Small Satellites with Large Exposure

How Does New Space Fare in Cyberspace?

By Captain Luke Stensberg, US Space Force, JAPCC

The Advent of Small Satellites

In recent years, both public and private actors have embraced innovations in the space industry that have allowed for a democratization of space, known colloquially as ***new space***. New space consists of various advancements that improve cost efficiency and accelerate development cycles, opening the door for new actors to access space. One prominent new space trend is small satellites, characterized by many, individually lesser-valued satellites that comprise a scalable and meshed constellation, typically in Low-Earth Orbit (LEO). Together they reduce latency due to their proximity to Earth and can offer robust coverage when adequately scaled.

The emergence of small satellites represents a significant departure from the traditional space operations conducted by large governmental organizations. Historically, these organizations would deploy exquisite capabilities in Geostationary Orbit (GEO), which was financially and technologically inaccessible to smaller players. Nowadays, new actors are emerging who can quickly and affordably procure or develop small satellites that leverage standardized and miniaturized Commercial Off the Shelf (COTS) components, piggyback on other launches, and even Command and Control (C2) missions with web-accessible ground infrastructure.[1] These advancements lower the need for full vertical integration, significantly cutting development barriers and overhead.

Besides development speed and cost savings, small satellite LEO architectures inherently offer operational resilience through their proliferation. For example, an adversary cannot easily deny space capabilities kinetically when many more satellites share the load in delivering the mission's Data, Products, and Services

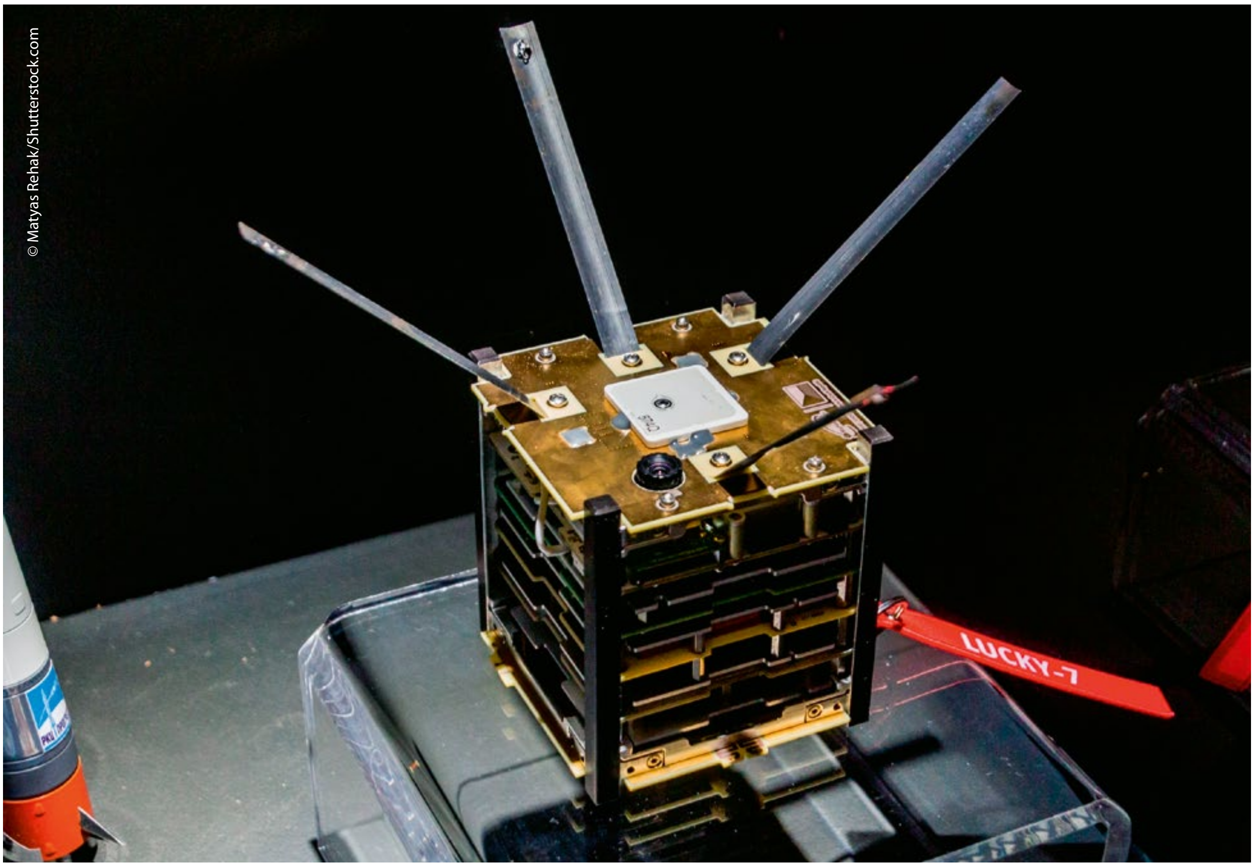
(DPS). Destroying one or even several small satellites would, at most, degrade said DPS. Beyond this, scaling up kinetic strikes to destroy the preponderance of these small satellites – enough to significantly degrade or fully deny the capability – is not as practical and could risk an ever-escalating positive feedback loop of debris yielding indiscriminate collateral damage. This could potentially reach the point of the Kessler Effect, in which LEO becomes hazardous for all space actors, friend and foe alike.[2] Surely, proliferated constellations tilt the cost-benefit analysis of kinetic-minded aggressors enough to think twice about taking on proliferated small satellite constellations in this manner. Consequently, a top US space official recently claimed that satellites are more likely to be targeted through non-kinetic means, specifically through the cyber domain.[3]

[…] *'As the space domain becomes more intertwined with the cyber domain to lower costs and increase convenience, the benefits may come with the additional risks inherent to cyberspace.'*

The Risk of Small Satellites in Cyberspace

Small satellite designs focus on affordability, simplicity, and standardization to promote scalability. This trend has even paved the way for the CubeSat concept. CubeSats are a subset of nanosatellites based on one or more 10x10x10 cm units (1U) that often utilize widely available and standardized components. These can be standalone or modular since multiple units, for example, three 1Us, may form a larger 3U CubeSat. Despite relative simplicity in design, small satellites can scale in numbers to produce constellations that can provide key DPS to NATO warfighters such as C2, ISR, and more. However, cybersecurity experts are warning that this ease of development, scalability, and operations may encourage potential design shortcuts that bring cybersecurity trade-offs.[4] Interconnectivity and standardization can diminish the obscurity of space systems, which once deterred malicious cyber actors from targeting such historically foreign systems.

[M] © Albert89/Shutterstock.com



© Matyas Rehak/Shutterstock.com

A one unit (1U) CubeSat typically weighs less than 2 kg and is relatively cheap, thanks to its reliance on COTS components.

These shifts in design are analogous to when industry began enabling remote access for Industrial Control Systems (ICS) to control water, energy, manufacturing, and logistical processes. While remote management improved ICSs' operational efficiency, it is evident many ICS systems were hastily networked, often neglecting cybersecurity. Recently, a cybersecurity firm reported that their ICS honeypots – decoy networks designed to mimic real networks to lure attackers – detected an average of 813 unique attacks daily. This is an alarming indicator because there is no current patch or remediation for 34 % of ICS cybersecurity vulnerabilities in 2023, up from 13 % in 2022.[5] At the strategic level, vulnerabilities in critical national infrastructure now pose geopolitical risk, as evidenced by the Five Eyes nations recently condemning China for targeting US infrastructure with malicious cyber activity.[6]

Therefore, the broader space community, both public and private, must balance their pace of innovation with cybersecurity to avoid ending up as vulnerable in cyberspace as terrestrial ICSs are. Implementing cybersecurity as an afterthought is less effective and more expensive reactively than if done proactively. Meanwhile, as the space industry is rapidly growing at 9 % per annum with projections to reach $1.8 trillion by 2035, this target-rich environment will surely attract malicious cyber actors.[7] If NATO nations decide to increase their reliance on small satellites, they need to understand how one cyber-attack could massively impact operations across multiple domains.

Security (Challenges) From the Ground Up

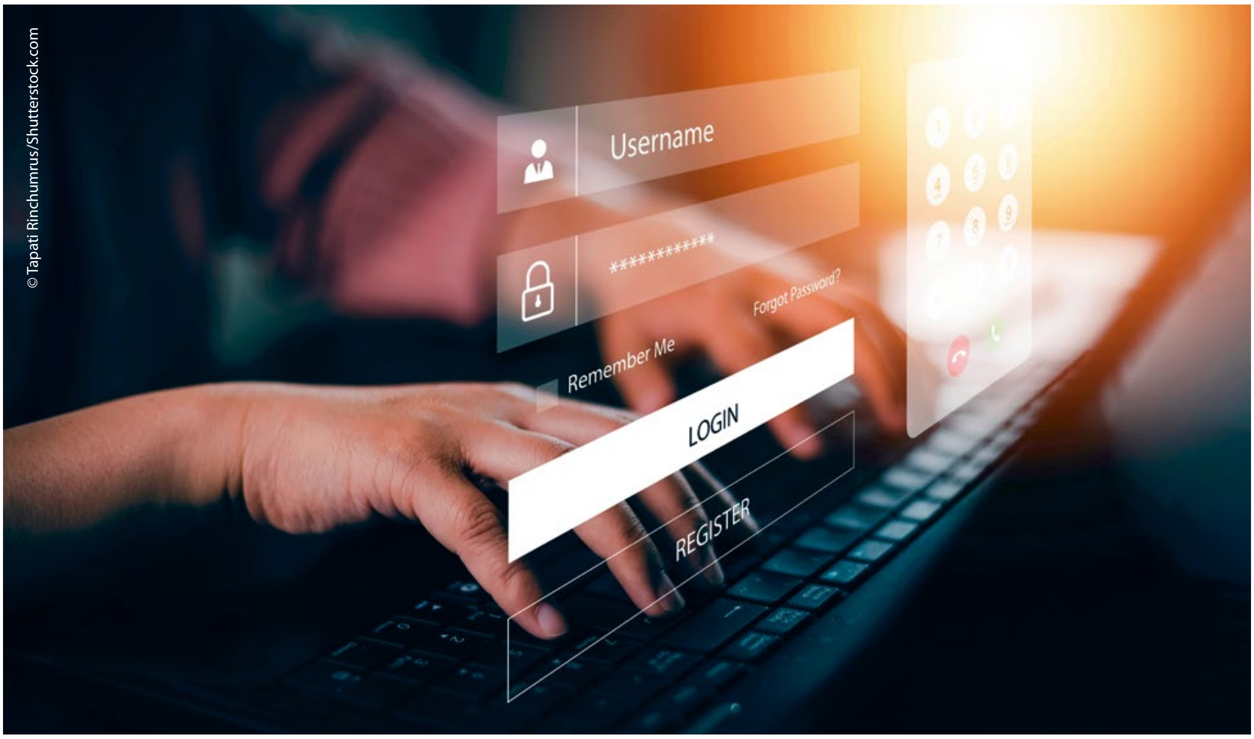
NATO defines space as possessing four segments: ground, user, link, and space.[8] All segments are crucial, so if a cyber actor can deny, degrade, disrupt, or destroy any of them, the entire delivery of space DPS is impacted. This expands the attack surfaces compared to the mission-relevant terrain of typical terrestrial networks. The following sections examine some new space concepts as they relate to each space segment, along with potential vulnerabilities if left unchecked. This article will only sparingly address the user segment since it is more agnostic to the type of space architecture utilized within this cybersecurity context, be it old or 'new'. For example, Russia's 2022 AcidRain cyber-attack on over 10,000 European ViaSat modems was user segment-focused, making the types of ViaSat ground stations and satellites irrelevant to the attack.[9]

The Ground and User Segments

Ground stations are required for tracking, C2, and data transmission to and from satellites, so naturally they pose as ripe targets to impact space operations. Any uplinked commands or downlinked tracking and telemetry data will flow with implicit trust between the ground station and satellite due to the (hopefully) encrypted link segment. Therefore, to impact the spacecraft, malicious cyber actors may look to leverage the ground station as a pathway.

Designing and building a network of ground stations for LEO spacecraft is very expensive. Unlike GEO satellites, which remain relatively stationary from the perspective of a ground station, LEO satellites may move in and out of view in less than 15 minutes due to their high velocity and lower altitudes. Therefore, a LEO constellation may require numerous ground stations scattered globally.[10] This has historically meant unsurmountable up-front infrastructure costs for smaller actors. To respond, large cloud service providers like Amazon Web Services and Microsoft Azure now offer leased access to their own worldwide network of ground station antennae along with cloud computing and web-accessible storage services.

This business model is called Ground Station as a Service (GSaaS), and it allows smaller actors to circumvent substantial initial investments required to build a network of ground stations. Satellite operators pay small usage fees to access a cloud environment that can relay space commands and data via the various



© Tapati Rinchumrus/Shutterstock.com

Technology has advanced to allow for efficient remote access to operational control systems, now including satellites.

© PX Media – stock.adobe.com

Data Centres host Ground Station as a Service (GSaaS) command and control services.

GSaaS antennae to communicate with the satellites. Besides C2, these cloud services can also push the user segments to the cloud by, for example, allowing customers direct access to the satellite imagery.

GSaaS migrates access to satellites from air-gapped, in-house networks to the cloud, expanding the attack surface due to the inability to completely isolate vulnerable assets. While the cloud environment can be very secure, some cloud customers falsely assume that they can outsource all their cybersecurity responsibilities to the cloud providers. In fact, experts estimate that 99% of cloud security failures will be the customer's fault by 2025.[11] Therefore cloud exploitations have already begun as a leading cybersecurity firm published in its 2023 annual report stating that cloud environment intrusions increased 75 % over 2022.[12] The most dedicated malicious cyber actors could even theoretically pay to legitimately gain access to GSaaS services, only to conduct their own reconnaissance by probing for vulnerabilities. As the space domain becomes more intertwined with the cyber domain to lower costs and increase convenience, the benefits may come with the additional risks inherent to cyberspace.

The Link Segment

The link segment is the electromagnetic connection between the ground and user segments to the satellite(s), and satellites to one another. A key development in small satellite communications is the shift from analogue transceivers to digital Software-Defined Radios (SDRs). SDRs are radios in which physical functions normally conducted by hardware are instead executed by software. While affordable and convenient, some commercially available SDRs used by small satellites may have configurable code that has been exploited in realistic lab settings.

In one study, a team of Air Force Institute of Technology researchers simulated a ground station linked to a small satellite with commonly used hardware, open-source software, and an SDR. They were able to glean valid commands from the lab's ground station to prepare their own identically formatted commands. However, they transmitted commands with malevolent adjustments to spoof the satellite's positioning data used to orient itself relative to the sun.[13] Despite the commands originating from an unknown source, the SDR still accepted the attacker's commands to adjust the satellite attitude improperly. Hypothetically, the malicious commands would have conducted a manoeuvre that could risk damaging solar cells and optical sensors, and would deplete limited propellant. Additionally, other researchers have also highlighted that certain SDR configurations are susceptible to buffer overflow cyber-attacks.[14] This type of attack has disruptive effects analogous to electromagnetic jamming, although with far more subtlety because it does not generate high levels of power that could be geolocated.

> **[…]** *'There are difficult dilemmas for small satellite designers when prioritizing resources onboard a confined small satellite bus with competing demands. Still, engineers should not overlook the potential total loss of mission due to a cyber-attack.'*

Encryption is a computationally intensive process that offers security and is commonplace in terrestrial networks. However, encryption becomes more challenging as satellites get smaller. A recent presentation showcased risks due to weak encryption in the CubeSat Space Protocol, affecting command validation and acceptance.[15] For resource-limited small satellites, lightweight encryption and hashing algorithms like ASCON may be more suitable. Established in 2023 as the National Institute of Standards and Technology's standard for lightweight cryptography, ASCON is likely a more secure family of algorithms.[16]

There are difficult dilemmas for small satellite designers when prioritizing resources onboard a confined small satellite bus with competing demands. Still, engineers should not overlook the potential total loss of mission due to a cyber-attack. As small satellites in LEO begin to leverage automation to relay commands to one another, any chink in the link segment's armour can lead to spiralling effects. These vulnerabilities underscore the risk of bolting COTS products together without cybersecurity as a central design requirement.

The Space Segment

Lastly, the space segment is the orbital component of the space architecture. As satellite development becomes cheaper and faster, small satellites' use of COTS products and open-source software has effectively made them IoT devices in orbit. Because smaller space operators do not have the resources to institute their own proprietary methods for C2 and data handling, some are leveraging common operating systems and programming languages onboard their satellites (e.g. Linux, Java, and C/C++). This convenience comes with risk because malicious cyber actors are also very familiar with these languages.

If a compromised ground segment sends malicious commands, the satellite may rely on its inherent trust relationship and execute the commands, assuming they are authenticated if properly formatted. Therefore, some experts have called for spacecraft designers to follow suit with terrestrial networks and institute zero trust bases within and between the four segments of space, even onboard the spacecraft themselves. One way to do this is by having intrusion detection software to detect and flag anomalous commands or malicious behaviours.[17] To glean which malicious behaviours may threaten one's space networks, the Space Information and Sharing Analysis Center is an organization that collaborates on space network vulnerabilities and associated adversarial TTPs. Similarly, the United States Cyber Command's 'Under Advisement' program has shown precedents for how government agencies can share cyber threat reporting at adequate classification levels with industry.

Additionally, if these small satellites continue to use COTS components and open-source software from communal repositories, cybersecurity professionals should be aware of their origins. Supply chain interdiction remains a robust avenue for malicious cyber actors to gain unauthorized access. The US Defense Intelligence Agency has reported that one unit in the Chinese People's Liberation Army has even carried out cyber espionage specifically against European and American space supply chains since at least 2007 in an effort to jump ahead of competition.[18] Furthermore, penetration testers recently demonstrated the

© EUTELSAT

Many terrestrial networks rely on interconnected system of satellites with automated connections to efficiently transmit data, products, and services.

impacts of supply chain injection when they installed malware to carry out a cyber-attack on a live, European Space Agency OPTSAT in orbit. The testers showcased several critical stages of an attack, including privilege escalation, persistent access, and lateral movement from the satellite's bus to the remote sensing payload. They manipulated the images taken by the nanosatellite's camera before being downlinked back to Earth. Although not demonstrated, they claim to have also been able to drain the satellite's batteries, tamper with its GPS coordinates, and shut down services.[19] In an operational environment, what would happen if an adversary replayed outdated imagery to mask ground activity?

Finally, even if cybersecurity is designed into systems before launch, the job is not over. Starlink has 'resisted all hacking and jamming attempts' partly because of its bounty program, which pays anybody who can find and report vulnerabilities, enabling swift patching.[20] This proactive mentality is similarly seen at the US Space Force's annual Hack-a-Sat, and a recent effort to create a virtualized test range to assess an Estonian CubeSat's cybersecurity posture.[21]

Conclusion

Although it may appear daunting, it is important to note that all these new space capabilities can be secure if the space community does not procrastinate or neglect the proper cybersecurity steps. Securing the four segments does not necessarily require novel cybersecurity techniques, but rather by enforcing high standards already in place for our most sensitive military networks. Pending established cybersecurity standards for space, mission owners can apply existing standards used by lightweight cryptography, IoT, and national security networks. As new space rapidly employs shared software, COTS products, small satellites, GSaaS, and other future developments, space mission owners need to prioritize cybersecurity with greater urgency throughout all the space segments. Failure to do so could compromise NATO operations.

Implementing proactive measures such as continuous vulnerability assessments, penetration testing, zero trust, and fostering collaboration between government and private sectors will greatly reduce risk so that new space innovations remain resilient against evolving cyber threats. ●

[1] 'Miniature Satellites with Massive Benefits', NASA Space Station Integration Office, July 2022. https://www.nasa.gov/missions/station/miniature-satellites-with-massive-benefits/ (accessed 17 June 2024).

[2] Swan, McKayla, 'Anti-satellite Tests: A Risk to the Security and Sustainability of Outer Space', Liberty University Journal of Statesmanship & Public Policy Vol. 3 Iss. 1, Article 4 p. 6 (2022). https://digitalcommons.liberty.edu/jspp/vol3/iss1/4 (accessed 17 June 2024).

[3] Erwin, Sandra, 'DoD space agency: Cyber attacks, not missiles, are the most worrisome threat to satellites', Space News, April 2021. https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites/ (accessed 17 June 2024).

[4] Kaczmarek, Sylvester, 'Cybersecurity for Space Assets: Focusing on SmallSats and CubeSats', Sylvester Kaczmarek. https://sylvesterkaczmarek.com/blog/cybersecurity-for-space-assets-focusing-on-smallsats-and-cubesats (accessed 17 June 2024).

[5] 'Industrial Control Systems Vulnerabilities Soar: Over One-Third Unpatched in 2023', The Hacker News, August 2023. https://thehackernews.com/2023/08/industrial-control-systems.html (accessed 17 June 2024).

[6] Siddiqui, Zeba and Bing, Christopher, 'Chinese hackers spying on US critical infrastructure, Western intelligence says', Reuters, May 2023. https://www.reuters.com/technology/microsoft-says-china-backed-hacker-targeted-critical-us-infrastructure-2023-05-24/ (accessed 17 June 2024).

[7] Torkington, Simon, 'These 6 countries are using space technology to build their digital capabilities. Here's how', World Economic Forum, April 2024. https://www.reuters.com/technology/microsoft-says-china-backed-hacker-targeted-critical-us-infrastructure-2023-05-24/ (accessed 17 June 2024).

[8] 'NATO Space Handbook', 2021.

[9] Page, Carly, ViaSat Cyberattack Blamed on Russian Wiper Malware', Tech Crunch, March 2022. https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/?guccounter=1 (accessed 17 June 2024).

[10] Evan Meyrick, Aaron Pickard, Tobias Rahloff et al, 'Ground Station as a Service: A Space Cybersecurity Analysis', 72nd International Astronautical Congress, October 2021. https://www.researchgate.net/publication/356378842 (accessed 17 June 2024).

[11] Panetta, Kasey, 'Is the Cloud Secure?', Gartner, October 2019. https://www.gartner.com/smarterwithgartner/is-the-cloud-secure (accessed 17 June 2024).

[12] '2023 Global Threat Report', Crowdstrike, 2023. https://www.crowdstrike.com/resources/reports/global-threat-report-executive-summary-2023/ (accessed 20 August 2023).

[13] B. Lin, W. Henry, R. Dill, 'Defending Small Satellites from Malicious Cybersecurity Threats', 17th International Conference on Cyber Warfare and Security, March 2022. https://papers.academic-conferences.org/index.php/iccws/article/view/60 (accessed 18 June 2024).

[14] S. D. Hitefield, M. Fowler, T. Charles Clancy, 'Exploiting Buffer Overflow Vulnerabilities in Software Defined Radios', IEEE, 2018. https://ieeexplore.ieee.org/abstract/document/8726592/ (accessed 18 June 2024).

[15] M. Manulis, 'Security challenges for satellite constellations and communications', [online video], 2021, https://www.youtube.com/watch?v=caz8-LeBs9Q&t=629s (accessed 18 June 2024).

[16] F. Schiffer and T. Rosteck, 'Improved security for the IoT: NIST selects Ascon as international standard for lightweight cryptography', Infineon, February 2023. https://www.infineon.com/cms/en/about-infineon/press/market-news/2023/INFCSS202302-064.html (accessed 18 June 2024).

[17] D. Werner, 'Small Satellites, Big Weakness', Aerospace America, September 2019. https://aerospaceamerica.aiaa.org/features/small-satellites-big-weakness/ (accessed 18 June 2024).

[18] '2022 Challenges to Security in Space', Defense Intelligence Agency, March 2022. https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf (accessed 18 June 2024).

[19] B. Bailey and B. Roeher, 'Hacking an On-Orbit Satellite: An Analysis of the CYSAT 2023 Demo', Medium, May 2023. https://medium.com/the-aerospace-corporation/hacking-an-on-orbit-satellite-an-analysis-of-the-cysat-2023-demo-ae241e5b8ee5 (accessed 18 June 2024).

[20] M. Kan, 'SpaceX Invites Security Researchers to Hack Starlink', PCMag, August 2022. https://www.pcmag.com/news/spacex-invites-security-researchers-to-hack-starlink (accessed 18 June 2024).

[21] 'University of Tartu and CybExer Technologies plan to connect ESTCube-2 satellite into a unique cyber security system', Cybexer Technologies, March 2022. https://cybexer.com/news/estcube-2-satellite-into-a-unique-cyber-security-system/ (accessed 18 June 2024).

ABOUT THE AUTHOR

Captain Luke Stensberg

US Space Force, JAPCC

Captain Stensberg is a subject matter expert in space and cyber integration, leading the way in the JAPCC's C5ISR & Space branch to enhance the Alliance's comprehension of these critical domains. Before this role, he served in a Space Force talent management function, and prior to that, as a Cyberspace Operations Planner at the 16th Air Force's Headquarters. There, he aligned strategies with US Cyber Command and, notably, the newly stood-up US Space Command. Other previous assignments include Flight Commander of Tactical Communications for the 485th Intelligence Squadron, managing C4ISR capabilities for 29 nations and over 900 intelligence analysts. He also provided Integrated Project Management support to the 694th ISR Group in Osan, Republic of Korea. Captain Stensberg was commissioned as a Cyberspace Operations Officer in 2016 from the United States Air Force Academy.