring crops and natural coastal defences against extreme weather. Emergency services (such as ambulance or fire units) that deal with mass casualties also rely on satellite communications and PNT technologies for command-and-control functions. Even moving patients from one place to another relies on GPS; airliners, ports and rail services are equally dependent on satellite navigation and communication systems. These services are vital both in periods of peace and times of conflict.

---

76 NATO (2021), 'Strengthened Resilience Commitment', https://www.nato.int/cps/en/natohq/official_texts_185340.htm.
77 NATO (1949), 'The North Atlantic Treaty', https://www.nato.int/cps/en/natohq/official_texts_17120.htm.
78 Roepke, W. and Thankey, H. (2019), 'Resilience: the first line of defence', 27 February 2019, https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.
79 Ibid.

The key approaches to resilience in this realm can be summarized as:

1. Adopting a systems approach by identifying critical systems and by mapping system architecture. All NATO members should conduct a similar exercise and confidentially share information with NATO when possible. This would help the alliance to assess weaknesses across systems, and to tailor resilience approaches according to the needs of each ally.
2. Preparing for and reacting to disturbances by diversifying systems and incorporating necessary redundancy measures before an incident occurs. In defence terms, redundancy refers to the deliberate inclusion of back-up systems or elements that can assume the function of a primary system if it fails or is compromised. This would include diversifying vulnerabilities across multiple systems so as to minimize a single point of failure.[80] For instance, this could be achieved by incorporating redundancy capabilities to take over from primary ones in case of stress.

Diversification can be achieved in different areas. Some researchers, for instance, argue that to secure satellites, it is better to invest in smaller satellites rather than larger ones, because 'the distribution of greater numbers of satellites would make the loss of any one satellite less catastrophic to the architecture as a whole'.[81] Such a distributed architecture could have thousands of satellites providing continuous coverage. For example, Starlink is composed of '1,000 satellites circling in LEO to provide continuous coverage over large parts of the Earth, with users of the system automatically being transferred between satellites as they pass in and out of range'.[82]

In order to prevent vulnerabilities within highly networked systems, NATO's baseline requirements could incorporate 'defence-in-depth' strategies, which would create protection across systems by using multiple layers of cybersecurity.

Highly networked small satellites could nonetheless be as vulnerable to cyberattacks as larger satellites. In order to prevent vulnerabilities within highly networked systems, NATO's baseline requirements could incorporate 'defence-in-depth' strategies, which would create protection across systems by using multiple layers of cybersecurity.[83] This could require integrating zero-trust security architecture across all allied states; such an approach ensures that every user and device must undergo rigorous identity verification before accessing any network resources, even

80 Single point of failure refers to any non-redundant system's failure, which would cause a failure of the entire system.
81 Pollpeter, K. (2015), 'Testimony before the U.S.-China Economic and Security Review Commission for the hearing on "China's Space and Counterspace Programs"', 18 February 2015, https://www.uscc.gov/hearings/hearing-chinas-space-and-counterspace-programs.
82 Harrison, T., Johnson, K. and Young, M. (2021), 'Defence against the Dark Arts in Space', *Center for Strategic and International Studies*, February 2021, p. 12, https://aerospace.csis.org/wp-content/uploads/2021/03/032321_HarrisonJohnsonYoung_DefenseAgainstDarkArtsInSpace_Report_Update-compressed.pdf.
83 Cyberark (n.d.), 'What is Defense-in-Depth?', https://www.cyberark.com/what-is/defense-in-depth.

if they are already operating inside the network's perimeter.[84] Other defence-in-depth strategies cover the mitigation measures discussed earlier, including protection against viruses and malware, patching, intrusion detection methods, encryption and authentication measures.

Table 1. Alternative PNT solutions

Alternative PNT solutions	Capability	Use case	Disadvantages
Terrain contour matching (TERCOM)	• Navigation system: Pre-recorded contour map of the terrain is assessed against measurements during the flight.	Cruise missiles (such as Tomahawk missiles)	• Limited data storage and computing systems. • Requires the pre-planning of the entire route of the launch, including its original launch point, otherwise it loses course.
Digital scene matching area correlator (DSMAC)	• Navigation system with autonomous missile guidance • Uses residual or infrared cameras • High-precision positioning[85]	Cruise missiles (such as Tomahawk or Kalibr missiles)	• Temporal changes in features, including shadows or seasonal changes in foliage, affect the reliability of DSMAC processing.[86]
Inertial navigation systems (INS)	• Navigation system • Allows for accurate tracking of an object's position and orientation in space.[87]	Dead reckoning navigation systems[88]	• Exposed to drift and errors of sensors.[89]
Quantum inertial sensing[90]	• Navigation system • Matter-wave inertial sensors	[Current research in laboratories]	• Does not entirely remove the drift and errors of inertial navigation sensing.[91]
Miniaturized atomic clocks	• Timing system: chip-scale atomic clocks with high-performance improvements.[92]	[Future implementation]	• Expensive and current performance is low due to 'physics associated with their designs'.[93]
Quantum enhanced atomic clocks	• Timing system: improving timing synchronization, and clock precision.	Future application in military communications and electronic warfare.	• Currently only at 'proof of principle' stage of development.[94]

Source: Compiled by the author.

84 Terry, R. (2025), 'Zero Trust Security Explained: Principles of the Zero Trust Model', 13 March 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security.
85 Irani, B. G. and Christ, P. J. (1994), 'Image Processing for Tomahawk Scene Matching', *Johns Hopkins APL Technical Digest*, 15(3), p. 250, https://www.jhuapl.edu/Content/techdigest/pdf/V15-N03/15-03-Irani.pdf.
86 Ibid., p. 254.
87 Turek, P., Grzywiński, S. and Bużantowicz, W. (2020), 'Selected Issues and Constraints of Image Matching in Terrain-Aided Navigation: A Comparative Study', https://www.intechopen.com/chapters/74476.
88 Wright, M. J. et al. (2022), 'Cold atom inertial sensors for navigation applications', Frontiers in Physics, 10:994459, doi: 10.3389/fphy.2022.994459.
89 Ibid.
90 Bouyer, P. (2016), 'Quantum technology for a new generation of inertial sensors', *The International Society for Optics and Photonics*, 1 March 2016, https://spie.org/news/6312-quantum-technology-for-a-new-generation-of-inertial-sensors?SSO=1.
91 Wright, et al. (2022), 'Cold atom inertial sensors for navigation applications'.
92 United States Government Accountability Office (2021), *Defense Navigation Capabilities*, Report to the Committee on Armed Services, U.S. Senate, https://www.gao.gov/assets/gao-21-320sp.pdf.
93 Ibid.; Technology.org (2019), 'DARPA Making Progress on Miniaturized Atomic Clocks for Future PNT Applications', 21 August 2019, https://www.technology.org/2019/08/21/darpa-making-progress-on-miniaturized-atomic-clocks-for-future-pnt-applications.
94 Department of Physics, University of Oxford (2022), 'A quantum network of entangled atomic clocks', 8 September 2022, https://www.physics.ox.ac.uk/news/quantum-network-entangled-atomic-clocks.

Redundant, mobile and hardened ground stations are equally important in times of conflict as they represent the most vulnerable component of a space system to cyberattacks. Ground stations serve as the primary interface between satellites and Earth, enabling command, control and communication functions. This makes them an attractive target for adversaries seeking to disrupt operations, compromise data integrity or deny access to critical services. These vulnerabilities highlight the need to prioritize the protection of ground infrastructure through robust cybersecurity measures and redundancy.

Across satellite capabilities, PNT technology requires protection and resilience. Current PNT systems rely heavily on GPS and GNSS solutions – however, as argued in an earlier paper on the subject, these systems can be vulnerable to cyberhacking.[95] GPS and GNSS signals are also susceptible to jamming; therefore, their use in times of conflict is challenging. Thus, alternatives[96] to GPS may help to support the alliance.

95 Unal (2019), *Cybersecurity of NATO's Space-based Strategic Assets*.
96 The UK Ministry of Defence is considering navigation options and has requested that companies report about commercial technologies used for navigation purposes. See UK Government (2022), 'Alternative Navigation for Weapon Systems: Market Exploration Document', 17 February 2022, https://www.gov.uk/government/publications/market-exploration-alternative-navigation-for-weapon-systems/alternative-navigation-for-weapon-systems-market-exploration-document.

05 Further recommendations and conclusions

NATO should seek to enforce procurement standards, collaborate with industry, and promote cross-domain integration. Embedding mitigation, adaptation and resilience across policy and operations is essential to maintain strategic advantage in space.

NATO's ability to secure its space-based assets hinges on adopting a comprehensive strategy that aligns with the three-tiered framework of mitigation, adaptation and resilience. The framework proposed in this paper serves as a guiding principle for addressing the challenges posed by the increasingly contested and interconnected space and cyber domains. NATO must focus on ensuring that its space assets are resilient, secure and capable of recovering quickly from disruptions.

Beyond the recommendations outlined in the three-tiered framework, the following recommendations aim to address the challenges in the space-cyber domain while considering the feasibility and prioritization of actions within NATO's framework:

1. **Implement industry-based practices and restrict who can access space assets as part of a layered defence approach.**
   As discussed in the section on mitigation, securing space assets requires comprehensive life cycle-focused cybersecurity measures. NATO should establish rigorous procurement standards for space-related systems and mandate practices including cryptographic encryption, post-quantum

readiness and intrusion detection. These measures, supported by industry standards, directly address the vulnerabilities posed by the alliance's reliance on civilian and commercial systems.

2. **Share best practices and lessons learned among members.**
   Given the diversity in national approaches to space and cybersecurity within NATO, fostering knowledge exchange is essential. By learning from successful mitigation and adaptation efforts across the alliance, for example through NATO's Joint Analysis and Lessons Learned Centre, NATO can harmonize its approaches and develop robust responses to shared challenges.

3. **Make good use of the NATO Space Technology Centre in order to support NATO missions and operations.**[97]
   The centre provides a unique opportunity to integrate advancements in AI, quantum technologies and cryptography into NATO's space-based operations. Using this platform to develop proactive and reactive capabilities will help NATO to address emerging threats while ensuring its technological edge.

4. **Establish policies with commercial actors to tap into non-military research and innovation.**
   With more than 70 per cent of NATO's satellite communications provided by the commercial sector, the private space industry plays a critical role in NATO's operational readiness. Building stronger partnerships ensures that commercial assets align with NATO's security requirements while fostering innovation and diversity in technological solutions.

5. **Encourage and facilitate increased collaboration between the space and cyber domains within NATO.**
   As emphasized throughout the paper, the space and cyber domains are inherently interconnected. Establishing cross-cutting teams and initiatives, such as those focused on joint training and knowledge-sharing, will enhance the alliance's ability to address threats that span these domains.

Conclusion

The rapid evolution of warfare, security and national resilience is increasingly shaped by advancements in technology, cyber capabilities and the militarization of space. These shifts are happening simultaneously and are taking place against a backdrop of heightened geopolitical tensions, with both state and non-state actors seeking to exploit vulnerabilities in critical infrastructure. In this context, the space–cyber nexus is no longer a theoretical concern but a real and pressing security challenge.

97 NATO (2021), 'NATO's Approach to Space', 2 December 2021, https://www.nato.int/cps/en/natohq/topics_175419.htm.

NATO also faces mounting strategic uncertainties, including shifting defence priorities among key member states, evolving national policies on space security, and increasing reliance on commercial space assets. These factors raise critical questions about NATO's ability to maintain collective defence commitments in the space domain.

Recent events, including Russia's invasion of Ukraine, have highlighted how vulnerable space-based assets are to cyberattacks, underscoring the urgent need to protect them from disruption. Cyberattacks on space-based assets can disrupt military operations, interfere with communications and have spillover impacts on civilian infrastructure. As NATO and its members deepen their reliance on space-based systems, the urgency of securing these assets against cyberthreats has never been greater.

While NATO has made strides in developing space and cyber capabilities, the framework proposed in this paper presents a new way of conceptualizing space cybersecurity within the alliance and more broadly, helping to bridge technical resilience with strategic policy responses.

By embedding the principles of mitigation, adaptation and resilience into the space and cyber strategies of both NATO and its members, the alliance can strengthen its overarching defence posture, enhance operational continuity and safeguard the integrity of its space infrastructure. Securing space-based assets is not just a technical necessity but a strategic imperative that will shape NATO's ability to deter threats, respond to crises and remain relevant in the years ahead.

About the author

Julia Cournoyer is a research associate in the International Security Programme at Chatham House and associate editor of the *Journal of Cyber Policy*. Her research primarily covers projects related to nuclear weapons policy, emerging technology, conflict prevention, biosecurity, cybersecurity and outer space security. In 2023, Julia was selected as a nuclear scholar with the Centre for Strategic and International Studies Project on Nuclear Issues (CSIS PONI Nuclear Scholars Initiative), and in 2024 was selected as a Ploughshares Nuclear Futures fellow. She has a master's in international security from the Paris School of International Affairs (Sciences Po) and a BSc in international relations from the London School of Economics and Political Science (LSE).

Acknowledgments

The research behind this paper benefited greatly from the insights and advice of several experts. The author would like to extend special thanks to Dr Beyza Unal for her invaluable contributions to this research. Dr Unal originated the concept of a three-tiered approach to protecting critical infrastructure and provided the first draft of this paper while working at Chatham House as deputy director of the International Security Programme. Dr Unal also authored a research paper, *Cybersecurity of NATO's Space-based Strategic Assets*, on this topic that provides the foundation for this research. The author is also deeply grateful for her mentorship and guidance over the past few years, which have been instrumental in shaping the author's thinking and approach.

The author is also grateful to colleagues including Dr Marion Messmer, Joyce Hakmeh, Dr Samir Puri, Jake Statham, Amanda Moss and Mike Tsang for their conceptual and editorial feedback, which greatly enhanced the paper. Thanks are also due to colleagues in the International Security Programme at Chatham House for their support throughout the drafting process.

The author further wishes to thank the anonymous peer reviewers for their thoughtful and constructive comments, which strengthened and refined the final version of the paper, as well as the various experts consulted during the course of this research.

Finally, the author expresses sincere gratitude to the Norwegian Ministry of Defence for funding this stream of work.

Cover image: Satellites fill the sky over Alberta, Canada, June 2024.
Photo credit: Copyright © Alan Dyer/VWPics/Universal Images Group/Getty Images

ISBN 978 1 78413 643 7
DOI 10.55317/9781784136437

Cite this paper: Cournoyer, J. (2025), *Securing the space-based assets of NATO members from cyberattacks: A framework to strengthen cybersecurity in outer space*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136437.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223