Public-Private Defence for Satellite Cybersecurity: Addressing Challenges Through Collaboration

Li Huang and Kimberly Cornell
University at Albany, USA

lhuang9@albany.edu
kacornell@albany.edu

Abstract: Commercial satellites play a pivotal role in maintaining civil communications and military operations. However, these privately operated space systems remain vulnerable, particularly when deployed in high-stakes public emergency scenarios where secure and continuous communication is critical. This paper examines the cyber risks associated with commercial satellite communication (SATCOM) networks, such as those operated by SpaceX and Amazon, when deployed during civil conflicts and national emergencies. We argue that the convergence of military reliance, profit-driven motives, and emerging AI-enabled cyber threats has created a critical need for a public–private cybersecurity paradigm. We analyse three core challenges: misaligned stakeholder interests, the rise of generative AI-enabled attacks, and transparency gaps in satellite protocol governance. Building on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the 2024 NIST AI Risk Management Framework (AI RMF), we propose an integrated approach for securing commercial SATCOMs. Our framework adapts NIST core functions to satellite systems and aligns sector-specific guidance from NIST Internal Reports (IR)s to facilitate coordination among government, military, and commercial actors. We further evaluate existing U.S. practices, including the Cybersecurity and Infrastructure Security Agency's Space System Working Group and the Space Force's Infrastructure Asset Pre-Assessment Program, to assess how cross-sectoral collaboration can be standardized and institutionalized. We argue for pre-emptive regulation on AI model deployment, cryptographic protocol disclosure, and open standards for hybrid satellite networks. By synthesizing technical frameworks with policy case studies, this study makes three contributions: first, it articulates a novel application of the NIST CSF to commercial satellite cybersecurity; second, it provides a conceptual bridge between AI risk management and satellite network governance; third, it offers practical strategies for harmonizing public benefit with private infrastructure in space-based communication. This research supports the development of a resilient satellite cybersecurity ecosystem that safeguards public trust and international stability.

Keywords: Commercial satellite, Cybersecurity, AI-Driven threat, Public-Private collaboration, NIST CSF, AI risk management framework

1. Introduction

Current estimates show over 7,500 satellites in orbit (Sebastian, 2025), potentially rising to nearly 100,000 in the next decade (Scharping, 2021). Private constellations like SpaceX and Kuiper are vital for global connectivity and security (Atlantic Council, 2024). Commercial satellite use expands to more actors, including agencies like the NSA (Greig, 2024). The U.S. must ensure trusted, secure space operations, driving innovation in launch, servicing, remote sensing, communication, and ground infrastructure (GeoTech Center, 2021). A strong space industry boosts U.S. security through industrial capacity, workforce, and innovation (Basham, 2024; Clark, 2024; Tucker, 2019).

Private companies like SpaceX, Amazon, and RocketLab focus on profit-driven innovation, which may conflict with cybersecurity (Atlantic Council, 2024; Basham, 2024; Clark, 2024; Tucker, 2019). Elon Musk's Starlink support to Ukraine initially aided critical communications, but subsequent threats to withdraw access due to funding constraints exposed vulnerabilities in proprietary systems for public benefit. As private satellites serve public and military needs, multiple stakeholders complicate security efforts (Starlink, 2022; Greig, 2024; Siegel, 2024; Industrial Cyber, 2024). Oversight is vital to balance profits and cybersecurity for national and humanitarian interests (Anderson and Moore, 2006; Quach et al., 2022; Van Camp and Peeters, 2022; Carlo and Obergfaell, 2024).

This study examines how public and private sectors can align interests to improve governance of AI-enabled satellite operations. We analyse cybersecurity challenges during emergencies, building on Cornell and Huang (Forthcoming). While that work is technical, this paper adds institutional, policy, and actor roles. Using NIST guidance, U.S. case studies, and governance practices, we propose a cybersecurity framework addressing mismatched interests, AI threats, and transparency, complementing technical models with governance for resilience and accountability.

2. Preliminaries

Space has become a conflict frontier involving governments, organizations, and entrepreneurs (Prado, 2024). Commercial satellites play a key role in warfare (Siegel, 2024), as they are vital for military and civilian communication. The Ukraine war shows how Starlink keeps Ukraine connected when terrestrial infrastructure fails (Starlink, 2022). Moreover, the dissemination of satellite imagery has bolstered U.S. and allied interests during the war in Ukraine. Photographic evidence of destroyed bases, bombed infrastructure, and the aftermath of missile strikes offered a glimpse into the realities of the war and exposed Russian hostilities and atrocities. Such imagery has the power to influence public opinion and, consequently, foreign policy. Russia targeted commercial space companies early, hacking Viasat during the invasion, harming Ukraine's space intelligence (Greig, 2024). Moscow also jams and disrupts unmanned aerial vehicles and satellites to hide troop movements, with jamming, cyberattacks, and electronic warfare, risking civil communication and space assets during conflicts.

However, as militaries increasingly target satellite intelligence, the civil services provided by commercial satellites are also being affected. Modern warfare, especially when it involves information infrastructure, cannot entirely separate military targets from public benefits. The US and its allies need to prioritize protecting commercial satellites from adversaries with advanced counter-space capabilities to prevent threats to future operations. Currently, no standard process exists for anti-satellite attack responses. Developing a flexible cybersecurity framework with communication protocols and data standards, adaptable to different actors, will secure space operations and serve the public. Without regulation, satellites cannot fully support humanitarian and civil services.

3. Literature Review

Cybersecurity of satellite communication (SATCOM) is a significant focus in academic research. Scholars have realized the vital role of commercial satellites during international humanitarian crises (Taggart et al., 2003; Doescher, Ristyb and Sunne, 2005). These satellites provide essential communication links when terrestrial infrastructure fails and offer invaluable imagery for assessing damage and directing aid efforts (Guida, 2021; Taggart et al., 2003; Doescher, Ristyb, and Sunne, 2023). Technological developments are making these commercial resources more accessible for government agencies, enhancing their ability to respond to crises. However, satellites and their ground stations are potential targets for cyber-attacks. These attacks aim to reduce the timely processing of satellite data into usable products and can disrupt communication, intercept sensitive information, or manipulate transmitted data (Bardin, 2025; Gilman, 2014). The increasing sophistication of cyber threats necessitates robust cybersecurity measures to protect SATCOM systems.

Various technological solutions have been proposed and implemented to enhance the security of SATCOMs in civil contexts (Maral, Bousquet and Sun, 2020). For instance, utilizing advanced encryption methods such as AES (Advanced Encryption Standard) ensures that data transmitted over satellite links is secure (Landau, 2000). End-to-end encryption further enhances security by protecting data from interception at any point in the communication chain (Cruickshank, 1996). However, despite the growing number of technical solutions, incidents involving SATCOM remain pervasive and severe (Industrial Cyber, 2024). As the space industry is increasingly competitive, actors in this field continuously develop and adopt new technologies and operational concepts for their space assets. However, these advancements not only introduce new risks but also create vulnerabilities in space systems through new data streams, communication links, and interconnected infrastructures. Cybercriminals strategically exploit these vulnerabilities to carry out their malicious intentions.

The increasing prevalence and severity of cyber threats to SATCOMs underscores the importance of external interventions (Elbert, 2004). Multiple mechanisms and institutions support SATCOMs for disaster response and humanitarian aid. The International Telecommunication Union (ITU) provides guidelines and support for deploying emergency communication systems during disasters, ensures the availability of SATCOM frequencies for emergency use, and offers training and resources to improve the use of SATCOMs in disaster response (Rothblatt, 1982).

Despite progress in technical safeguards, most studies emphasize encryption or data-link security rather than cross-sector governance. Existing scholarship often isolates technical safeguards from policy and governance considerations. Few examine how public-private coordination and AI risk management frameworks can be integrated into commercial satellite cybersecurity, leaving an interdisciplinary gap. This paper contributes by bridging NIST's technical standards with policy-driven governance mechanisms, generating a unified model that links technical, organizational, and regulatory dimensions of satellite cybersecurity.

4. Methodology Approach

This study adopts a qualitative document-analysis method, synthesizing guidance from NIST CSF, AI RMF, reports (such as NIST IRs 8270, 8323, 8401, 8441), U.S. Space Force (USSF) directives, and case analyses such as Starlink in Ukraine. Primary sources were selected for their relevance to commercial satellite security and cross-sector governance. The analysis maps policy provisions and institutional mechanisms to the NIST CSF core functions, identifying practical coordination gaps among stakeholders and best practices. The Starlink-Ukraine case reference illustrates practical implications and validates conceptual consistency.

5. Challenges

Several challenges hinder the development of a strong security posture in commercial SATCOM. During humanitarian crises, SATCOM can become vulnerable and less secure.

5.1 Misaligned Interests

Misaligned interests hinder network communication, leading to conflicts such as those between security responsibilities and beneficiaries (Anderson and Moore, 2006). These conflicts include profit versus privacy, as seen in hospitals and insurers prioritizing costs over patient privacy. In SATCOMs, private sector goals clash with regulatory aims; private satellite owners seek profits, risking vulnerabilities if costs are cut. There is also tension between corporate data privacy and security priorities, with private companies often valuing data monetization over privacy (Quach et al., 2022). These conflicts challenge regulation and security efforts.

5.2 Technological Challenges: AI-Driven Cyber Threats

The rapid advancement of AI technologies has introduced new threats to SATCOM (Sierra Space, 2024). Generative AI models can identify and exploit known vulnerabilities in real-world systems (Fang et al., 2024), significantly enhancing the effectiveness of cyber-attacks on satellite systems. Many legacy SATCOM systems still use outdated cryptographic units that conform to previously suggested standards (Breda et al., 2022).

AI algorithms can automate the detection of weak points in satellite networks (Wang et al., 2023), making it easier for attackers to launch sophisticated cyber-attacks. Large language model (LLM)-informed reconnaissance leverages generative AI to analyse SATCOM protocols and radar imaging tools, allowing attackers to gather crucial information about potential targets.

In international conflicts, the deployment of generative AI models on satellites can influence the course and outcome of wars by creating interference (Maguire, 2024). Recently, Fancy Bear, a division of the Russian GRU military intelligence, has begun applying AI models to leverage satellite and radar infrastructures, potentially interfering with the war process in Ukraine (Security Staff, 2024). Additionally, AI-driven spoofing attacks can mislead satellite navigation systems, causing significant disruptions in military and civilian operations (Egozi, 2024).

5.3 Lack of Transparency

The lack of access to standardized protocols and the potential unregulated actions of private companies in deploying generative AI models present significant risks to SATCOMs. Without commonly accepted protocols, ensuring the security and integrity of SATCOMs becomes challenging, increasing susceptibility to cyber-attacks. Moreover, private companies may not disclose their AI development processes, data sources, or training methodologies. This lack of transparency prevents regulatory authorities from recognizing the potential harmful consequences of these AI models and complicates effective regulation (Feuerriegel et al., 2024; Scherer, 2015; Felzmann et al., 2019). Furthermore, private companies might not adhere to rigorous testing and validation processes, increasing the likelihood of deploying flawed or insecure AI models that can be exploited by adversaries (Jobin, Ienca and Vayena, 2019).

6. Satellite Cybersecurity Framework

We propose a tiered satellite cybersecurity framework based on the NIST CSF and AI RMF, integrated with threat modelling and empirical risk analysis. First, the NIST framework (NIST, 2014) assesses security, offering a structured approach:

- Identify: Understand cybersecurity risks to satellite systems by cataloguing assets, assessing vulnerabilities, and identifying critical components.

- Protect: Implement safeguards to ensure the security of satellite operations, e.g., access control, encryption, etc.
- Detect: Promptly identify cybersecurity events, including monitoring SATCOMs and detecting unauthorized access or anomalies.
- Respond: Mitigate the impact of cybersecurity incidents affecting satellite systems, ensuring coordinated and effective response actions.
- Recover: Restore satellite systems and services after a cybersecurity incident, including repairing affected components and improving resilience for future threats.

Second, the NIST IRs offer detailed guidance for space assets, hardware, and infrastructure. IR 8270 covers spacecraft, IR 8401 addresses terrestrial infrastructure, IR 8323 targets GPS users, and IR 8441 covers hybrid systems like terminals and payloads.

6.1 Interest Alignment

NIST frameworks can address misaligned interests between private companies and authorities in commercial SATCOM security by fostering collaboration and establishing shared goals. Its cybersecurity framework is developed through collaborative input from both government and private sector stakeholders. The collaborative input ensured the formation of consensus-driven standards and guidelines, which balance national security needs with the operational priorities of private entities (Scarfone et al., 2009; Rivest et al., 1992). Second, NIST facilitates public-private partnerships, encouraging intelligence sharing among diverse stakeholders. By highlighting the economic risks of cybersecurity failures, the framework emphasizes the mutual benefits of robust cybersecurity, including the protection of critical infrastructure and the competitive advantage of securing communication networks (Van Camp and Peeters, 2022; Scholl, Scholl and Suloway, 2023; Carlo and Obergfaell, 2024). Furthermore, with a focus on transparency and adaptability, it helps harmonize regulatory requirements with business innovation, enabling a balanced and cooperative approach to SATCOM security (Carayannis and Roy, 2000).

6.2 AI Risk Management

In 2024, NIST published AI RMF to address risks in AI-driven SATCOM (NIST, 2024). Incorporating both traditional cybersecurity concerns and AI-specific threats, it guides organizations to identify vulnerabilities unique to AI systems, such as adversarial attacks, data poisoning, or model drift, which could compromise SATCOMs. Additionally, AI RMF emphasizes secure development of AI systems in SATCOM through practices such as robust model training to defend AI models against manipulated inputs, advocating for the use of verified and sanitized datasets, and employing interpretable AI models to detect malicious behaviour (Lim and Kwon, 2024; NIST, 2024). More importantly, NIST frameworks promote collaboration across sectors, working with industry and academia to develop threat intelligence and stay ahead of evolving AI cyber threats (Protik, 2023). By encouraging innovation in defensive AI technologies, the framework supports a secure and adaptive approach to managing AI risks in SATCOM.

The integration of the AI RMF outlines four core functions of SATCOM security:

- Map: Identify AI-enabled components within SATCOM systems, including where LLMs, routing optimization, or anomaly detection are deployed.
- Measure: Assess risk using metrics such as model interpretability, robustness to adversarial inputs, and the potential for misuse (e.g., spoofing or data extraction).
- Manage: Implement security controls and incident response strategies tailored to AI-specific vulnerabilities like data poisoning or model drift.
- Govern: Establish organizational policies for responsible AI use, ensuring transparency and accountability through audits and regulatory reports.

6.3 Transparency in Protocols

To address the lack of transparency in the deployment of generative AI in SATCOMs, greater transparency, and scholarly research on the protocols used are encouraged. Authorities should set clear guidelines and promote research on protocols. NIST has created frameworks emphasizing standardized protocols and regulations to reduce AI deployment risks (NIST, 2024). Companies should provide detailed documentation on their AI models, including training data, sources, and algorithms, accessible to regulators and researchers for accountability. The industry should also develop detailed open standards for SATCOM protocols. For example, NIST's 2023 'Cybersecurity Framework Profile for Hybrid Satellite Networks' (HSN, 2024) offers cybersecurity guidance that

can inform communication protocol standards. Table 1 shows the stakeholder responsibility matrix, pairing challenges with actors best suited to address them, translating conceptual frameworks into practical roles for accountability and coordination.

Table 1: Responsibility matrix among stakeholders

Challenge	Government	Military	Commercial	Multilateral Organizations
Misaligned Interests	Policy enforcement, procurement standards	Operational assurance, mission alignment	Profit-security trade-off decisions	Norm-setting and trust frameworks
AI-Driven Threats	Regulate AI development	AI Defence innovation, rapid response	Secure AI deployment, testing	Promote shared AI threat intelligence
Lack of Transparency	Mandate disclosure, standardization	Cyber vetting of contractors	Publish protocols, share risk data	Foster global accountability

6.4 Integrated Framework of Public-Private Satellite Cybersecurity

To visualize the proposed framework, we integrate the NIST CSF and the AI RMF into a layered model for satellite-network governance, depicted in Figure 1. The outer layer, incorporating the five CSF functions from Section 6, structures the technical and operational defences of SATCOM systems. The inner layer contains AI RMF's four core functions from Section 6.2, overseeing AI components like threat detection, routing, and analytics. At the intersection are three actor domains, government, military, and commercial, linked by channels for sharing, transparency, and accountability. The model illustrates a continuous loop where safeguards, AI risk controls, and governance reinforce each other to maintain a resilient satellite-cybersecurity ecosystem.

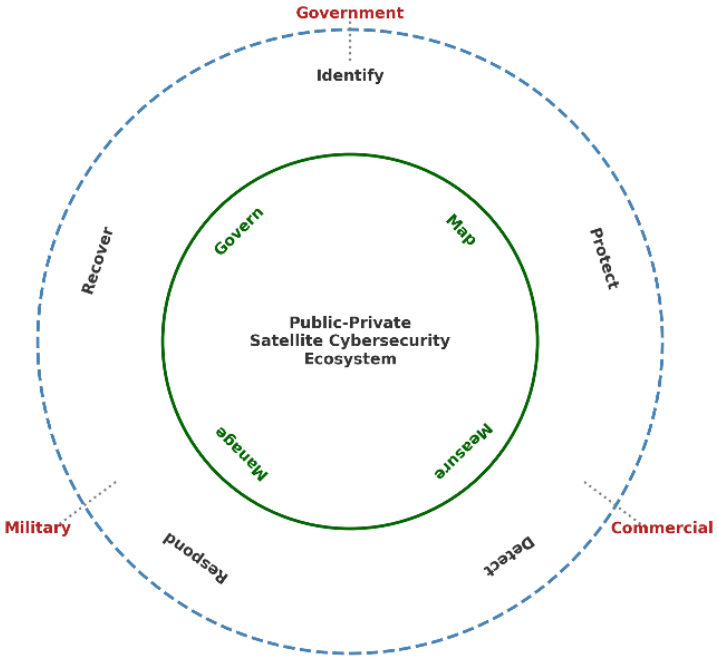

Figure 1: Integrated NIST CSF–AI RMF Framework for Public-Private Satellite Cybersecurity

7. The U.S. Practice

We outline key practices implemented by the U.S. to enhance satellite security and evaluate the collaborative efforts of multiple stakeholders in safeguarding SATCOM. The U.S. has adopted diverse strategies to establish and maintain multi-layered cooperation in satellite cybersecurity, aiming to prevent disruptions and ensure the resilience of SATCOMs for public benefits as well as national security.

7.1 Government Perspective

The U.S. government hosts forums, workshops, and research projects where agencies and private companies collaborate on cybersecurity and innovation. In 2021, the Cybersecurity and Infrastructure Security Agency formed the "Space System Critical Infrastructure Working Group," which operates under the Critical Infrastructure Partnership Advisory Council (CISA, 2021). This group, comprising government and industry members, brings together stakeholders of critical space infrastructure to improve the security and resilience of U.S. space systems, identify areas for improvement, and develop solutions for managing cyber risks to protect critical space-based assets.

7.2 Military Perspective

The USSF focuses on the resilience of space infrastructure and the cybersecurity defence of space networks, underscoring the growing integration of space and cyber domains. In 2023, General B. Chance Saltzman outlined three priorities, including deploying combat-ready forces to enhance the resilience of ground stations, networks, and mission facilities (USSF, 2023). Currently, USSF coordinates with U.S. Cyber Command through a dedicated Air Force component (Dziwisz and Romaniuk, 2023). In the future, the USSF aims to establish its own Cyber Command component, like other combat commands, to better address space cybersecurity (USSF, 2023). The focus is shifting from traditional IT support to rapid cybersecurity defence of critical space networks (USSF, 2024).

7.3 Commercial – Government

Collaboration between private companies and public agencies frames SATCOM security as a shared priority that benefits both. The USSF's Infrastructure Asset Pre-Assessment Program (IAPP), launched in 2022, serves as a model for evaluating the cybersecurity posture of commercial satellite assets prior to government and military procurement (Space Force, 2022). In 2020, the USSF's Commercial Satellite Communications Office announced a new cybersecurity program, which was implemented as the Infrastructure Asset Pre-Assessment Program in January 2022, with an expected 18-month timeline (Infrastructure asset pre-assessment program, 2020). This program aims to test the cybersecurity qualifications of commercial SATCOM products and advance the security posture of current and future commercial SATCOMs procurements for the Department of Defence (Infrastructure asset pre-assessment program, 2020). By 2026, the program will apply standardized security assessments to all commercial satellite contracts, streamlining procurement and enhancing resilience (Infrastructure asset pre-assessment program, 2020).

The IAPP represents a significant step in embedding cybersecurity into satellite procurement. It provides a standardized mechanism for assessing the security posture of commercial satellite assets before government or military adoption. Using vulnerability assessments, compliance checks, and red-teaming simulations, the program generates cybersecurity ratings that inform procurement eligibility. Beyond fostering accountability in the private sector, IAPP offers a replicable model for allied nations. Its implications extend internationally; countries with limited cybersecurity capacity could adopt IAPP protocols to audit foreign satellite providers operating within their borders, thereby enhancing global resilience.

7.4 Commercial–Military

The development of military-commercial hybrid networks at the technological level is crucial to integrating SATCOM systems. In 2021, Viasat signed a seven-year research contract with the U.S. Air Force Research Laboratory to develop a "hybrid-network" framework suitable for both commercial and government SATCOMs, aiming to seamless network operations across commercial and military satellite networks (Erkel, 2023).

7.5 Collaboration

The collaboration between the U.S. government, private sector, and military in SATCOM security focuses on strengthening satellite cybersecurity through joint initiatives and shared expertise. It standardized cybersecurity practices across stakeholders to mitigate space risks. For instance, the U.S. could work with NATO, the European Space Agency, and Asia-Pacific space alliances to promote IAPP as a de facto standard. A global registry of certified satellite operators, aligned with NIST CSF and AI RMF guidelines, would provide a much-needed trust layer for space assets used in emergencies, defence, and international aid missions.

8. Discussion and Conclusion

This study explores a pathway through which public and private sectors can align their interests to enhance the cybersecurity of commercial SATCOMs, particularly in humanitarian crisis contexts. We identified three

interrelated challenges: misaligned stakeholder interests, AI-driven cyber threats, and a lack of transparency in protocol governance. These challenges highlight the complexity of securing satellite networks that are profit-driven, publicly utilized, and rapidly evolving technologically.

To address these issues, this study proposed an integrated NIST CSF–AI RMF model that bridges technical safeguards and governance mechanisms. The outer CSF layer organizes operational defences around the five functions, while the inner AI RMF layer focuses on risk management for AI-enabled systems. By embedding these frameworks within the collaborative domains of government, military, and commercial stakeholders, the model visualizes how transparency, intelligence sharing, and accountability can reinforce one another.

Case analyses of U.S. practices, including the Cybersecurity and Infrastructure Security Agency's Space Systems Working Group and the USSF's IAPP, demonstrate that structured collaboration and pre-procurement cybersecurity assessments can standardize trust among partners. Overall, these findings illustrate that technical resilience and institutional coordination must evolve together to secure commercial satellite ecosystems.

8.1 Implications

8.1.1 Theoretical implications

This study contributes to cybersecurity governance theory by integrating AI risk management into space cybersecurity frameworks. It shows how NIST CSF and AI RMF can jointly function as a socio-technical governance model, linking policy compliance with technical assurance. The framework supports public–private cyber governance by addressing asymmetric information, promoting standardization, and institutionalizing accountability.

8.1.2 Practical implications

The proposed model provides a structure for operationalizing collaboration among government agencies, defence institutions, and private satellite operators. For instance, commercial entities can adopt it as an internal compliance benchmark to ensure AI components meet risk-management requirements under the AI RMF. Defence sectors can employ the model to establish continuous cybersecurity assurance across hybrid commercial-military networks. The responsibility matrix in Section 6 translates coordination principles into actionable roles, enabling practitioners to implement layered accountability in real-world operations.

Overall, these findings show that technical resilience and institutional coordination must evolve together to secure commercial satellite ecosystems. Building on prior technical models that integrate NIST CSF and AI RMF into satellite cybersecurity architectures, this study contributes a governance-oriented extension that emphasizes stakeholder alignment, transparency, and policy mechanisms. Together, these efforts support the development of a robust, multi-layered defence strategy for space-based infrastructure.

8.2 Limitations and Future Research

This study is primarily based on qualitative document analysis using publicly available reports and policy documents, which limits empirical validation. Future research should include quantitative risk modelling, cryptographic protocol testing for satellite systems like Starlink, and expert interviews. Integrating economic valuation models (e.g., Return on Security Investment) and AI-based threat prediction could also enhance the analytical depth of future work.

Ethics declaration: Ethical approval was not required.

AI declaration: AI tools were not used in the creation of this paper.

References

Anderson, R. and Moore, T., 2006. The economics of information security. *science*, *314*(5799), pp.610-613.

Atlantic Council (2024) *Assured space operations for public benefit.* Available at: https://www.atlanticcouncil.org/ content-series/geotech-commission/chapter-6/ (accessed: 2024-06-13).

Bardin, J.S., 2025. Satellite cyber attack search and destroy. In *Computer and Information Security Handbook* (pp. 1561-1580). Morgan Kaufmann.

Basham, S. (2024) *The critical role of space in modern warfare and the imperative of joint space capabilities in Europe.* Available at: https://www.eucom.mil/article/42685/thecritical- role-of-space-in-modern-warfare-and-the-imperative-of-joint-spacecapabilitie (accessed: 2024-06-13).

Breda, P., Markova, R., Abdin, A., Jha, D., Carlo, A. and Mantı, N.P., 2022, September. Cyber vulnerabilities and risks of AI technologies in space applications. In *73rd International Astronautical Congress (IAC), Paris, France*.

Carayannis, E.G. and Roy, R.I.S. (2000) Davids vs Goliaths in the small satellite industry: The role of technological innovation dynamics in firm competitiveness. *Technovation*, 20(6), pp.287–297.

Carlo, A. and Obergfaell, K. (2024) Cyber attacks on critical infrastructures and satellite communications. *International Journal of Critical Infrastructure Protection*, 46, 100701.

Clark, S. (2024) Taking stock: Private investment in space companies rebounded in 2023. *Ars Technica*. Available at: https://arstechnica.com/space/2024/01/taking-stock-privateinvestment-in-space-companies-rebounded-in-2023/ (Accessed: 2024-06-20).

Cornell, K.A. and Huang, L., Forthcoming. *Resilient Satellite Cybersecurity: Integrating NIST and AI Governance*. To be presented at the 16th EAI International Conference on Digital Forensics & Cyber Crime (ICDF2C), Miami, Florida, November 2025. To appear in Springer LNICST series, expected May 2026.

Cruickshank, H. (1996) A security system for satellite networks. In: *Fifth International Conference on Satellite Systems for Mobile Communications and Navigation*, pp.187–190. IET.

Cybersecurity and Infrastructure Security Agency (2021) *CISA launches a space systems critical infrastructure working group*. Available at: https://www.cisa.gov/news-events/news/cisa-launches-space-systems-critical-infrastructure-working-group.

Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN) (2024) *NIST Interagency Report 8441*. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8441.pdf (Accessed: 11 September 2024).

Doescher, S., Ristyb, R. and Sunne, R. (2005) Use of commercial remote sensing satellite data in support of emergency response. In: *ISPRS Workshop on Service and Application of Spatial Data Infrastructure*, pp.14–16.

Dziwisz, D. and Romaniuk, S.N. (2023) US Cyber Command (USCYBERCOM). In: *The Handbook of Homeland Security*, pp.305–314. CRC Press.

Egozi, A. (2024) New protections deployed against attacks on navigation systems. *Aviation International News*. Available at: https://www.ainonline.com/aviation-news/airtransport/2024-07-16/new-protections-deployed-against-attacks-navigationsystems.

Elbert, B.R. (2004) *The satellite communication applications handbook*. Artech House.

Erkel, D. (2023) *The Success of Emerging Space Actors: Effective Strategies in the NewSpace Era*. Ph.D. thesis. Massachusetts Institute of Technology.

Fang, R., Bindu, R., Gupta, A. and Kang, D. (2024) LLM agents can autonomously exploit one-day vulnerabilities. Available at: https://arxiv.org/abs/2404.08144.

Felzmann, H., Villaronga, E.F., Lutz, C. and Tamò-Larrieux, A. (2019) Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. *Big Data & Society*, 6(1), 2053951719860542.

Feuerriegel, S., Hartmann, J., Janiesch, C. and Zschech, P. (2024) Generative AI. *Business & Information Systems Engineering*, 66(1), pp.111–126.

GeoTech Center (2021) *Cybersecurity of space-based assets and why this is important*. Available at: https://www.atlanticcouncil.org/insight-impact/in-the-news/cybersecurity-of-space-based-assets-and-why-this-is-important/.

Gilman, D. (2014) Cyber-warfare and humanitarian space. In: *Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management*. European Interagency Security Forum (EISF).

Greig, J. (2024) NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation. Available at: https://therecord.media/viasat-hack-was-two-incidentsand-resulted-in-sanctions (Accessed: 13 June 2024).

Guida, E. (2021) *The use of satellites in humanitarian contexts*. Norwegian Centre for Humanitarian Studies.

Industrial Cyber (2024) *New Deloitte report addresses increasing danger of cyber threats in space, issues call to action*. Available at: https://industrialcyber.co/reports/newdeloitte-report-addresses-increasing-danger-of-cyber-threats-in-space-issues-callto-action/#:~:text=Reports,of%20the%20space%20industry%20itself.

Infrastructure asset pre-assessment program (2020) Available at: https://www.airandspaceforces.com/tag/infrastructure-asset-pre-assessment-program/.

Jobin, A., Ienca, M. and Vayena, E. (2019) The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), pp.389–399.

Landau, S. (2000) Communications security for the twenty-first century: The Advanced Encryption Standard. *Notices of the AMS*, 47(4), pp.450–459.

Lim, J.S. and Kwon, T. (2024) Applying NIST AI Risk Management Framework: Case study on NTIS database analysis using Map, Measure, Manage approaches. *Journal of Korean Society of Industrial and Systems Engineering*, 47(2), pp.21–29.

Maguire, P. (2024) AI at the crossroads of cybersecurity, space and national security in the digital age. *SpaceNews*. Available at: https://spacenews.com/ai-crossroads-cybersecurity-space-national-security-digital-age/ (accessed: 2025-01-17).

Maral, G., Bousquet, M. and Sun, Z. (2020) *Satellite Communications Systems: Systems, Techniques and Technology*. 6th ed. Chichester: John Wiley & Sons.

National Institute of Standards and Technology (NIST) (2014) *Cybersecurity Framework*. Available at: https://www.nist.gov/cyberframework.

National Institute of Standards and Technology (NIST) (2024) *AI Risk Management Framework*. Available at: https://www.nist.gov/itl/ai-risk-management-framework.

Prado, B. (2024) Space: The next frontier for innovation, economics, accessibility, and infrastructure. *Atlantic Council*. Available at: https://www.atlanticcouncil.org/blogs/geotech-cues/event-recap-space-the-next-frontier-for-innovation-and-more/ (Accessed: 13 June 2024).

Protik, R.C. (2023) Updated standard for secure satellite communications: Analysis of satellites, attack vectors, existing standards, and enterprise and security architectures. *arXiv preprint*, arXiv:2310.19105.

Quach, S., Thaichon, P., Martin, K.D., Weaven, S. and Palmatier, R.W. (2022) Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), pp.1299–1323.

Rivest, R.L., Hellman, M.E., Anderson, J.C. and Lyons, J.W. (1992) Responses to NIST's proposal. *Communications of the ACM*, 35(7), pp.41–54.

Rothblatt, M.A. (1982) ITU regulation of satellite communication. *Stanford Journal of International Law*, 18, 1.

Scarfone, K., Benigni, D., Grance, T. et al. (2009) Cyber security standards. Gaithersburg, MD: National Institute of Standards and Technology (NIST).

Scharping, N. (2021) The future of satellites lies in the constellations. *Astronomy*, June. Available at: https://astronomy.com/news/2021/06/the-future-of-satellites-lies-in-giant-constellations.

Scherer, M.U. (2015) Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, 29, pp.353–400.

Scholl, M., Scholl, M. and Suloway, T. (2023) *Introduction to cybersecurity for commercial satellite operations*. Gaithersburg, MD: US Department of Commerce, National Institute of Standards and Technology.

Sebastian, K.A. (2024) *Union of Concerned Scientists (UCS) satellite database*. Available at: https://www.ucsusa.org/resources/satellite-database (Accessed: 21 November 2022).

Security Staff (2024) US adversaries employ generative AI in attempted cyberattack. *Security Magazine*, February. Available at: https://www.securitymagazine.com/articles/100418-us-adversariesemploy-generative-ai-in-attempted-cyberattack.

Siegel, J. (2024) Commercial satellites are on the front lines of war today. Here's what this means for the future of warfare. *Atlantic Council*. Available at: https://www.atlanticcouncil.org/contentseries/airpower-after-ukraine/commercial-satellites-are-on-the-front-lines-of-war-today-heres-what-this-means-for-the-future-of-warfare/ (Accessed: 2024-06-13).

Sierra Space (2024) Generative AI in the space industry: Revolutionizing engineering, monitoring, and support roles. Available at: https://www.sierraspace.com/blog/generative-ai-in-the-space-industry-revolutionizing-engineering-monitoring-and-support-roles/.

Space Force (2022) *Space Force finally rolls out cyber standards for commercial SATCOM providers*. Available at: https://www.airandspaceforces.com/space-force-finally-rolls-outcyber-standards-for-commercial-satcom-providers/#:~:text=Space%20Force%20Finally%20Rolls%20Out,Space%20Force%20graphic.

Starlink (2022) Why is Elon Musk launching thousands of satellites? *BBC News*, August. Available at: https://www.bbc.com/news/technology-62339835.

Taggart, D., Bayuk, F., Ping, D., Hant, J. and Marshall, M. (2003) Usage of commercial satellite systems for homeland security communications. In: *2003 IEEE Aerospace Conference Proceedings* (Cat. No. 03TH8652), vol. 2, pp.2_1155–2_1165. IEEE.

Tucker, P. (2019) The NSA is studying satellite hacking. *Defense One*, September. Available at: https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/ (Accessed: 2022-11-23).

U.S. Space Force (USSF) (2024) *Commercial Space Strategy*. Available at: https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/USSF_Commercial_Space_Strategy.pdf.

United States Space Force (USSF) (2023) *CSO releases lines of effort*. Available at: https://www.spaceforce.mil/News/Article/3270867/cso-releases-lines-of-effort/.

Van Camp, C. and Peeters, W. (2022) A world without satellite data as a result of a global cyber-attack. *Space Policy*, 59, 101458.

Wang, Y., Chen, P., Ai, S., Liang, W., Liao, B., Mo, W. and Wang, H. (2023) Two-stage anomaly detection in LEO satellite network. In: Yung, M., Chen, C. and Meng, W. (eds.) *Science of Cyber Security*. Cham: Springer Nature Switzerland, pp.423–438.