GCSP
Geneva Centre for
Security Policy

JANUARY 2024 | ISSUE 35

Strategic Security Analysis

Critical International Infrastructure: A Case for Secure, Sustainable Non-terrestrial Networking

Sandra Scott-Hayward

www.gcsp.ch

The Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security and peace. The foundation is supported by the Swiss government and governed by 54 member states. The GCSP provides a unique 360° approach to learn about and solve global challenges. The foundation's mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions to build a more peaceful future.

Strategic Security Analyses

The GCSP Strategic Security Analyses series publishes short papers that address a current security issue. These papers provide background information about the theme, identify the main issues and challenges, and propose policy recommendations.

This series is edited by Dr. Jean-Marc Rickli, Head of Global and Emerging Risks.

About the author

Dr Sandra Scott-Hayward is a GCSP Polymath Fellow and a Senior Lecturer (Associate Professor) with the School of Electronics, Electrical Engineering and Computer Science, and a Member of the Centre for Secure Information Technologies at Queen's University Belfast (QUB). She is also the Director of the QUB Academic Centre of Excellence in Cyber Security Education.

About this publication

This publication is part of a special series of papers under the **Polymath Initiative** supported by the Didier and Martine Primat Foundation. For more information, please visit the Polymath Initiative website: https://www.gcsp.ch/the-polymath-initiative.

ISBN: 978-2-88947-321-2

The views, information and opinions expressed in this publication are the author's own and do not necessarily reflect those of the GCSP or the members of its Foundation Council. The GCSP is not responsible for the accuracy of the information.

Cover photo: NicoElNino, Shutterstock.com

Key points

- It is anticipated that by 2030, low-latency (low Earth orbit satellite-based) Internet will be carrying many terabits per second, eclipsing traditional geostationary communications. Rather than replacing the well-connected, fibre-to-the-home infrastructure available in urban environments, satellite communication will target mobile, rural, and rapid start-up communication.
- To facilitate the global Internet, the growth of “disposable” space infrastructure and the vast volume of space debris is somewhat at odds with the terrestrial UN Sustainable Development Goals.
- In recent years, Space has been recognised as a “critical national infrastructure” sector, with the designation of satellite constellations as critical space infrastructure.
- Compared with the maturity of government and military space standards, the process of ensuring the security of commercial satellite operations is in its infancy.
- Machine learning and artificial intelligence (AI) techniques are fundamental to the successful deployment of satellite mega-constellations, commercial satellite operations and space-air-ground integrated networks. The security of their implementation is paramount.
- The UN High-Level Advisory Body on Artificial Intelligence should include this critical international infrastructure in its recommendations for the international governance of AI.

Introduction

Space-air-ground integrated networks (SAGINs) or space-air-ground sea integrated networks extend terrestrial network infrastructure to non-terrestrial networks (NTNs), integrating satellite and unmanned aerial vehicle (UAV) communications, high-altitude platforms, and space systems. These integrated networks can provide connectivity to remote locations, enhance service delivery, and support new ventures. NTN integration is an ambitious mission in 3GPP[1] to extend the Internet to sky and outer space.

While there is a benefit to using machine learning (ML) and artificial intelligence (AI) to manage the analysis of massive volumes of space and terrestrial network data and to provide intelligent systems management in space missions and terrestrial network services, the extension of terrestrial networking to integrate space systems merits analysis in terms of security and the use of AI. ML and AI solutions are being explored to advance cooperative and autonomous behaviour, self-organisation, and optimisation in SAGINs.

Specifically, there are questions around the impact of interactive systems in space e.g. AI-driven satellite-UAV cooperation, and security considerations vis-à-vis the dynamic and programmable environment. There is also the question of the global nature of space, e.g. how the various authorities that own the various elements of SAGINs such as satellites, UAVs, ground stations, etc. are able to cooperate/collaborate. Other issues include ways to regulate or account for the lack of regulation of systems in space, and the questions of sustainability and the impact of the expansion of terrestrial systems into space.

Other issues include ways to regulate or account for the lack of regulation of systems in space, and the questions of sustainability and the impact of the expansion of terrestrial systems into space.

This Strategic Security Analysis paper begins with this latter question, in light of the sheer volume of satellites in orbit today and the almost daily increase in space hardware. Beyond the potential for collisions and the question of the physical safety of satellite systems, their deployment as low Earth orbit (LEO) mega-constellations raises the issue of ensuring their cyber security. Furthermore, mega-constellations produce mega data that demands ML-based analytics, leading to the need to overcome the security challenges that come with the application of ML and AI.

Hard-hitting hardware

There is a long history of communications and navigation systems operating from space, e.g. military communications satellites, and position, navigation, and timing (PNT) services through global navigation satellite systems (GNSS) such as the US Global Positioning System (better-known as GPS), and Europe's Galileo operating in geostationary orbit (GEO).[2] More recently, private companies and government agencies alike have been planning and implementing LEO[3] constellations, with each numbering hundreds or thousands of satellites. In the UK, a new framework for greater PNT services to underpin critical national infrastructure (CNI) was published in October 2023,[4] with the *Space-based PNT Technical Concepts* report[5] detailing varying LEO, MEO[6] and GEO approaches. Similarly, in the United States, the Department of Defense's Space Development Agency is deploying satellite constellations in a range of orbits.[7] Beyond PNT services, LEO broadband constellations aim to bring low-cost, high-speed connectivity to remote rural regions.

The sheer volume of satellites in orbit is increasing daily. SpaceX's Starlink[8] network, which uses satellites to beam a broadband signal down to Earth, already has about 5,000 satellites in space, with plans for 42,000 in total. The Eutelsat OneWeb[9] broadband satellite mega-constellation is at a smaller scale with 618 satellites in LEO, and Telesat Canada has a global network of 198 LEO satellites.[10] In September 2023, Amazon launched its first two prototype satellites into space. This is part of its Project Kuiper,[11] which aims to bring fast and affordable broadband services to all corners of the globe. Given the vast reach of Amazon services coverage on the ground, we can anticipate a rapid expansion in space. Indeed, in total Amazon plans to build and deploy 3,236 satellites over the next six years.

What were once individual, high-value items (GEO satellites) launched infrequently are now sent into space in increasing volumes at an accelerating pace.

The global Internet plan, which is presented as a well-intentioned initiative to provide services to unserved or underserved communities "to bridge the digital divide" (the gap between those communities that have reliable, affordable Internet access and those that do not)[12] is admirable. However, how responsible is the approach taken to achieve this? Take the question of sustainability, for example. What were once individual, high-value items (GEO satellites) launched infrequently are now sent into space in increasing volumes at an accelerating pace. Given how poorly we perform at producing sustainable and environmentally friendly products for deployment on Earth (even with the increasing introduction of regulatory systems to manage such processes), it seems unlikely that we should expect sustainable practices in space. Once deployed, a large proportion of the satellites and high-altitude platforms may be forgotten.

Taking Amazon's plans as an example, as a commitment to space safety, Amazon reports that it will actively de-orbit[13] the two Project Kuiper satellites before they ultimately burn up in the Earth's atmosphere. But what is the plan for the other 3,234 satellites? The European Space Agency (ESA) also demonstrated a successful de-orbiting of the wind-monitoring Aeolus satellite in July 2023.[14] This was a first-of-its-kind manoeuvre: when it was given commands by mission control, the satellite re-entered the atmosphere over Antarctica, with any debris falling into the ocean.

While there is some activity to address space sustainability, it seems in direct contention to the fast-growing attritable, low-cost swarming UAV market. Unmanned aerial systems (UASs) are a key component of SAGINs. They are located between terrestrial (ground) networks and satellites (in space), offering communications coverage and mobility from high altitude with greater accessibility than space network elements. The QinetiQ Jackdaw is one example of a "disposable" UAS designed with an endurance of three hours for intelligence, surveillance, and reconnaissance; decoy;

and electronic warfare missions.[15] The vulnerability of UAV swarms will be discussed later in the paper.

From a security perspective, the increasing volume of satellites in space is a concern. According to Jean-Marc Nasr, EVP Airbus Defence & Space, in LEO "every 8mins there is a 'red alert'" warning of "a potential collision".[16] To address this, in June 2023 the ESA announced its Zero Debris Charter, which is an initiative to encourage responsible companies to promise to de-orbit their satellites at the end of their lives and cut down on space junk.

Beyond the issue of collisions in space, cooperation and competition pose security concerns. In space, satellites share an ecosystem with no national and few natural boundaries. Who takes responsibility? And is global space regulation feasible, practical, or enforceable?

> One of the goals of 6G is to enable large-scale LEO satellite constellations to form different moving networks that can be integrated with the Internet.

Remote, programmable, ML-based critical national infrastructure – a global vulnerability?

It is anticipated that, by 2030, low-latency (LEO satellite-based) Internet will be carrying many terabits per second, eclipsing traditional geostationary communications. One of the goals of 6G is to enable large-scale LEO satellite constellations to form different moving networks that can be integrated with the Internet. For example, combining a LEO mesh-based network with GEO military communications satellites could provide highly resilient and superfast connectivity that boosts the operability of CNI. With this approach, messages can be optimally routed through the network to offer speed and security, with space becoming a multi-node Internet rather than the traditional two-way uplink/downlink of ground to satellite communications to send or receive data/messages.

Delay-tolerant networking (DTN) is the answer to outer space's long latencies and intermittent connections. NASA has developed a suite of communication protocols for DTN to support an interoperable space network. The Bundle Protocol (BP) is one of these, with a security protocol known as BPSec providing data authentication, integrity and confidentiality services for the BP. The programmability of software-defined networking is being explored to support the implementation of DTN protocols. New networking and communications paradigms are required to support sparse population and/or low power and/or astronomically distanced network nodes.

In October 2023, Eutelsat OneWeb in the UK successfully connected its LEO satellite constellation to a 5G mobile network[17] in a clear step towards the 6G/NTN goal.

Vulnerability to cyber attack

The space segment of non-terrestrial networks includes LEO constellations. In an example of their vulnerability to cyber attack, following Russia's invasion of Ukraine in 2022, Viasat satellite ground receivers across Europe were compromised by Russian hackers. It is reported that a vulnerable network device allowed the attacker to gain access to a highly trusted part of the Viasat network, from where the attacker sent commands to end-user modems, taking them offline.[18] Starlink satellites providing emergency wireless coverage in the Ukraine also suffered from signal jamming[19] attacks to disrupt their communications.

The vulnerability of GNSS to both interference, signal jamming and other cyber security threats is recognised. Given how reliant we are today on PNT services, recommendations for the application of a cyber security framework to protect these services have been developed, e.g. the *Foundational PNT Profile* of the US National Institute of Standards and Technology (NIST).[20]

Different to PNT satellites and regardless of their altitude or size, communications satellites transmit more power, and therefore more power is needed to jam them. However, based on their orbit, LEO satellites require frequent handovers that introduce delays and expand the threat surface for interference.

As described earlier in this paper, satellites are becoming smaller and purpose-specific, leading to a similar situation to the one we have seen with Internet of Things devices, i.e. smaller form factors; affordable; and fewer memory, computation, and processing resources. The lower compute power limits encryption capabilities and security protection measures such as jamming or interference detection/protection.

Operators of terrestrial telecommunications networks have been hesitant to introduce programmable components due to the lack of an assured network state. How much more challenging might this be across NTNs?

Programmability poses a similar challenge. Software-defined radio and software-defined networks offer great flexibility in their functionality. However, remote connectivity is an attack surface that requires security. For example, the Airbus Telecommunications new reprogrammable Eurostar Neo satellite can be reprogrammed throughout its life because of its electric propulsion that supports a larger payload and a digital processor. Operators of terrestrial telecommunications networks have been hesitant to introduce programmable components due to the lack of an assured network state. How much more challenging might this be across NTNs?

Some interesting proposals have been made for the protection of high-value assets such as military-grade communications satellites to allow them to provide robust and secure communications, e.g. equipping them with sensors, cameras, or radar warning receivers to detect rogue satellites attempting to close with and damage/destroy them, or deploying bodyguard satellites to protect a high-value military satellite by blocking the approach of an unfriendly satellite.

With the expansion of the space sector, distributed, independently owned and operated satellite system components are being integrated to provide shared services. This aggregation is termed a hybrid satellite network (HSN), the components of which may have varying levels of trust such that cyber security considerations of confidentiality, integrity and availability require critical consideration. While standards are rapidly emerging for the security of HSNs,[21] it is highly unlikely that commercial satellites can or will match the security measures of mature terrestrial communications networks and military-grade satellites.

ML-based SAGINs and communications

The application of ML techniques is as popular in SAGINs as elsewhere. For example, ML/AI techniques can be applied to mitigate interference and enable satellite systems to co-exist with terrestrial systems, such as in the OneWeb demonstration described above. ML/AI methods are used for radio resource optimisation,[22] satellite communication network operations optimisation, and the management of LEO mega-constellations.

When adopting ML/AI for these systems and in light of the designation of satellite constellations as critical space infrastructure, the security of the ML/AI is essential. A poisoning attack (an adversary corrupting the ML system’s training data) or an evasion attack (an adversary manipulating input data to cause misclassification) could have both physical and cyber security consequences. For example, consider satellite routing based on decisions from an ML-based algorithm taking inputs from weather conditions (i.e. when link reliability is based on weather conditions). An attacker capable of manipulating the input can influence the routing algorithm and control the path of traffic through the network, potentially re-routing information to a malicious endpoint.

While ML/AI techniques in SAGINs are still in the research phase, UAV swarms are at a more advanced stage of development and deployment, and thus offer a good example of ML/AI vulnerabilities in this collaborative networking environment.

The case of the security of UAV swarms

As with any software system, in the UAV swarm scenario there may be logic errors/bugs in the swarm algorithms that adversaries can exploit. Analysing the attack surface of the distributed system will present potential threats to any element (UAV/network node) in the system and every connection/communication between system elements, e.g. the presence of a single rogue agent or multiple rogue agents, connectivity and communication interception, false signalling, etc. The number of inputs to support the operation of the UAV swarm is significant.

A rogue UAV might observe the movement and communication between the UAVs and introduce a signal very similar to those of the legitimate UAVs, but that alters the behaviour of the swarm.

Communication between the UAVs in the swarm and their movement is based on a process of action and reaction, which is collective intelligence based on decentralised behaviour. What this means is that each individual UAV is doing its own thing, but in relation to the other UAVs in the swarm by reading signals from them. If in the design phase for this system an attacker poisons or corrupts the data used in the ML/AI model development, then unexpected behaviour is potentially possible among the UAVs in the swarm. Of course, if appropriately secured, there may be a low likelihood of an attacker being able to access the data/design. However, an evasion attack is also possible in the UAV swarm. A rogue UAV might observe the movement and communication between the UAVs and introduce a signal very similar to those of the legitimate UAVs, but that alters the behaviour of the swarm. The challenge here is that the autonomy of the UAV swarm is designed for self-organisation, so that, once deployed, the UAVs coordinate with one another and make decisions without human controller intervention, while there may also be limited oversight of the swarm's behaviour.

One of the main ways to protect the signalling, task and target data in the swarm is encryption. There are designs for (and some demonstrations of) quantum safe communication channels to secure UAS data transmissions. This is an important direction of research and development.

One of the major concerns regarding the use of ML/AI in SAGINs is that, in contrast to the traditional government/defence funding of space and aerial technologies,[23] ML/AI is being adopted from private big tech companies without security being considered. Given their designation as critical infrastructure, a high level of robustness and resilience should be demanded of SAGINs.

Space applications and service providers – use and misuse

The use cases of navigation and timing, communications, observation and reconnaissance, and the protection of satellites are motivating both governments and private organisations. As previously described, commercial satellite operations are rapidly expanding. This expansion extends from the infrastructure to the potential applications and services delivered by that infrastructure.

With the advent of the terrestrial Internet, information became more freely available and accessible, offering opportunities for innovative services and products, both for good and nefarious activities. With the advance towards a global Internet, new opportunities for innovation are becoming available with the wealth of data becoming available.

Examples of space data include Earth observation data such as the Copernicus Climate Change Service (C3S)[24] implemented by the European Centre for Medium-Range Weather Forecasts, which provides data for climate monitoring and decision-making, very high temporal resolution imaging (e.g. Planet Labs[25]), video from space (e.g. the UK's Sen Corporation[26]), maritime and aviation traffic monitoring, supply chain and animal tracking, and deforestation detection.[27]

The Sentinel Data Access Service[28] is an online portal designed to help organisations to search and download data available from public and private satellite operators. The Data Discovery Hub[29] lists both open and licensed Earth observation and geospatial datasets, as well as Climate, Environment and Monitoring from Space (CEMS), which offers space-based climate change and Earth observation data and services.[30] Earth-i specialises in providing geospatial information based on multi-operator, multi-resolution, multi-sensor Earth observation data, including satellite images.[31] International space-based data and analytic nano-satellite operator Spire collects space-based Earth observation data through a constellation of over 165 satellites.[32]

Some examples of companies using space data include Paddle Logger,[33] which offers a water enthusiast tracking service; PlanetWatchers,[34] which uses space-based data to track and assess storm damage; and Orbital Witness,[35] which deploys data from satellites in real estate legal cases.

Some of the potential cyber security threats to these businesses include the intentional jamming and spoofing of sensor data, the interception and theft of sensor data, the intentional corruption of sensor systems, and denial-of-service attacks on the sensor system. The impact ranges from unreliable to unavailable data undermining the offered service.

The ongoing war in Ukraine provides an example of the potential impact of this.[36] Various commercial satellite imagery companies have provided real-time, high-resolution images during the war in the Ukraine.[37] These images are then analysed using ML/AI techniques to identify relevant structures, defences, and fortifications, providing insight into the current situation in the country and potential planned attacks and defences. From the security perspective, there are multiple considerations: (1) the availability of such images relies on the secure operation of and trust in the NTN to deliver them to the ground station[38]/end user; (2) the integrity of the images must be assured, i.e. that they have not been tampered with to present false information; and (3) the ML/AI applied to analyse the imagery must be secured. The December 2022 NIST Interagency Report on applying the cyber security framework to satellite command and control[39] and the July 2023 NIST Interagency Report on cyber security for commercial satellite operations[40] are steps towards introducing cyber security risk management to this industry. In the former report, ML is referenced as a technology to support threat detection/response capabilities, but it is not mentioned in the latter one.

These images are then analysed using ML/AI techniques to identify relevant structures, defences, and fortifications, providing insight into the current situation in the country and potential planned attacks and defences.

Secure, sustainable Space use: target or aspiration?

Despite the challenges and threats, there are some positive indicators that there is a move towards a more secure and sustainable use of space.

In June 2023 a new initiative known as Astra Carta[41] was launched at the Space Sustainability Summit in the UK. Astra Carta seeks to harness and unite the private sector in creating sustainable practices for the space sector by treating LEO as a natural resource that is being polluted by space debris, similar to the pollution of the world's oceans. This follows the 2022 UK Plan for Space Sustainability with the goal of developing responsible space standards and regulatory frameworks, incentivising sustainable space firms and boosting active space debris removal.[42] Although a range of global organisations support this initiative, there is scope for further international cooperation. For example, in a 2019 study of legal regulation in the use and development of AI for space,[43] the authors conclude that an international treaty should be adopted to cover the creation of an international law enforcement agency monitoring AI use in space technologies.

Regarding the very high number of satellites in space, from the perspective of the lower value of each satellite (because they are relatively easily and affordably replaceable), the sheer numbers of satellites lowers the value of possible compromise for any individual satellite. Secondly, the satellite system can be operated cooperatively, with decisions being taken by multiple satellites rather than individually. As such, an attacker would have to eliminate all the satellites involved in a decision (and know which ones are involved) in order to compromise that particular function or communication path.

Regarding signal jamming, various strategies can be used to protect against jamming such as frequency hopping or spread-spectrum modulation, both of which are methods to dynamically change the signal so that it is more difficult for an attacker to target. Recent research is exploring ML-based detection and protection techniques (but, of course, a potential adversary is also exploring the application of ML to jamming techniques). "Smart jamming" is an example of this in which an independent transmitter can jam target radio frequency ML-based classifiers by transmitting adversarial perturbations and substantially reduce the classification accuracy.

Recent research is exploring ML-based detection and protection techniques (but, of course, a potential adversary is also exploring the application of ML to jamming techniques).

Having highlighted the challenges of adversarial attacks on ML/AI, it must be noted that these are not unique to SAGINs. It will be possible to apply the robust AI solutions being researched and developed to enable the required protections against these threats.

Conclusion

AI for Good,[44] space sustainability and closing the digital divide are all areas of focus of the International Telecommunication Union. However, they are largely addressed in isolation. In terms of the global Internet, not only must these initiatives be addressed at the international level, but they must also be considered conjunctively.

In October 2023 the UN Secretary-General launched the UN High-Level Advisory Body on Artificial Intelligence.[45] This group of experts is tasked with supporting UN efforts to ensure that AI is used for the greater good of humankind. In his announcement, the Secretary-General specifically highlighted the transformative potential of AI to achieve the UN Sustainable Development Goals, as well as the issues of misinformation, disinformation and surveillance (among others), each of which is pertinent to the discussion in this paper. This Advisory Body should not only be the starting point for a global conversation on the governance of AI, but should also investigate and highlight critical international infrastructure in its recommendations for the international governance of AI.

> In terms of the global Internet, not only must these initiatives be addressed at the international level, but they must also be considered conjunctively.

Endnotes

[1] The 3rd Generation Partnership Project (3GPP) unites seven telecommunications standard development organisations; see 3GPP, "About 3GPP", 2023, https://www.3gpp.org/about-us.

[2] An orbit is the curved path that an object in space takes around another object due to gravity. GEO is used by telecommunications and weather-monitoring satellites. Their orbit makes them appear to be 'stationary' over a fixed position, and their distance from Earth (35,786 kilometres) provides wide coverage.

[3] LEO is relatively close to the Earth's surface, ranging from 100 to 2,000 kilometres. LEO is used for satellite imaging supplying high resolution images. In contrast to GEO, LEO satellites move rapidly across the sky, so communications satellites in LEO generally operate as a constellation to provide the necessary coverage.

[4] UK DSIT (Department for Science, Innovation and Technology), "Critical Services to Be Better Protected from Satellite Data Disruptions through New Position, Navigation and Timing Framework", October 2023, https://www.gov.uk/government/news/critical-services-to-be-better-protected-from-satellite-data-disruptions-through-new-position-navigation-and-timing-framework.

[5] UK Space Agency, *Space-based PNT Technical Concepts*, 18 October 2023, https://www.gov.uk/government/publications/space-based-pnt-technical-concepts/space-based-pnt-technical-concepts.

[6] Medium Earth orbit (MEO) is approximately 5,000 to 10,000 kilometres above the Earth's surface and is commonly used by navigation satellites.

[7] US Space Development Agency, "The Space Force Is Launching Its Own Swarm of Tiny Satellites", August 2023, https://www.sda.mil/the-space-force-is-launching-its-own-swarm-of-tiny-satellites/.

[8] Starlink, "High-speed Internet", 2023, https://www.starlink.com/.

[9] Eutelsat OneWeb, "About Us", https://oneweb.net/about-us.

[10] Telesat, "Telesat Lightspeed™", https://www.telesat.com/leo-satellites/.

[11] Amazon, "Everything You Need to Know about Project Kuiper, Amazon's Satellite Broadband Network", October 2023, https://www.aboutamazon.com/news/innovation-at-amazon/what-is-amazon-project-kuiper.

[12] In 2019 close to 87% of individuals in developed countries used the Internet, compared with only 19% in least developed countries; see UN Secretary-General, *Roadmap for Digital Cooperation*, Report, June 2020, https://www.un.org/en/content/digital-cooperation-roadmap/#:~:text=This%20report%20lays%20out%20a,of%20the%20Envoy%20on%20Technology.

[13] De-orbiting is a controlled way of dealing with space debris. De-orbiting systems are designed to drag satellites to what is known as the graveyard orbit, which lies away from common operational orbits, to reduce their probability of colliding with operational satellites and creating space debris. These systems can be passive or active, referring to an integrated system to help move the satellite into a graveyard orbit or an external service/product.

[14] ESA (European Space Agency), "Aeolus: A Historic End to a Trailblazing Mission", July 2023, https://www.esa.int/Applications/Observing_the_Earth/FutureEO/Aeolus/Aeolus_a_historic_end_to_a_trailblazing_mission.

[15] QinetiQ, "Jackdaw Uncrewed Aerial System (UAS)", accessed December 2023, https://www.qinetiq.com/en/what-we-do/services-and-products/jackdaw.

[16] RAS (Royal Aeronautical Society), "ESA to Satellite Operators: 'Take Your Garbage Home'", Paris Air Show 2023 – Day Four and Summary, June 2023, https://www.aerosociety.com/news/paris-air-show-2023-day-four-and-summary/.

[17] University of Surrey, "LEO Satellite Constellation Connects to 5G, Paving the Way for High-speed Internet Access to Remote Mobile Phone Users", October 2023, https://www.surrey.ac.uk/news/leo-satellite-constellation-connects-5g-paving-way-high-speed-internet-access-remote-mobile-phone.

[18] Forbes, "Viasat Reveals How Russian Hackers Knocked Thousands of Ukrainians Offline", March 2022, https://www.forbes.com/sites/leemathews/2022/03/31/viasat-reveals-how-russian-hackers-knocked-thousands-of-ukrainians-offline/.

[19] Signal (radio frequency) jamming is the emission of an interference signal to prevent legitimate access to the medium or disrupt the reception of a signal.

[20] M. Bartock et al., *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services*, National Institute of Standards and Technology (NIST) IR 8323, June 2022, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8323r1.ipd.pdf.

[21] J. McCarthy et al., *Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)*, NIST IR 8441, September 2023, https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8441.pdf.

[22] N. Kato et al., "Optimizing Space-air-ground Integrated Networks by Artificial Intelligence", *IEEE Wireless Communications*, Vol.26(4), 2019, pp.140-147.

[23] For example, in the aircraft industry many advances emerged in military aircraft design. These technologies and designs were then adopted in civilian aircraft.

[24] Copernicus Climate Change Service, "Climate Intelligence", accessed December 2023, https://climate.copernicus.eu/climate-intelligence.

[25] Planet, "Daily Earth Data to See Change and Make Better Decisions", 2023, https://www.planet.com/.

[26] Sen Corp. Ltd, accessed December 2023, https://about.sen.com/.

[27] For examples such as climate monitoring and deforestation detection and the efficiencies anticipated from transport and supply chain monitoring, we might ask if the benefit to the planet is worth the environmental cost of the vast space infrastructure.

[28] Satellite Applications Catapult, "Sentinel Data Access Service (SEDAS)", 2023, https://sa.catapult.org.uk/opportunity/sentinel-data-access-service-sedas/.

[29] Satellite Applications Catapult, Data Discovery Hub, "Satellite Data, Resources, and Applications at Your Fingertips", 2018, https://data.satapps.org/.

[30] Satellite Applications Catapult, "Satellite Application Catapult – CEMS", accessed December 2023, https://www.ukspacefacilities.stfc.ac.uk/Pages/Satellite-Applications-Catapult---CEMS.aspx.

[31] Earth-i, "About us", 2023, https://earthi.space/about-us/.

[32] Spire, "We Hear You, Earth.", accessed December 2023, https://spire.com/.

[33] Paddle Logger, "Get More from Your Time on the Water", 2023, https://paddlelogger.com/.

[34] PlanetWatchers, "Tell the Story of Every Field", accessed December 2023, https://www.planetwatchers.com/.

[35] Orbital Witness, "Instant Property Insight", 2023, https://www.orbitalwitness.com/.

[36] IEEE Spectrum, "Satellite Signal Jamming Reaches New Lows: Starlink and Other LEO Constellations Face a New Set of Security Risks", May 2023, https://spectrum.ieee.org/satellite-jamming.

[37] BBC, "Space, the Unseen Frontier in the War in Ukraine", October 2022, https://www.bbc.co.uk/news/technology-63109532.

[38] A major function of ground stations is the transmission, collection, and storage of large quantities of information, including audio and video data, and images related to Internet connectivity, mobile phone transmissions, and military and civil Earth observation data.

[39] S. Lightman et al., *Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control*, NIST IR 8401, December 2022, https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.pdf.

[40] M. Scholl and T. Suloway, *Introduction to Cybersecurity for Commercial Satellite Operations*, NIST IR 8270, July 2023, https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8270.pdf

[41] SMI (Sustainable Markets Initiative), "Sustainable Markets Initiative Launches Astra Carta", June 2023, https://www.sustainable-markets.org/news/the-launch-of-the-astra-carta/.

[42] M. Botwin and E. Marion, "UK Unveils Plan for Space Sustainability: Top Points", DLA Piper, 2023, https://www.dlapiper.com/en/insights/publications/2022/06/uk-unveils-plan-for-space-sustainability-top-points.

[43] L. Soroka and K. Kurkova, "Artificial Intelligence and Space Technologies: Legal, Ethical and Technological Issues", *Advanced Space Law*, Vol.3(1), 2019, pp.131-139, https://www.researchgate.net/publication/335598465_Artificial_Intelligence_and_Space_Technologies_Legal_Ethical_and_Technological_Issues.

[44] AI for Good, "About", International Telecommunications Union, 2023, https://aiforgood.itu.int/.

[45] UN Office of the Secretary-General's Envoy on Technology, "High-Level Advisory Body on Artificial Intelligence", 2023, https://www.un.org/techenvoy/ai-advisory-body.

GCSP
Geneva Centre for
Security Policy

People make peace and security possible

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
E-mail: info@gcsp.ch
www.gcsp.ch

ISBN: 978-2-88947-321-2