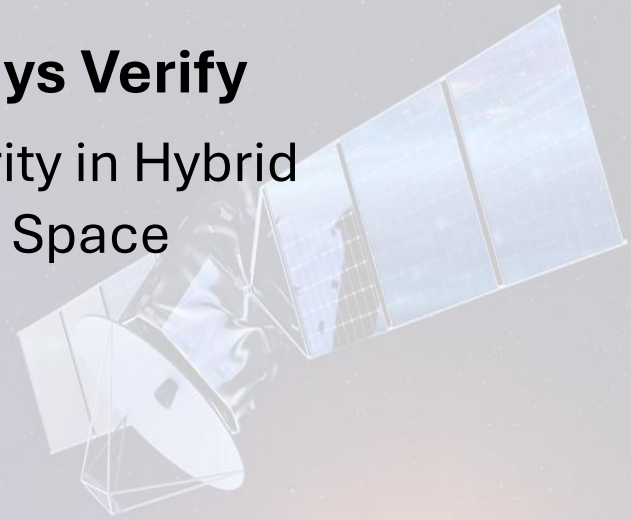
Potomac Institute for Policy Studies

*Science for Policy. Policy for Science.*

# Never Trust, Always Verify

## Improving Cybersecurity in Hybrid Architectures for Space



Jason Blessing

February 2026

**SCHOLAR PAPER SERIES**

ISSUES IN: Space

PAPER NUMBER: 20260223-01

901 N. Stuart Street, Suite 1200
Arlington, Virginia 22203
Phone: (703) 525-0770

www.potomacinstitute.org

**KEY POINTS**

- US space systems remain highly vulnerable to cyberattacks. While the ground and user segments of space systems are the most at-risk, space segments are increasingly exposed to compromise.
- Since 2022, the United States Space Force (USSF) has increasingly emphasized the transition to zero trust frameworks for securing space systems from cyber threats.
- At the same time, the USSF has explored the use of hybrid architectures for space to enhance the effectiveness and resilience of USSF operations and mission execution.
- Such hybrid architectures introduce greater complexity into zero trust implementation in terms of attack surfaces, assets and security postures, and incident response.
- The USSF can successfully implement zero trust across its hybrid architectures, but doing so will require a strategic vision for how modular assets interconnect in the security environment. This should include inventorying existing assets, prioritizing the most at-risk architectures, requiring a common interface, and regular red-teaming efforts.

## INTRODUCTION

In 2022, the Department of Defense (DoD) released its Zero Trust Strategy to enhance the security and resiliency of its networks.[1] Traditionally, the DoD has relied on perimeter-based cybersecurity through firewalls and intrusion detection and prevention systems to ensure internal networks, users, devices, and activities are trusted. These security measures scrutinize initial access; yet once compromised, few barriers prevent malicious hackers from moving freely in and across systems. In contrast, zero trust emphasizes continuous verification of users, devices, networks, and activity. This requires a "never trust, always verify" framework for networked infrastructure that grants the minimum level of permissions and access necessary to execute a mission.[2] Following DoD and Department of the Air Force requirements,[3] the United States Space Force (USSF) has begun pursuing zero trust to protect its digitally reliant assets.[4]

At the same time, the USSF has also explored using hybrid architectures for its missions. For the USSF, a hybrid architecture for space is a way to leverage military, civil, and commercial space assets into a dynamic, integrated, and unified system. Such hybrid architectures can greatly enhance the execution, resilience, and effectiveness of USSF operations. Yet, hybrid architectures for space entail distinct cybersecurity challenges that complicate the implementation of zero trust. **The USSF can successfully implement zero trust across its hybrid architectures, but doing so will require a strategic vision for how modular assets interconnect in the security environment.**

Hybrid architectures can greatly benefit USSF mission execution. But without zero trust, USSF operations using hybrid architectures are only as secure as the most vulnerable assets of its partners. **The utilization of hybrid architectures and the implementation of zero trust must occur in tandem to maximize both effectiveness and security.** This paper explores the challenges associated with securing hybrid architectures for space from cyber threats. The following sections describe the vulnerabilities of broader space systems to cyber threats, outline the additional cybersecurity challenges related to hybrid architectures, detail the main principles of zero trust cybersecurity, and provide initial steps for the USSF to implement zero trust across hybrid architectures for space.

## CYBER VULNERABILITIES IN SPACE SYSTEMS

Space systems underpin much of society's modern, digitally-based activity. Space systems consist of four distinct segments:

1. The space segment, which encompasses satellites on orbit;
2. The ground segment, which includes ground stations, network operating centers, other networked infrastructure, and launch capabilities;
3. The link segment, comprised of the radio wave uplinks and downlinks that transfer data between satellites and ground elements; and
4. The user segment, made of end-user devices and networks.

For militaries, space systems serve a variety of purposes, including: positioning, navigation, and timing for GPS routing and targeting enemy forces; providing information on missile launches; environmental monitoring to aid mission planning; secure satellite communications for command and control; and intelligence, surveillance, and reconnaissance. The military's heavy utilization and reliance make space systems key targets for disruption or destruction. Each segment is vulnerable to kinetic and non-kinetic attacks. However, the ground, user, and space segments are vulnerable to cyberattacks, where attackers rely on computer code to gain control of specific devices, networks, or digital data. While not directly impacted by cyberattacks, the link segment transmits any manipulated commands or corrupted data resulting from digital compromise across the ground, space, and user segments.[5]

The motivations and goals for cyberattacks are diverse and can include information theft, manipulating communications, corrupting data, denying network access or service, and even satellite control.[6] Unlike kinetic attacks, cyberattacks generally have reversible or delayed effects and generally fall below the threshold of armed conflict. However, space system compromises have high risks of cascading effects. Because space systems often serve as single points of failure for critical infrastructures across civilian and military sectors, the impacts of a cyberattack are potentially wide-ranging.

Securing space systems from cyberattacks requires protecting terrestrial networks, the satellites in space, and the transmitted data. The ground and user segments are particularly conducive to targeting due to their reliance on terrestrial computer networks. Hackers can use malicious software (e.g., malware, ransomware, wiperware) and other tools to deny, degrade, disrupt, or destroy access to or functionality of computer devices, networks, or data.

**HACKING SPACE SYSTEMS: THE 2022 VIASAT ATTACK**

The Russian invasion of Ukraine in 2022 began with one of the most disruptive and publicly visible cyberattacks on space systems. Russian hackers targeted the US commercial company Viasat, which was providing communications services for Ukrainian military forces. The cyberattack disrupted Ukrainian military communications reliant on Viasat and caused internet blackouts for thousands of Viasat customers across Europe. The attack unfolded in four phases:[7]

***Phase 1: Ground Segment Network Compromise.*** Russian hackers compromised a Virtual Private Network (VPN) used by Viasat administrators in one of the company's management centers in Turin, Italy. Through the VPN, hackers gained access to Viasat's management servers and data on end-user modems.

***Phase 2: Lateral Movement and Malware Injection.*** Using permissions gained through the initial compromise, Russian operators moved laterally from the management servers to access servers that deliver software updates to user modems. Hackers introduced the AcidRain wiperware (i.e., malware intended to destroy data) onto these update servers.

***Phase 3: Payload Delivery to User Segment.*** Hackers then initiated a false software update from Viasat servers to user modems that contained the AcidRain wiperware. The malware disabled over 40,000 modems across Europe by wiping the flash memory, including a substantial number of modems located in Ukraine likely used by the Ukrainian military.

***Phase 4: Distributed Denials of Service (DDoS).*** Using the privileged access gained through the initial VPN compromise and lateral network movement, hackers overloaded Viasat terminals and servers with traffic to ensure that servers could not respond to requests from offline modems attempting to reconnect to Viasat services. Russian operators targeted terminals servicing modems in specific regions encompassing parts of Ukraine. These DDoS attacks also aimed to overwhelm incident responders with network traffic.

While the space segment has traditionally remained protected from cyberattacks due to the remoteness of satellites, this is no longer the case.[8] Satellite firmware, the essential software built into hardware to perform basic functions and communicate with operating system software, is increasingly at risk of digital compromise.[9] Recent events like the USSF's Moonlighter challenge and the European Space Agency's ethical hacking exercise show that live, in-orbit satellites are susceptible to hacking.[10]

These threats are only set to grow, as adversaries like China develop new cyber capabilities to hijack satellites.[11] At the same time, manufacturing constraints on satellites complicate the implementation of cybersecurity measures. Satellites generally face size, weight, and power restrictions and must prioritize survivability in high-radiation and extreme-temperature environments. These requirements limit on-satellite cybersecurity solutions to lighter and lower power options.[12]

Space systems vulnerabilities are exacerbated by a reliance on legacy technologies. Satellites and the networks required to operate them can have decades-long lifespans.[13] Such legacy systems possess obsolete hardware that cannot support newer software, operating systems, or security updates and vulnerability patches to protect against modern cyber threats. Legacy systems also tend to possess outdated database systems and arcane information technology (IT) security systems, which limit integration with modern applications and cybersecurity measures.[14]

Military assets in particular tend to utilize custom applications built on older programming languages and platforms. These assets are even more difficult to maintain and update over time. The technical

debt accumulated by legacy space systems across decades—the increasing costs of maintaining and modifying systems while neglecting or delaying modernization—means that system dependencies often remain unknown or undocumented.[15] As a result, antiquated government space systems represent one of the USSF's greatest cyber vulnerabilities.

## THE CHALLENGE OF SECURING HYBRID ARCHITECTURES FOR SPACE

Hybrid architectures for space seek to leverage and integrate military, civil, and commercial space assets into a single unified system with the goal of providing real-time information and decision advantage to warfighters on the ground. For the US military, this can also entail the integration of assets from Allies and partners abroad, as well as foreign commercial elements. Different assets can be utilized for different purposes, meaning that active participation in the hybrid architecture is fluid and mission-based. This modularity is crucial for increasing resilience by providing multiple paths for communications and data transfer.[16] How those modular assets are interconnected is key for cyber defense.

Space systems cyber vulnerabilities become more complex in hybrid architectures in several ways:

**Complexity of the attack surface.** The military's increasing reliance on commercial space systems[17] expands the attack surface by providing hackers with new avenues for targeting military systems. As the number of users, networks, and satellites across a hybrid architecture increases, so do the number of attack vectors for digital compromise. The proliferation of small satellite constellations in the private sector further complicates the attack surface. Unlike their larger exquisite military-grade counterparts, these smaller satellites are often made of commercially available off-the-shelf parts.[18] When underpinned by a common design, these satellites introduce both a greater number of potential vulnerabilities and a greater chance that a single vulnerability compromises an entire constellation. Moreover, commercial development schedules may introduce time constraints that limit the ability to implement robust cybersecurity measures across supply chains.[19]

**Complexity of assets and their security postures.** Hybrid architectures integrate new commercial technologies and legacy systems into a unified system at a greater speed and scale than traditional USG acquisition processes. This diversity of assets in a hybrid architecture creates a greater risk of both complex security gaps between technologies and disruption to operational continuity. Legacy systems will inevitably remain in place,[20] and they generally lack the ability to support granular authentication controls or modern data encryption. They are therefore more exposed to contemporary cyber threats like ransomware and phishing.[21]

Moreover, the rapid adoption of new technologies alongside legacy systems can disrupt operational continuity and efficiency.[22] Interoperability can become difficult since legacy technologies rely on increasingly outdated and siloed database structures. This can lead to data compatibility and sharing issues that reduce operational visibility, performance, and efficient decision making.[23] Coupled with unknown or undocumented system dependencies, integrating vulnerable legacy technologies with new ones can create unanticipated and complex interactions that malicious hackers can exploit.

**Complexity of response.** Hybrid architectures also complicate incident response and remediation across participants and systems. Differing threat information sharing standards and practices

across a hybrid architecture can prevent a comprehensive view of the security postures of participants and their assets.[24] For one, fluid participation in a hybrid architecture can slow the dissemination of cyber threat intelligence and remediation measures. Participation on a mission-by-mission basis can mean different operators and users may have different levels of access to classified information.

At the same time, participants in the hybrid architecture may have conflicting attack identification and attribution processes[25] or incident reporting thresholds. This is particularly true for foreign elements of a hybrid architecture, which can have different national security standards than the US for sharing classified information with commercial actors. Even when information sharing is sufficient, participants in a hybrid architecture may have varying capacities for incident response. Uneven implementation of mitigation or remediation measures can prolong the effects of a cyberattack.

Cyberattacks on space systems can also present jurisdictional challenges for defensive efforts. Determining federal responsibility for defending corporate networks will become an increasingly important legal question as the US Government expands its use of commercial mega-constellations.[26] In hybrid architectures, cyberattacks can produce unintended consequences and high spillover effects for government systems.

## ENHANCING CYBERSECURITY THROUGH ZERO TRUST

Zero trust eliminates the implicit trust within enterprise-owned networks and systems by assuming anyone on a network could be an attacker. This means internal enterprise networks and internal users are considered no more trustworthy than external, non-enterprise networks or users.[27] As such, implementing zero trust enhances security by minimizing access to resources (data, computing, applications, services, etc.) and continuously authenticating and authorizing identity and security compliance for each access request.

**DEFINING ZERO TRUST**

***Zero trust*** is a set of concepts intended to enhance security by minimizing access to resources through least privileged, per-request access and continuous verification.

***Zero trust architecture (ZTA)*** is a cybersecurity plan that implements zero trust concepts to limit breaches, reduce lateral movement on internal networks, and decrease risks to assets and functionality. ZTA defines the access policies, workflows, and relationships among policies, administrators, and users for physical and virtual network structures.

Zero trust operates on three broad assumptions. First, no inherent trust exists among networks, resources, data, users, and devices. An organization's private networks are not considered safe zones, and users requesting remote access should not fully trust local, non-enterprise network connections. Network resources are also subjected to extra scrutiny, and user credentials alone are insufficient for gaining access to an organization's resources. Second, not all devices or resources on private networks will be owned or managed by a single organization. Finally, users, devices, and

workflows moving between enterprise networks and non-enterprise networks have consistent security policies and postures.[28]

Security models build on zero trust therefore differ from traditional, perimeter-based models in critical ways. In perimeter-based security models, access control is static. Network users are implicitly trusted after initial authentication. Once connected to the network, they have full access to network resources and all network traffic remains unencrypted. In contrast, users in a zero trust environment are continuously verified after initial authentication. Moreover, they will only have access to specific network resources, and network traffic is encrypted.[29] Table 1 summarizes this comparison.

| Concept | Traditional Perimeter Security Model | Zero Trust Security Model |
|---|---|---|
| Identity management | Static Access Control | Dynamic Access Control |
| Endpoint Protection | Authenticate to connect to network | Authenticate to connect to network resources |
| Security Analytics | Once identified, implicit trust on network | Continuous confirmation of user identity on network |
| Encryption | Internal network traffic unencrypted | End-to-end encryption for all network sessions |

Table 1. Comparing Traditional Perimeter and Zero Trust Security Models

Accordingly, zero trust relies on four key concepts:

**Just-in-Time Access.** All authentication and resource access decisions are based on policy decisions made at the time of a user's access request. This minimizes authentication delays.[30] User access is not granted prior to a request and access to any network resource is determined on a per-session basis.[31]

**Least Privileged Access.** Users are only granted the access and permissions required to complete a specific request. These granular privileges are only valid for the duration of the request and are immediately terminated upon completion.[32]

**Encryption of Data.** Encrypting data ensures that all communications and data transfers are secured regardless of user or network. Data encryption reduces the risks of data compromise by coding sensitive data into formats that are non-sensitive. For example, sensitive, personally identifiable information can be replaced with alphanumeric characters.

**Dynamic Access Control.** Verification and access rely on as many attributes as possible at the time of a request. In addition to user identity and credentials, this can include information about devices, applications, services, behavioral patterns, and network environments. While access may be granted to a specific resource on the network, access to any additional resource requires reverification. As a result, dynamic access control provides continuous scrutiny and information collection to improve security postures and limit potential lateral movement of bad actors across a compromised network.[33]

These concepts are implemented across an organization's networks through a zero trust architecture (ZTA). A zero trust architecture generally consists of algorithms that determine access, administrators working with the algorithms, and individual enforcement points across a network. All users must request access through enforcement points such as firewalls, gateways, portals, or proxy servers. Based on organizational access and security policies, algorithms continually grant, deny, or restrict user access at these enforcement points. Administrators work with the algorithms to allow or deny user requests and ensure policy compliance at the enforcement point.[34]

An organization's assets are only accessible through an enforcement point, and policy or security factors can prevent access to certain enforcement points for network access. When implemented, a ZTA also allows an organization to distinguish between internal assets owned and managed by the enterprise, external assets, and the respective security postures. As a result, zero trust architectures limit breaches, reduce lateral movement on internal networks, and reduce risks to assets and functionality.[35]

In a hybrid architecture for space, this will require clearly distinguishing and discriminating between governmental assets, commercial assets, and international assets from Allies and partners. Participation in the hybrid architecture does not grant automatic or universal access to the architecture's resources. Instead, users and assets are subjected to continuous scrutiny at given enforcement points with access determined by USSF policy.

## IMPLEMENTING ZERO TRUST IN SPACE HYBRID ARCHITECTURES

For the USSF, establishing and employing a ZTA in hybrid architectures for space will be difficult given their size and complexity. However, there are at least four steps the service can take to start to facilitate zero trust across its hybrid architectures and increase security without hindering mission effectiveness.

**Inventory and catalog the ground, space, and user assets that support mission-essential functions in a hybrid architecture.**

A comprehensive inventory should encompass assets in each segment of space systems and the communication paths between them. USSF assets should be the initial priority for inventory, but the service will also need to catalog commercial and other partner assets included in contracts or agreements. This inventory should include interconnections between individual satellites, between satellites and ground states, satellites and users, and the terrestrial connections between ground stations and users. Artificial intelligence and machine learning (AI/ML) can be a critical enabler for this process by facilitating and automating data tagging, labeling, and identity baselining. Utilizing AI/ML for these ends will require the USSF to develop a comprehensive strategy for processing and governing data across its hybrid architectures.

A key element of the inventory process will be to identify which technologies and systems can support a ZTA and which ones pose barriers to zero trust. For instance, many legacy technologies may not be able to integrate with the capabilities required to implement zero trust. For these cases, the USSF will need to formulate, implement, and document workarounds until legacy technologies can be upgraded to be fully compliant with a ZTA.[36] Inventorying and cataloging commercial assets across a hybrid architecture can uncover which existing vendors or partners have products that fail to meet zero trust requirements.

**Prioritize ZTA implementation for the most at-risk hybrid architectures.**

ZTA implementation should target the greatest risks to USSF missions. The hybrid architectures presenting the most risk are those highly vulnerable to cyberattacks and where the consequences of failing to execute a mission are high. These two factors—consequences of mission failure and vulnerability to cyberattacks—offer a preliminary way to determine priority levels for ZTA implementation across hybrid architectures. Table 2 provides an initial look at ZTA implementation priority from highest (Priority Level 1) and lowest (Priority Level 4).

| | | **Consequences of Mission Failure** | |
|---|---|---|---|
| | | *HIGH* | *LOW* |
| **Vulnerability to Cyberattacks** | *HIGH* | **Priority Level 1** | **Priority Level 3** |
| | *LOW* | **Priority Level 2** | **Priority Level 4** |

Table 2. Hybrid Architecture Priority Levels for Zero Trust Implementation

USSF assets used to execute operations for the most sensitive and highest impact missions are the logical starting point. These systems are already largely inventoried and implicitly trusted, making ZTA implementation both easier and a greater imperative. However, implementing zero trust for these exquisite systems must be accompanied by greater supply chain scrutiny. Zero trust will remain an incomplete security solution without validating bespoke hardware supply chains for these systems and securing them from manufacturing, supplier, and other third-party risks.

Since these are primarily US government-owned assets, the USSF will have more flexibility in controlling access requirements based on operational tempos and an evolving cyber threat environment. This can also ensure zero trust policy consistency and adherence across a hybrid architecture. Only with consistent internal implementation should the service expand implementation of synchronization of ZTAs to hybrid architectures with more complex commercial and international participation.[37]

**Enable both interoperability and security for zero trust through standardized application programming interfaces (APIs) for hybrid architectures.**

Hybrid architectures and ZTAs necessitate standardization for access and communication. APIs are software interfaces that can form connections between computers or computer programs; they offer a bridge of communication across systems with different configurations. Dedicated and standardized APIs for hybrid architectures facilitate interoperability by offering a common set of rules or protocols for commercial assets and their government counterparts to better communicate and share data.[38] Moreover, a common API can also help align security practices for a ZTA employed by the USSF. Currently, the space industry lacks common cybersecurity standards for procedures like event logging, information sharing, and incident reporting.

Without a governmentally-driven API, the USSF may not be able to seamlessly shift from leveraging one commercial participant to another in the event of disruption. The financial and time costs of transitioning to other assets in the hybrid architecture would be steep; for example, continuing USSF

operations may require translating data from one proprietary format to another.[39] The longer term risk is vendor lock for a single provider or a specific subset of providers within a hybrid architecture, thereby reducing mission resiliency. Without a common API, every new asset would require costly, customized integration into a hybrid architecture. Standardized government APIs would help the USSF avoid the costs of dealing with the different proprietary APIs for integration that inevitably emerge from the private sector.

**Expand red-teaming initiatives to include regular penetration testing and "hack-a-sat" exercises across hybrid architectures.**

Compliance with zero trust policies in a hybrid architecture is critical, but compliance without regular red-teaming breeds complacency. It creates a checklist mentality that defaults to a lowest common denominator security posture across participants.

Joint and wide-ranging penetration testing and satellite hacking exercises should be an essential aspect of cybersecurity in a hybrid architecture. These efforts can identify vulnerabilities and security gaps between assets, explore evolving system dependencies, and propose remediation for participant vulnerabilities in and across hybrid infrastructures. In addition to helping avoid operational blind spots, regularized red-teaming within a zero framework can help combat the institutional resistance to change that typically accompanies ZTA implementation, a key hurdle for the USSF, Air Force, and the broader DoD.[40] Dedicated, planned red-teaming will need to encompass both the information technologies and the operational technologies in a hybrid architecture.[41] Utilizing cyber ranges and digital twinning represents an important avenue to facilitate vulnerability hunting exercises.[42]

## CONCLUSION

Both zero trust cybersecurity and the use of hybrid architectures represent new paradigms for the USSF. While offering greater effectiveness and resiliency in overall mission execution, the modularity of hybrid architectures entails complex cyber vulnerabilities. The "never trust, always verify" foundation of zero trust is therefore critical as the USSF seeks fluidly to leverage commercial and international partners through hybrid architectures for its missions. This is even more true for the most sensitive and highest impact USSF missions. Future work should therefore explore, refine, and expand on the priority levels introduced in Table 2 to better facilitate implementation efforts.

Yet, zero trust security is not bulletproof. Insider threats, supply chain and manufacturing compromises, subversion of the ZTA decision process, and denial of service attacks, will continue to jeopardize USSF networks and assets. Implementation must also balance the reality of budgetary constraints and inconsistent zero trust standards and governance[43] across the DoD. Despite these challenges, a clear strategic vision can drive both greater cybersecurity and greater effectiveness for the USSF.

## ABOUT THE AUTHOR

**Jason Blessing, Ph.D.,** is a Research Fellow at the Potomac Institute for Policy Studies. His research expertise focuses on cybersecurity, defense, and international relations.

# ENDNOTES

[1] United States Department of Defense. (2022b). *DoD Zero Trust Strategy*. Office of Prepublication and Security Review. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.
[2] Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A Systematic Literature Review. *Journal of Network and Systems Management*, *34*(1), 25–62. https://doi.org/10.1007/s10922-025-09998-x.
[3] DoD CIO Cybersecurity Architecture Division. (2023). *Department of Defense (DoD) Cybersecurity Reference Architecture: Version 5.0*. Office of Prepublication and Security Review. https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf; United States Department of Defense. (2019). *Department of Defense Instruction 8500.01: Cybersecurity*. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf; (2021). *Department of Defense Control Systems Security Requirements Guide*. https://dl.dod.cyber.mil/wp-content/uploads/external/pdf/Jan_26_Control_Systems_SRG.pdf; (2022a). *Department of Defense Instruction 8510.01: Risk Management Framework for DoD Systems*. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf.
[4] For instance, the service recently granted a $17 million contract to Xage Security to help achieve zero trust access controls and data protections. The primary threat to the link segment is electronic warfare, which broadly encompasses directed energy attacks that manipulate the electromagnetic spectrum. Space Systems Command Public Affairs. (2024, March 27). *SSCs Zero Trust Cyber Effort Has Mission in Mind*. Space Systems Command. https://www.ssc.spaceforce.mil/Newsroom/Article/3722882/sscs-zero-trust-cyber-effort-has-mission-in-mind.
[5] Cybersecurity and Infrastructure Security Agency. (2024). *Space Systems Security and Resilience Landscape: Zero Trust in the Space Environment*. https://www.cisa.gov/sites/default/files/2024-06/Space%20Systems%20Security%20and%20Resilience%20Landscape%20-%20Zero%20Trust%20in%20the%20Space%20Environment%20%28508%29.pdf, p. 9; Kavallieratos, G., & Katsikas, S. (2023). An Exploratory Analysis of the Last Frontier: A Systemic Literature Review of Cybersecurity in Space. *International Journal of Critical Infrastructure Protection*, *43*(100640).
[5] US Government Accountability Office. (2022). *Space Acquisitions: Changing Environment Presents Continuing Challenges and Opportunities for DOD*. https://www.gao.gov/products/gao-22-105900.
[5] Van Camp, C., & Peeters, W. (2022). A World without Satellite Data as a Result of a Global Cyber-Attack. *Space Policy*, *59*, 101458. https://doi.org/10.1016/j.spacepol.2021.101458; Willbold, J., Schloegel, M., Vogele, M., Gerhardt, M., Holz, T., & Abbasi, A. (2023). *Space Odyssey: An Experimental Software Security Analysis of Satellites*. 1–19. https://doi.ieeecomputersociety.org/10.1109/SP46215.2023.10351029.
[5] Hitchens, T. (2023, August 15). Italian team wins Space Force's first on-orbit Hack-A-Sat contest. *Breaking Defense*. https://breakingdefense.sites.breakingmedia.com/2023/08/italian-team-wins-space-forces-first-on-orbit-hack-a-sat-contest/; Martin, A. (2023, April 25). *Hackers to show they can take over a European Space Agency satellite*. The Record. https://therecord.media/space-cybersecurity-satellite-hacked-esa-thales.
[6] Cybersecurity and Infrastructure Security Agency, 2024, p. 9; Kavallieratos & Katsikas, 2023.
[7] Blessing, J. (2022, September 2). Revisiting the Russian Viasat Hack: Four Lessons About Cyber on the Battlefield. *AEIdeas*. https://www.aei.org/foreign-and-defense-policy/revisiting-the-russian-viasat-hack-four-lessons-about-cyber-on-the-battlefield/; Burgess, M. (2022, March 23). *A Mysterious Satellite Hack Has Victims Far Beyond Ukraine*. WIRED. https://www.wired.com/story/viasat-internet-hack-ukraine-russia/; Gatlan, S. (2022, March 31). *Viasat confirms satellite modems were wiped with AcidRain malware*. BleepingComputer. https://www.bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/; Greig, J. (2023, August 11). *NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation*. The Record. https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions.

[8] US Government Accountability Office, 2022.
[9] Van Camp & Peeters, 2022; Willbold, Schloegel, Vogele, Gerhardt, Holz, & Abbasi, 2023.
[10] Hitchens, 2023; Martin, 2023.
[11] Defense Intelligence Agency. (2022). *Challenges to Security in Space: Space Reliance in an Era of Competition and Expansion*. https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf, pp. 8–29; Srivastava, M., Sevastopulo, D., Leahy, J., & Schwartz, F. (2023, April 21). *China building cyber weapons to hijack enemy satellites, says US leak*. Financial Times. https://www.ft.com/content/881c941a-c46f-4a40-b8d8-9e5c8a6775ba.
[12] Han, S., Li, J., Meng, W., Guizani, M., & Sun, S. (2022). Challenges of Physical Layer Security in a Satellite-Terrestrial Network. *IEEE Network*, *36*(3), 98–104. https://doi.org/10.1109/MNET.103.2000636.
[13] Shahzad, S., Joiner, K., Qiao, L., Deane, F., & Plested, J. (2024). Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers. *Systems*, *12*(10), 434–457. https://doi.org/10.3390/systems12100434, p. 440.
[14] NASA Office of Inspector General. (2025). *Audit of NASA's Zero Trust Architecture* (IG-25-004). https://oig.nasa.gov/office-of-inspector-general-oig/audit-of-nasas-zero-trust-architecture/; Ogunwole, O., Onukwulu, E. C., Joel, M. O., Adaga, E. M., & Ibeh, A. I. (2023). Modernizing Legacy Systems: A Scalable Approach to Next-Generation Data Architectures and Seamless Integration. *International Journal of Multidisciplinary Research and Growth Evaluation*, *4*(1), 901–909. https://doi.org/10.54660/.IJMRGE.2023.4.1.901-909.
[15] Ogunwole, Onukwulu, Joel, Adaga, & Ibeh, 2023.
[16] Defense Innovation Unit. (2025, May 12). *Hybrid Space Communications Network Leverages Commercial Technology, Enabling Faster Decision-Making on the Battlefield*. https://www.diu.mil/latest/hybrid-space-communications-network-leverages-commercial-technology-enabling; Easley, M. (2025, May 12). *With Pilot Planned for 2026, DIU Brings Additional Vendors into 'Hybrid' Space Satellite Network Project*. DefenseScoop. https://defensescoop.com/2025/05/12/diu-hybrid-space-architecture-hsa-pilot-vendors/; SmallSat Alliance. (n.d.). *Hybrid Space Architecture Statement of Principles*. SmallSat Alliance. https://smallsatalliance.org/wp-content/uploads/2020/09/Hybrid-Architecture-Statement-of-Principles-v21.pdf.
[17] Aviation Week. (2023, December 18). *U.S. Space Force Places Premium On Proliferation In 2024*. Aviation Week Network. https://aviationweek.com/defense-space/budget-policy-operations/us-space-force-places-premium-proliferation-2024.
[18] Vessels, L., Heffner, K., & Johnson, D. (2019). Cybersecurity Risk Assessment for Space Systems. *2019 IEEE Space Computing Conference (SCC)*, 11–19. https://doi.org/10.1109/SpaceComp.2019.00006.
[19] Bailey, B., Speelman, R. J., Doshi, P. A., Cohen, N. C., & Wheeler, W. A. (2019). *Defending Spacecraft in the Cyber Domain*. The Aerospace Corporation. https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf.
[20] Erwin, S. (2026, January 4). *Space Force Begins Base Network Overhaul as Cybersecurity Demands Grow*. SpaceNews. https://spacenews.com/space-force-begins-base-network-overhaul-as-cybersecurity-demands-grow/.
[21] Oyegbade, I. K., Igwe, A. N., Ofodile, O. C., & Azubuike, C. (2023). Transforming financial institutions with technology and strategic collaboration: Lessons from banking and capital markets. *International Journal of Multidisciplinary Research and Growth Evaluation*, *4*(6), 1118–1127. https://doi.org/10.54660/.IJMRGE.2023.4.6.1118-1127.
[22] Ogunwole, Onukwulu, Joel, Adaga, & Ibeh, 2023.
[23] Sharma, P., & Barua, S. (2023). From Data Breach to Data Shield: The Crucial Role of Big Data Analytics in Modern Cybersecurity Strategies. *International Journal of Information and Cybersecurity*, *7*(9), 31–59.
[24] Defense Innovation Unit, 2025.

[25] Attribution involves the technical investigation of tactics, techniques, and procedures used by a threat actor and the identification of the intended operational goals. Political attribution—determining who is responsible and why—requires geopolitical and legal contexts. Political or financial considerations may keep partners from publicly attributing an attack, reducing the prospects for a multilateral response. Egloff, F. J., & Smeets, M. (2023). Publicly Attributing Cyber Attacks: A Framework. *Journal of Strategic Studies*, *46*(3), 502–533; Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37.
[26] Georgescu, A., Botezatu, U.-E., Arseni, S.-C., Barbu, A., & Boiangiu, L. (2016). Deliberate Threats to Critical Space Infrastructure—ASAT and the Strategic Context. *Naval Academy of Scientific Bulletin*, *19*(2), 419–427. https://doi.org/10.21279/1454-864X-16-I2-063.
[27] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology, US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf, pp. 1–6.
[28] Cybersecurity and Infrastructure Security Agency. (2023). *Zero Trust Maturity Model Version 2.0*. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf; Rose, Borchert, Mitchell, & Connelly, 2020, p. 8.
[29] Gambo & Almulhem, 2025; United States Government Accountability Office. (2022). *Science and Tech Spotlight: Zero Trust Architecture* (GAO-23-106065). https://www.gao.gov/assets/gao-23-106065.pdf.
[30] Shore, M., Zeadally, S., & Keshariya, A. (2021). Zero Trust: The What, How, Why, and When. *Computer*, *54*(11), 26–35.
[31] Rose, Borchert, Mitchell, & Connelly, 2020, pp. 6–7.
[32] Kerman, A. (2020, October 28). Zero Trust Cybersecurity: 'Never Trust, Always Verify.' *NIST*. https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify.
[33] Kerman, 2020; Rose, Borchert, Mitchell, & Connelly, 2020, pp. 6–7; Shore, Zeadally, & Keshariya, 2021.
[34] Gambo & Almulhem, 2025.
[35] Rose, Borchert, Mitchell, & Connelly, 2020, pp. 1, 4, 21–22.
[36] NASA Office of Inspector General, 2025.
[37] Cybersecurity and Infrastructure Security Agency, 2024, pp. 11–12.
[38] Waterman, S. (2024, July 22). *The Air Force's Zero Trust Strategy is Out—And Acknowledges Big Hurdles*. Air & Space Forces Magazine. https://www.airandspaceforces.com/air-force-strategy-zero-trust-risks/.
[39] Rose, Borchert, Mitchell, & Connelly, 2020, p. 30. Satellite communications represents one mission where commercial participation is likely heavy. For a potential implementation of ZTA in satellite communications contexts, see: Fu, P., Wu, J., Lin, X., & Shen, A. (2022). ZTEI: Zero-Trust and Edge Intelligence Empowered Continuous Authentication for Satellite Networks. *GLOBECOM 2022*, 2376–2381. https://doi.org/10.1109/GLOBECOM48099.2022.10000958.
[40] The Air Force's Zero Trust Strategy directly acknowledges the challenge of cultural resistance to ZTA implementation. Department of the Air Force Chief Information Officer. (2024). *Department of the Air Force Zero Trust Strategy*. https://www.dafcio.af.mil/Portals/64/Documents/Strategy/DAF%20Zero%20Trust%20Strategy%20v1.0%20(002).pdf.
[41] United States Department of Defense. (2025). *Executive Summary: Zero Trust for Operational Technology*. Office of Prepublication and Security Review. https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OperationalTechnologyActivitiesOutcomes.pdf.
[42] Cyber Range Project Team, & NICE Community Coordinating Council. (2023). *The Cyber Range: A Guide* (pp. 1–15). National Institute of Standards and Technology, United States Department of Commerce. https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf.
[43] Cybersecurity and Infrastructure Security Agency. (2025). *Zero Trust Architecture Implementation* [Fiscal Year 2024 Report to Congress]. United States Department of Homeland Security. https://www.dhs.gov/sites/default/files/2025-04/2025_0129_cisa_zero_trust_architecture_implementation.pdf.

# Potomac Institute for Policy Studies

*Science for Policy. Policy for Science.*

Never Trust, Always Verify



ABOUT THE POTOMAC INSTITUTE FOR POLICY STUDIES

The Potomac Institute for Policy Studies is an independent, nonpartisan, 501(c)(3), non-profit science and technology policy research institute. The Institute identifies and leads discussion on key science and technology issues facing our society. From these discussions and forums, we develop meaningful policy recommendations and ensure their implementation at the intersection of business and government.

FURTHER INFORMATION AND PERMISSIONS MAY BE REQUESTED FROM:

Potomac Institute for Policy Studies

Email: info@potomacinstitute.org

901 N. Stuart Street, Suite 1200
Arlington, Virginia 22203
Phone: (703) 525-0770

www.potomacinstitute.org