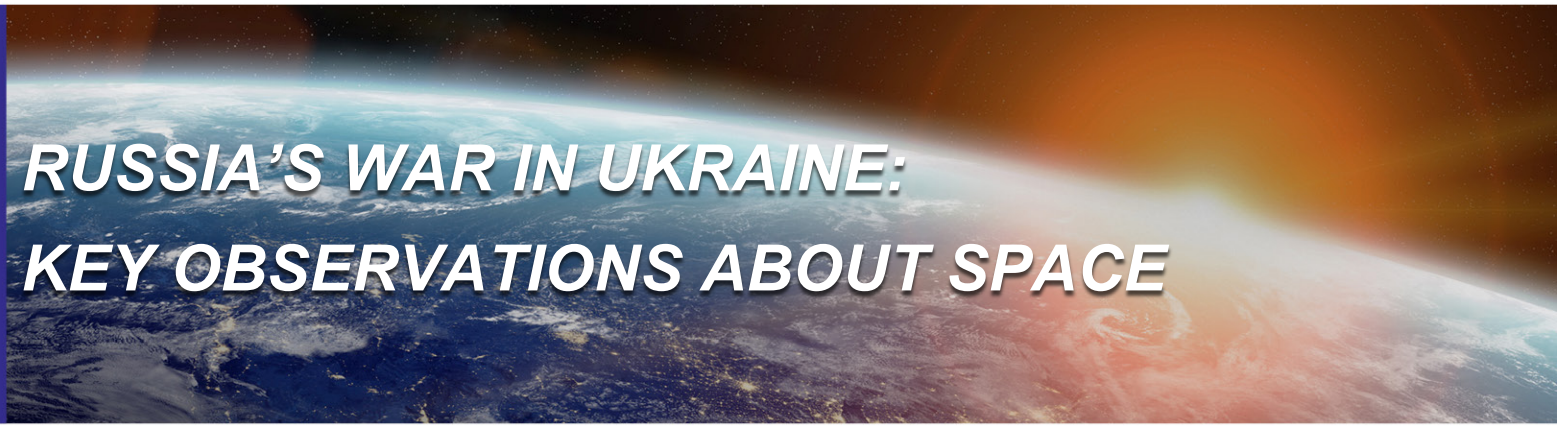
SPACE AGENDA 2025



RUSSIA'S WAR IN UKRAINE: KEY OBSERVATIONS ABOUT SPACE

Michael P. Gleason

Executive Summary

The war in Ukraine offers lessons for the U.S. Department of Defense (DOD) and the U.S. Space Force (USSF). While focusing on the ground-based components of space systems and on the importance of integrating data from space capabilities at the battle-edge, this chapter highlights several lessons including:

- A key reason Russia has not been able to exploit its advantage in sovereign space capabilities compared to Ukraine is that Russian forces have not sufficiently integrated data from Russian space capabilities at the operational and tactical levels.
- In sharp contrast, Ukraine has successfully integrated data from space and disseminated it quickly to the warfighter using innovations in *ground-based* space system hardware, software, and applications.
- Ukraine shows that independent access to space and fleets of satellites is not sufficient for advantage in war. Innovations in ground-based technology have done just as much, if not more, than the satellite capabilities themselves to maximize the effectiveness and lethality of Ukrainian forces.

While Russia has attacked and continues to threaten commercial space ground systems and data networks, the war in Ukraine also warns that commercial satellites should not expect to be exempt from attack, including destructive attacks, in a war that extends into space. Moreover, Russian physical, cyber, and electronic attacks in Ukraine against commercial space systems' ground and link segments warn similar attacks will occur in future conflicts. Commercial ground and link segments, which are crucial for the warfighter, must be protected.

In addition, the vulnerability of commercial space systems should incentivize the United States to accelerate changes to regulations, policy, bureaucracy, systems, and operations to enable sharing data from hardened U.S. military space capabilities. Innovators must come up with new ideas to meaningfully improve data access for allies and partners.

Finally, the USSF should evaluate its priorities and investment decisions to see if they adequately reflect the importance of integration, networks, and other components of the ground-based segment of space systems.

Introduction

Prior to Russia's further invasion of Ukraine in 2022, most national security experts would have predicted that Russia would gain significant advantage from its outer space capabilities in the event of an intensified conflict between the two nations. After all, Russia has independent access to space, decades of experience using space for military purposes, and significant satellite and counterspace capabilities, while Ukraine had neither a space program nor any national satellites. As the war has unfolded, it is actually Ukraine that has been more effective utilizing space-based capabilities. Ukrainian forces have successfully leveraged commercial space services, including imagery, radar, and communications, to enable communications among their forces and to target Russian forces.

The war in Ukraine offers lessons for the Department of Defense (DOD) and the U.S. Space Force (USSF) on how future conflicts could extend to space. This chapter highlights three of those lessons.

First, Ukraine's innovative use of data and networks to provide actionable information to fielded forces has had a powerful effect on the battlefield. Although satellites tend to draw the most attention among strategists and policymakers, ground systems and data networks have proven vital to Ukrainian forces' ability to integrate the data from space into their operations and weapon systems. Effective data integration has strengthened Ukraine's defense against numerically superior Russian forces.

Second, Russia has attacked and continues to threaten commercial space ground systems and data networks in this war, suggesting Russia knows how critical these capabilities have been for Ukraine. This highlights the vulnerability of ground systems and data networks. These segments of space systems (whether commercial or military) will likely be targeted in future conflicts that extend to space. To date, Russia's attacks have consisted of temporary, reversible attacks against satellites or cyberattacks against ground infrastructure and not destructive attacks against the satellites themselves, signaling some level of restraint. Russia's attacks have raised questions about how, if at all, the United States should protect commercial space systems that come under attack in a conflict.

Finally, Russia's attacks on commercial space systems makes a case for the United States to make the data from hardened, jam resistant U.S. military space capabilities significantly more available to allies, partners, and other supported nations.

Ukraine's Use of Commercial Space Capabilities

In its fight against Russia's invasion and occupation of its territory, Ukraine has benefitted greatly from its access to global commercial space services. At the start of the war, a member of Ukraine's cabinet wrote a letter to eight space remote sensing companies asking for their support.[1] Commercial electro-optical imagery and synthetic aperture radar companies, which can detect movements at night and through clouds, have helped Ukraine's military forces target Russian assets and carry out battle damage assessments.[2] In March 2022, HawkEye 360, a commercial radiofrequency mapping company, publicly announced "the capability to detect and geolocate Global Positioning System (GPS) interference, with analysis of data over Ukraine revealing extensive GPS interference activity."[3] Even prior to Russia's invasion and during the early days of the conflict, commercial remote-sensing satellites helped monitor the Russian buildup of forces and troops within occupied Ukraine and in Russia and Belarus, providing observers around the world a compelling picture of what was happening on the ground.

Commercial satellite communications have also been fundamental to Ukraine's defense. The commercial companies that have provided information to Ukraine include Viasat, OneWeb, SES, Iridium, Inmarsat, Eutelsat, Avanti, and, most prominently, Starlink. President Zelensky has used Starlink to connect to Ukrainians, national parliaments, and international organizations around the world. Ukrainian forces have used Starlink for secure communication and situational awareness, connecting leadership to military units on the battlefield. The capability has also facilitated "tele-maintenance"

of weapon systems in Ukraine. When something has broken, Ukrainian forces have used Starlink to connect with U.S. maintenance specialists at a base in Poland to diagnose and resolve the problem via video.[4]

Lesson 1: Prioritize Integration Between Satellites and Terrestrial Forces

A key reason Russia has not been able to exploit its advantage in indigenous space capabilities is that Russian forces have not sufficiently integrated data from their space capabilities at the operational and tactical levels. Analysis suggests there are several reasons for this, including inadequate doctrine, strategy, training, material investment, and a lack of priority on "getting space support to the warfighter," (as is said in U.S. military parlance).[5] An assessment of Russia's space capabilities from 2019 indicated that even its newest space-based ISR systems had issues: "In addition to the high failure rate of the satellites, the products and services that they do provide often fail to meet the requirements of end users and are not competitive with equivalent foreign capabilities."[6]

In sharp contrast to Russia's failures to integrate data from space, Ukraine has demonstrated that what matters is not only what satellite data or services are provided, but also how they are delivered to the warfighter. Innovations in ground-based satellite hardware, software, and applications allow Ukrainian units in the field to rapidly process and disseminate information from satellites. The networked, distributed approach to using and sharing information from space pursued by Ukraine and its allies has demonstrated the asymmetric advantages of this approach compared to the centralized, hierarchical structure used by Russia. Enabled by commercial telecommunication satellites (including Starlink among others), and while leveraging data from a wide variety of commercial remote sensing satellites, Ukrainian forces have been able to innovate and adapt with more decentralized command and control and more direct communications and coordination between tactical units.

One reason the impact has been so significant is the underlying environment that enabled or encouraged data to be shared quickly with key stakeholders. The ground-based hardware, software, and applications allowing units to rapidly process and disseminate information have proven invaluable to Ukrainian military efforts against Russia. Ukrainian forces have also benefited from receiving raw data, which enables customization, rather than processed data, along with requisite training on how to exploit the raw data flexibly. The timeline for transferring data from space to warfighters has dropped from days to hours or, in some circumstances, to fewer than 10 minutes.[7]

The "Uber for artillery" application, GIS Arta, allows units collecting information on potential targets, including from satellites, to share that information directly with units that could fire on the targets.[8] This application pairs sensors with shooters in a decentralized network instead of having to funnel specific information up and back down through centralized command nodes. As another example, Palantir software can draw imagery from a total of 306 commercial satellites. Soldiers in battle can use handheld tablets to request more satellite coverage if they need it.

Western military and intelligence services work closely with Ukrainians to facilitate this information sharing.[9] Cloud-based environments have also helped remove data stovepipes and minimize the need to translate between systems.[10]

Russia's inability to accomplish these tasks helps explain the underwhelming contribution of its superior space capabilities to its fight in Ukraine. While space power theory, doctrine, and strategy often stress the importance of satellites, Ukraine shows that independent access to space and fleets of satellites are not sufficient for providing an advantage in war. Accessing commercial innovations and implementing practices for sharing satellite information at the battle edge have done just as much, if not more, than the satellite capabilities themselves to maximize the effectiveness and lethality of Ukrainian forces in the war.

Applications to U.S. Doctrinal Concepts. Russia's war in Ukraine provides an opportunity to test some doctrinal concepts as espoused in the 2020 USSF document, *Space Capstone Publication: Spacepower, Doctrine for Space Forces*. The Space Capstone Doctrine asserts that space systems provide their greatest potential when *integrated* with other forms

of military power and states a spacecraft provides little value if the data it provides cannot be exploited.[11] Underlining this doctrinal concept, in April 2023, then-Major General David Miller—who at the time was director of operations, training, and force development for the U.S. Space Command—observed that warning, surveillance, and targeting information coming from satellites ultimately had no value if it could not be delivered to the warfighter in a tactically useful time-frame.[12]

Disseminating data from space rapidly and then making that data useful tactically (for example, by integrating it into weapon systems) for warfighters in other domains is not a simple task. It took significant investment and many years for U.S. joint forces to become proficient at it, and there is still plenty of room for improvement.[13] Along with apt doctrine, strategy, and training, making data useful requires sophisticated networks, data processing software, automation, tailored applications, adequate spectrum, decentralized data-sharing processes, and requisite hardware (for example, antennas, modems, and user equipment suited to harsh environments). Assessing Russia's and Ukraine's different experiences in making use of data from satellites validates the doctrinal claim that a satellite's value is directly tied to the end user's ability to effectively use data from the satellite when and where they need it.

These observations underscore the importance of space doctrine, information-sharing processes, and ground-based enabling segments beyond the satellites, whether commercial or government owned. Russia's inability to exploit its space superiority relative to Ukraine and Ukraine's ability to exploit space even though it lacks satellites confirm USSF doctrinal assertions and senior leader statements that space systems provide little value if the data they provide cannot be exploited.[14]

However, Russia's war in Ukraine provides opportunities for analysts to test other aspects of USSF doctrine and organizational priorities. For example, current USSF doctrine (and space power theory in general) may not sufficiently account for commercial space services contributions to war at the strategic, operational, and tactical levels. Arguably, access to data from commercial satellites now provides a sound alternative to independent access to space and national space systems. In addition, analysts should evaluate if USSF investments reflect the importance of integration, networks, and other components of the ground-based segments of space systems. In light of the experiences in Ukraine, it would be prudent to assess USSF priorities and investments across the board to seek out areas for improvement.

Lesson 2: Prepare for Attacks Against Commercial Ground Segments and Satellites

Commercial space actors have come under attack in Russia's war on Ukraine. For example, in the hours before troops invaded Ukraine in February 2022, Russia conducted a cyberattack that disabled Viasat modems, including terminals used for Ukrainian command and control.[15] The attack produced international and strategic effects, disabling tens of thousands of ground-based terminals throughout Europe and disrupting wind turbines and internet services. In addition to highlighting a major cyber vulnerability in these ground systems, the event showed how many aspects of civilian infrastructure and communications in Ukraine and Europe relied on the terminals.

The nature of Russia's cyberattack was also revealing in that it demonstrated the vulnerability of terrestrial space systems. Cyberattacks on the ground segments of space systems can be effective and are more likely than destructive attacks on orbiting satellites, or even cyberattacks against the satellites themselves.[16] Several U.S. leaders across industry and the military have observed that ground systems and software, such as cloud environments, can be particularly vulnerable in conflict. U.S. Space Force Chief General Saltzman said in May 2022, "One of the observations that I would offer on that is that, if you think the only way to dismantle space capabilities is by shooting down satellites, you're missing the bigger picture…as these cyberattacks are on ground networks."[17] In addition to cyberattacks, commercial space actors are wrestling with continued jamming attacks against their link segments.[18]

Beyond cyberattacks, physical attacks can also manifest against commercial ground segments. Satellite control centers, terminals, or various communication nodes traveling with military units can be just as vulnerable to physical attack (for example, by cheap drones, artillery, bombs and missiles, and sabotage) as any other facility or capability on Earth. It is far

less expensive and less challenging technologically to physically attack the ground segment compared to attacking orbiting satellites, which require high-tech space tracking systems and other exotic and expensive capabilities such as direct-ascent missiles or co-orbital weapons capable of reaching specific orbits.

While attacks on the ground, link, and data segments of space systems may be cheaper, easier, and similarly effective as physically attacking satellites, Ukraine indicates that orbiting commercial satellites should not expect to be exempt from attack, including destructive attacks, in a war that extends into space. [19] While U.S. government leaders have raised options for protecting commercial space systems, including indemnification and providing threat information to commercial actors, Ukraine demonstrates that it is an increasingly urgent issue. The hardening of ground systems, software, and cloud environments may be a key investment in securing space systems as a whole.

Lesson 3: Provide Easier Access to Data from Hardened U.S. Military Space Capabilities

Russia's attacks on commercial space systems likely increase the perceived value to allies and partners of access to data from hardened, jam resistant U.S. military space capabilities. These U.S. military space systems provide robust services that are more protected than other government or commercial space systems against cyberattack, jamming, electromagnetic energy, and other types of interference. However, the data and services from these U.S. systems is often difficult to share with allies and partners.[20] U.S. regulations, classification policy, bureaucratic barriers, and other practices often preclude effective data and network sharing with allies, partners, and other supported nations.[21] While the U.S. may seek to share capabilities in times of crisis, gaining access to these systems at a tactical level could be challenging due to the need for expensive terminals, and other specialized equipment, that have to be integrated with other military equipment on short timelines.

Russia's war in Ukraine should incentivize the United States to accelerate changes to regulations, policy, bureaucracy, systems, and operations to reduce barriers to sharing access to higher-end U.S. military space capabilities. Where commercial satellite services face persistent jamming, interference, cyberattack and physical threats, providing allies and partners access to data from protected satellite systems could quickly become a U.S. imperative; this imperative could grow if adversaries field even more aggressive capabilities to challenge commercial satellites.[22] While sensitive U.S. information needs to be protected and recipients need to have appropriate safeguards in place, there may be advantages to the United States if it can design and implement more accessible methods for allies and partners to get crucial data from and through U.S. space systems.

The United States has taken steps recently to make access to data from U.S. space systems easier, but there is plenty of room for further improvement and innovation. For example, in January 2024, the DOD lowered some classification barriers, making data from the space systems easier to share with allies and partners.[23] Other efforts to improve access to data from U.S. space systems include the DOD's combined space operations (CSPO) initiative, which facilitates satellite data sharing among key allies, including Australia, Canada, France, Germany, Italy, Japan, Norway and the United Kingdom.[24] In addition, military coalition exercises that practice space information sharing also contribute to lowering barriers to data sharing. In February 2024, 25 nations participated in the most recent Global Sentinel exercise, which began in 2014 and focuses on space security cooperation and operational collaboration. While many NATO and other close U.S. allies participated, less frequently involved partners such as Brazil, Colombia, and Peru also joined, with India and Mexico attending as observers. Other initiatives, such as personnel exchanges, combined education and training, exercises, and cooperative development, are incrementally trying to improve space data sharing with allies and partners.[25]

Given the sluggishness of current U.S. initiatives to lower classification, export control, and other barriers, innovative ideas are needed to improve partner access to the data that hardened U.S government space systems provide. One option would be to define a pre-set menu of approved U.S. military space services that can be provided to allies, partners, and other supported nations, which could allow allies and partners to better plan how to leverage U.S. space capabilities, lower barriers in a crisis, and enable quicker and more efficient access to data when time matters most.

These space services could accelerate information sharing and enhance alliance effectiveness in several ways. Identifying the user equipment needs, such as specialized modems, terminals, antennas, and other hardware and software, ahead of a crisis could lead to solutions that reduce delays caused by classification issues, export licensing requirements, and other barriers. Finding suitable ground sites, establishing necessary data links, procuring terminals, and provisioning requisite cybersecurity and local physical security require time and resources. The earlier these needs are identified and addressed, the quicker the access to data from U.S. space systems can begin in the event of crisis or conflict. In a more stable period, establishing such infrastructure could look more like traditional Foreign military sales. Financial contributions from partners could be prearranged. In the case of urgent situations like Russia's invasion of Ukraine, these factors could take the form of emergency security assistance.

Conclusion

In war, the state that possesses superior space systems is not guaranteed more effective space support for the warfighter. Instead, the ground and link segments that facilitate networked data dissemination methods and innovative application of the data from satellites have allowed Ukraine, with no satellites of its own, to make better use of space than Russia. Increasing opportunities to make use of space information and services developed by commercial space services have enabled Ukraine to close the gap in space capability while Russian forces have apparently struggled to provide sufficient space-derived information to their warfighters in a timely fashion. Ukraine has demonstrated that what matters is not only what satellite data or services are available but also how fast they are delivered to the warfighter and how well equipped the warfighters are with proper user equipment and training for integrating and using data from space. This dynamic indicates that policy, information-sharing structures, data-processing capability, and data-dissemination networks, while not always the most visible components of space strategy, can be the deciding factor in gaining a competitive advantage in war. Current USSF doctrine in this regard is on target, but USSF priorities and investments should be assessed given these observations.

In addition, while U.S. space strategy for several years has contemplated the vulnerability of commercial satellites and ground systems that the DOD relies upon for many missions around the globe, it is unclear how willing the department is to invest in protection of commercial space systems, in space, or on the ground. Competing priorities for scarce resources often leave these concerns unaddressed. The need to defend critical national security space systems takes priority, but Ukraine shows that protecting commercial space systems, especially the ground and link segments of space systems, is increasingly urgent. USSF strategy, priorities, and investment decisions should take these factors into consideration.

Importantly, Ukraine also shows that any country (allies, adversaries, or non-aligned) with sufficient access to data from commercial satellites has an alternative to developing costly independent access to space and national satellite systems. Ukraine provides them the incentive to focus investments on data distribution and ground systems. In addition to being concerned about the possibility of Russian attacks on commercial space systems, to defend U.S. troops in the field, the DOD and combatant commands may be called upon to deny access to space services from a third country's commercial space enterprise.

Finally, although Ukraine has leveraged the data from commercial satellites to a remarkable extent, Ukraine also demonstrates that important advantages may be available to the United States if it can make the data from hardened, jam-resistant U.S military space capabilities more readily available to allies, partners, and other supported nations.

References

[1] Eric Mack, "Ukraine Asks Commercial Satellite Operators for Help Tracking Russian Troops," CNET, March 2, 2022. https://www.cnet.com/science/space/ukraine-asks-commercial-satellite-operators-for-help-tracking-russian-troops/.

[2] Robin Dickey and Michael Gleason, "Space and War in Ukraine: Beyond the Satellites," *Aether*, Vol. 3 No. 1 (Spring 2024), https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-3_Number-1/Dickey_Gleason.pdf.

[3] "Hawkeye 360 Signal Detection Reveals GPS Interference," Hawkeye 360, press release, March 4, 2022, https://www.he360.com/.

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

[5] David T. Burbach, "Early Lessons from the Russia-Ukraine War as a Space Conflict," Atlantic Council, August 30, 2022. https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/early-lessons-from-the-russia-ukraine-war-as-a-space-conflict/. Pavel Luzin, "Russia's Space Program After 2024," Foreign Policy Research Institute, July 22, 2024. https://www.fpri.org/article/2024/07/russias-space-program-after-2024/. Report of the Commission to Assess United States National Security Space Management and Organization, Space Commission, Pursuant to Public Law 106-65 (January 11, 2001). 53. https://aerospace.csis.org/wp-content/uploads/2018/09/RumsfeldCommission.pdf.

[6] Robin Dickey and Michael Gleason, "Space and War in Ukraine: Beyond the Satellites," *Aether*, Vol. 3 No. 1 (Spring 2024), https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-3_Number-1/Aether_Volume_3_Number_1..pdf.

[7] David Sandy (former chief of staff, UK Ministry of Defence Space Directorate), interview by Michael Gleason, virtual, February 2023.

[8] David Burbach, comments, in "David, Goliath, & Space – Is This How Future Wars Will Be Fought?" Downlink Podcast, February 16, 2023.

[9] David Ignatius, "How the Algorithm Tipped the Balance in Ukraine," Washington Post, December 19, 2022. https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/.

[10] Todd Harrison and Matthew Strohmeyer, "Commercial Space Remote Sensing and Its Role in National Security," Center for Strategic and International Studies, February 2, 2022. https://www.csis.org/analysis/commercial-space-remote-sensing-and-its-role-national-security.

[11] Space Capstone Publication: Space Power, Doctrine for Space Forces, USSF, (June 2020), 5, 16.

[12] "Spacepower Security Forum 2023: A Mission to Protect and Defend Assets in Space," transcript of conference proceedings, Mitchell Institute for Aerospace Studies, April 5, 2023. https://mitchellaerospacepower.org/.

[13] Mark Jelonek, "Toward an Air and Space Force: Naval Aviation and the Implications for Space Power, *Air University Press*, (September 1999). 39-58. https://media.defense.gov/2017/Nov/21/2001847063/-1/-1/0/CP_0005_JELONEK_AIR_AND_SPACE_FORCE.PDF.
Gottrich, D. and Grimaila, M.R., "Managing the Integration of Space and Information Operations.
Daniel F. Gottrich, Michael R. Grimaila, "Managing the Integration of Space and Information Operations," *High Frontier Journal*, Vol. 2, No. 3, Apr. 2006, pp. 44-49. https://scholar.afit.edu/cgi/viewcontent.cgi?article=1158&context=facpub.

[14] Space Capstone Publication: Space Power, Doctrine for Space Forces, USSF, (June 2020), 16.

[15] Antony J. Blinken, "Attribution of Russia's Malicious Cyber Activity Against Ukraine," Department of State, May 10, 2022. https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/.

[16] Sandra Erwin, "U.S. Space Force to step up protection of satellite ground systems in the wake of Russia's cyber attacks," *SpaceNews*, (May 19, 2022) https://spacenews.com/u-s-space-force-to-step-up-protection-of-satellite-ground-systems-in-the-wake-of-russias-cyber-attacks/.

[17] Sandra Erwin, "U.S. Space Force to step up protection of satellite ground systems in the wake of Russia's cyber attacks," *SpaceNews*, (May 19, 2022) https://spacenews.com/u-s-space-force-to-step-up-protection-of-satellite-ground-systems-in-the-wake-of-russias-cyber-attacks/.

[18] Sandra Erwin, "Space industry group warns of escalating cyber threats, outmatched defenses," *SpaceNews* (June 18, 2024). https://spacenews.com/space-industry-group-warns-of-escalating-cyber-threats-outmatched-defenses/.

[19] Ibid.

[20] Jennifer D. P. Moroney, Stephanie Pezard, et al., "Overcoming Barriers to Working with Highly Capable Allies and Partners in the Air, Space, and Cyber Domains: An Exploratory Analysis," RAND, (July 2003). 25 – 27. https://www.rand.org/pubs/research_reports/RRA968-1.html.

[21] Jennifer D. P. Moroney, Stephanie Pezard, et al, "Overcoming Barriers to Working with Highly Capable Allies and Partners in the Air, Space, and Cyber Domains: An Exploratory Analysis," RAND, (July 2003). vi. https://www.rand.org/pubs/research_reports/RRA968-1.html.

[22] Robert "Tony" Vincent, "Getting Serious about the Threat of High Altitude Nuclear Detonations," *War on the Rocks*, (September 23, 2022). https://warontherocks.com/2022/09/getting-serious-about-the-threat-of-high-altitude-nuclear-detonations/#:~:text=On%20July%209%2C%201962%2C%20the,device%20in%20low%20Earth%20orbit.

[23] Courtney Albon, “Pentagon rewrites space classification policy to improve info-sharing,” C4ISRNET, (January 17, 2024). https://www.c4isrnet.com/battlefield-tech/space/2024/01/17/pentagon-rewrites-space-classification-policy-to-improve-info-sharing/.
[24] Joseph Clark, “DOD Prioritizing Cooperation With Allies in Space,” DOD News, Dec. 14, 2023 | By, DOD New https://www.defense.gov/News/News-Stories/Article/Article/3617707/dod-prioritizing-cooperation-with-allies-in-space/.
[25] Jennifer D. P. Moroney, Stephanie Pezard, et al., “Overcoming Barriers to Working with Highly Capable Allies and Partners in the Air, Space, and Cyber Domains: An Exploratory Analysis,” RAND, (July 2003). 6. https://www.rand.org/pubs/research_reports/RRA968-1.html.

About the Author

Dr. Michael P. Gleason is a national security senior project engineer in The Aerospace Corporation's Center for Space Policy and Strategy and is a well-regarded author on space policy subjects, including international cooperation, space traffic management, national security, and deterrence. He has presented his research on critical space policy issues at conferences in Canada, Europe, Japan, and across the United States. A graduate of the U.S. Air Force Academy, Gleason served 29 years active in the Air Force space career field, including stints in spacecraft operations, on the Air Force Academy faculty, at the Pentagon, and at the Department of State. He holds a doctorate in International Relations from George Washington University (GWU) and is an alumnus of the GWU Space Policy Institute. Gleason is the recipient of the Defense Superior Service Medal and the Department of State Superior Honor Award.

About Space Agenda 2025 Publications

This paper was published as a chapter of *Space Agenda 2025*, with Angie Bukley, Colleen Stover, and Victoria Woodburn serving as editors in chief. *Space Agenda 2025* is an effort by the Center for Space Policy and Strategy (CSPS) at The Aerospace Corporation to highlight and provide insights into some of the major space challenges facing policymakers. You can find the complete list of individual *Space Agenda 2025* papers at http://csps.aerospace.org/SA2025, as well as download the combined set of 16 chapters in the *Space Agenda 2025 Compendium* at https://csps.aerospace.org/papers/space-agenda-2025-compendium, all available to you with our compliments.

About the Center for Space Policy and Strategy

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decisionmakers. The Center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

For more information, go to www.aerospace.org/policy or email policy@aero.org.