CYBERDEFENSE REPORT

Terra Calling: Defending and Securing the Space Economy

From Science to Fiction and Back to Reality

Zürich, January 2021

Cyber Defense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zürich

ETH zürich

Available online at: css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Stefan Soesanto

ETH-CSS project management: Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Benjamin Scharte, Head of the Risk and Resilience Research Group; Andreas Wenger, Director of the CSS.

Editor: Jakob Bund
Layout and graphics: Miriam Dahinden-Ganzoni

DOI: 10.3929/ethz-b-000460220

Table of Contents

Executive Summary

With the growing importance of the space domain and the increasing activities in space by both nation-state actors and private sector entities, the question as to the state of cybersecurity and -defense in the space economy is a pressing one. While many other reports have been written on the topic, this study provides the reader with an elemental baseline that seeks to be both holistic and detailed, and endeavors to rectify many persisting misconceptions and outright false information that has been pervading the discussion on cybersecurity and the space economy.

Currently, there is no existing consensus on how the space economy ought to be defined. Section 1 tries to rectify that by outlining five parts that span multiple domains, multiple sectors, and multiple assets across the globe that make up the space economy.

Section 1.1 subsequently outlines the still ongoing discussions in both the US and the EU on designating the space sector as its own critical infrastructure sector. In the US, the relatively new Space Information Sharing and Analysis Center (ISAC) has been pushing the issue, while in the EU, the European Commission is currently again in the process of trying to create pan-EU critical infrastructure sector designations – after two previous unsuccessful attempts to do so in 2006 and 2013.

Section 1.2 focuses on terrestrial assets and geo-dispersion by taking a closer look at OneWeb's infrastructure as an example for commercial entanglement. The study argues that when it comes to intelligence collection, nation-state adversaries will preferably sit in any of OneWeb's data centers or hook into national satellite network portals (SNPs) rather than try to infiltrate a satellite operation center. Similarly, if satellite destruction or collision is the aim, then targeting any other company or institution whose assets are not globally entangled with multiple governments would be more desirable. In regard to the military realm, the study highlights the example of Automatic Dependent Surveillance – Broadcast (ADS-B). Concluding that, while the system can be jammed and spoofed, the risk of exploitation can be minimized to such an extent that its vulnerabilities become almost irrelevant. The study thus notes the need for both military and civilian operators to manage and explain varying risks to a public flooded with breaking news stories and heightened cybersecurity concerns.

On the subject of supply chains, the study notes that supply chain fragmentation is the norm in the space economy, as specialized manufacturers and alternative suppliers are few and far between. However, while there have been examples of APT intrusions into supplier, contractor, and major aeronautic company networks, most – if not all of them – are espionage related. The study also explains that adversarial nation states most likely face the same, if not more extensive supply chain risks – as the Iranians learned first-hand through the deployment of Stuxnet. One can only speculate to what degree adversarial space industry supply chains have been targeted in the past, and are compromised today, to for example enable pinpoint sabotage or facilitate continuous intelligence collection efforts.

Section 1.3 focuses on space-based assets. It notes that particularly military satellite systems owned by Western nations are not always single-use or single-owned – and can pivot if necessary, to commercial satellite services to bridge short-term redundancy gaps. Adversaries who seek to disrupt or degrade specific satellite services will have a hard time to achieve persistent and tangible effects. A similar logic applies to commercial space assets given that service disruptions might create regional cascading effects that are undesirable, uncontrollable, and too public for an adversary's risk appetite.

On the subject of legacy systems, the study notes that there are different logics at play between commercial satellite operators and the military when it comes to satellite life spans. The latter prefers higher refresh rates, while the former is interested in long-term use. A potential solution to bridge this gap is to build hybrid satellite constellations that connect military and commercial satellites – which would also introduce a whole new cybersecurity dimension in space as satellite-to-satellite communications are rather rare. The study also explains the difference between operating systems on Earth and real-time operating systems used in space. This also includes the problem of patching vulnerabilities in space which is similar to the forever-day vulnerability problem in industrial control systems back on Earth. The study thus notes that the cybersecurity lessons learned in space are not very much different from the best practices on Earth.

In terms of the data colonization of space, i.e., the deployment of data centers in space, the study points out that while there are still major hurdles to their creation, a move toward mirroring Earth-based infrastructure in space is going to create synergies and overlaps that have long shielded space-based infrastructure from non-state adversaries.

Section 1.4 explains the fundamentals of up- and downlinks and highlights that there is a major difference between intercepting unencrypted communications from an Iridium constellation satellite and conducting real-time packet injections into target communications as carried out at Menwith Hill Station.

Section 2 discusses two case studies: NASA and Galileo. The NASA case study highlights that there are fundamental hurdles for cybersecurity progress that are not caused by technical problems but are induced by administrative and organizational shortcomings. Meanwhile, the Galileo case is an example of public communication failures and an opaque organizational structure that can exacerbate a severe IT problem. Both cases exemplify the difficulties of tackling cybersecurity in a highly bureaucratic and multi-stakeholder environment within the space economy.

Section 3 takes a closer look at five major cybersecurity incidents that have been widely cited and used in numerous research papers and conference talks on the topic of cybersecurity in space. The study calls out several misinterpretations, the spread of false information, and rectifies the narrative to separate reality from fiction and rumors. The section also utilizes the case of Jay Dyson and H4GiS to showcase how cybersecurity issues at work can migrate into a private setting and become deeply personal. As militaries around the globe are increasingly attracted to the idea of running information warfare campaigns to create persistent psychological effects within a population or target workforce, maintaining and caring for the mental health of network defenders will highly likely become a priority for government agencies and the private sector alike.

Section 4 explains the Hack-A-Sat challenge at DEFCON 2020 to highlight the various challenges and different knowledge necessary to both the adversary and the defender to control and command space assets. It also specifically emphasizes the efforts by the hacking community and the US government in advancing outreach and getting people involved into satellite security and securing the space economy at large.

Section 5 outlines various implication for Switzerland, including:

(1) The Swiss federal government would be well-advised to comprehensively map out current Swiss space dependencies and redundancies across the identified nine critical infrastructure sectors and 27 sub-sectors.

(2) It might also be prudent to map out potential cascading effects of what might occur if one or several satellites, ground stations, relevant webservers and/or data outside of Swiss territory becomes unavailable due to a persistent cyber incident.

(3) The federal government ought to proactively engage the European Commission and coordinate with other members of the European Space Agency (ESA) to insert itself into the EU debate on pan-European critical infrastructure.

(4) The federal government would do well to open up the debate on ESA's cybersecurity posture, threat environment, and public outreach and communication practices.

(5) It might be prudent to stand up a joint cyber task force together with various ESA member countries to proactively tackle cyber-related incidents affecting the Agency.

(6) The federal government should seek clarification from the European Commission as to whether Swiss companies and government departments can get involved in the Commission's plan to build up a European satellite communication system.

(7) The Swiss Defense Department, in cooperation with RUAG and Armasuisse, could partner up with selected European or US counterparts to pick up on the success of Hack-A-Sat and advance a series of hacking challenges pertaining to the space economy across Europe and the US.

(8) Swiss government departments and/or research institutions might want to serve as neutral arbiters that collect information and investigative reports on past cyber incidents affecting the space economy to paint a realistic picture of what actually occurred (excluding attribution claims).

(9) A comprehensive and structured revisiting of past cases by a Swiss government department will most likely spur a reflection on how past incidents have been covered by the media and have been able to proliferate throughout the information security and policy community unchallenged – leading hopefully to better journalistic practices and better research conduct.

(10) Switzerland should also keep an eye out on the legal debates that have and will increasingly occur when it comes to the interception of satellite communications by intelligence agencies, and the legal status of data transmitted and hosted in space.

Section 5.1 provides a brief horizon scan that highlights three trends:

(a) Satellite Internet broadband constellations will become an essential extension – if not even a dominating part – of cyberspace as we know it. Opening up new regulatory and legal questions in a domain populated by vendors with little cybersecurity experience.

(b) The increased hybridization of space assets will most likely lead to new adversarial targeting dynamics against space-based assets.

(c) The sheer data volume and realignment of data streams through space will open up new target and attack vectors on Earth.

Introduction

The aim of this study is to provide the reader with a deeper understanding of the fundamental cybersecurity and -defense challenges pertaining to the space economy.

Section one kicks off the main analysis by outlining the broad contours of what constitutes the space economy and takes a closer look at the problems on the terrestrial surface, space-based assets, and the area of up- and downlinks. Section two dives into two case studies. The first case disseminates the evolution of NASA's cybersecurity posture since 2003. The second case takes apart the cybersecurity incident at the European GNSS Agency (GSA) in July 2019, which crippled the global navigation satellite system (GNSS) Galileo for seven days. Section three disentangles the cyber threat landscape by examining public reporting on the most referenced satellite hacking incidents in terms of its veracity and fact-based representation. Section four unpacks the Hack-A-Sat space security challenge at DEFCON 2020, run by the US Air Force and the Defense Digital Service of the US Department of Defense (DoD). And section five outlines several recommendations for the Swiss government and provides a brief horizon scan highlighting three future trends.

Please note that this report will not discuss threat vectors that fall into the electronic warfare domain, i.e., signal spoofing and up- and downlink signal jamming. Nor will it touch upon space governance issues, all things surrounding quantum, and the broader spectra of space militarization, and anti-space weaponry (such as anti-satellite missiles, directed energy weapons, and physical orbital threats).

1 Multi-domain Multi-sectoral Multi-asset

To answer the question as to what constitutes the space economy, we have to look at a highly diverse set of stakeholders – ranging from satellite manufacturers and launching providers, to government agencies, academia, and commercial entities – whose products are delivering a host of distinct services to third parties dispersed across multiple domains and multiple industrial sectors back on Earth. Roughly, the space economy can be divided into five parts:

(1) **Space-based assets** – This category includes everything from the International Space Station (ISS) and the Hubble Telescope to the increasing number – and different types – of satellites orbiting Earth.

(2) **Earth-based control stations** – In the case of Europe's global navigation satellite system Galileo, this currently comprises numerous assets distributed across the globe. These facilities include two ground stations for satellite and mission control, six stations for telemetry, tracking and control (TT&C), ten stations for mission data uplink (ULS), and several distributed reference sensor stations (GSS).

(3) **Earth-based communication stations, terminals, and devices** – Their usage is limited to the receiving and relaying of satellite signals and information – particularly useful when connecting from remote locations. This includes SCADA systems (think remote pipeline analytics), satellite TV/phone/and Internet connections, maritime communication links, as well as bank and point-of-sale transactions (for example at gas stations).

(4) **The space industry** – stretching from all the services and entities involved in manufacturing space components to all the equipment and research necessary to facilitate asset delivery into Earth's orbits for commercial, civilian, and military purposes.

(5) The **space economy supply chain** – meaning every hard- and software supply chain for every individual product, system, chip, and line of code that is used within the space economy. This naturally includes supply chains for commercial and proprietary products, systems, chips, and code that is not purposefully build for the space economy as such.

Since the inception of the space race between the United States and the Soviet Union in 1957, Earth's orbits have become more congested, contested, competitive, and complex. Today, there are ten nations and one international organization that can independently launch cargo into space: China, France, India, Iran, Israel, Japan, Russia, North Korea, South Korea, the US, and the European Space Agency (NASIC 2019, p. 12).

The build-up of these indigenous capabilities has resulted in the creation of three regional navigation satellite constellations (India's NavIC, Japan's QZSS, and China's BeiDou for Asia), and four worldwide navigation satellite constellations (the United States' GPS, Europe's Galileo, Russia's GLONASS, and China's BeiDou worldwide).

In August 2020, there were 2,787 active satellites circling Earth, of which 51 per cent were US-owned (1,425), 13 per cent were Chinese (382), 6 per cent were Russian (172), and 29 per cent were operated by other nations (808) (UCS 2020a). Back in January 2014, there were only 1167 actively operating satellites (UCS 2020b, p. 62).

The latest figures released by the US Federal Aviation Administration (FAA) show that "in 2017, the United States, Russia, Europe, China, Japan, India, and New Zealand conducted a total of 90 orbital launches, 33 of which were commercial" (FAA 2018, p. 39). This is not a big change compared to 2012, when "78 launches carried a total of 139 payloads to orbit. Approximately 20 per cent of launches provide commercial services. The remaining 80 percent were used for non-commercial civil government, military, or non-profit purposes" (FAA 2013, p. 70). While the number of orbital launches has been hovering between a high of 143 in 1965 and a low of only 55 in 2004, the number of payloads carried into orbit has been steadily increasing since 2010 (Mazareanu 2020). Utilizing space-track.org and cross-referencing each launch with other databases and articles, we can calculate that in 2010 119 payloads were launched into orbit. In 2014, the number stood at 255, and in 2019 it increased to 468.[1]

There are three primary reasons that explain the increased payload trajectory.

One, the introduction of new light-, medium-, heavy-, and proposed super-heavy lift space launch vehicles (NASIC 2019, p. 12-13).

Two, standardized off-the-shelf nanosatellite designs (so-called CubeSats), which have an average operational life expectancy of around one year and weigh between 1-1.33 kg (1 unit) and 35-40 kg (27 units) (NASA 2017, p. 4; JAXA, n.d.). According to nanosats.eu, there were 749 active nanosats orbiting Earth in October 2020 – which roughly accounts for 25 per cent of all active satellites in orbit at the time (Nanosats 2020). According to the FAA, "organizations from nearly 60 countries have developed and built at least one orbital payload since 1957, usually a satellite. The payload building capability of more than half of these countries is limited to CubeSats, small satellites built from pre-fabricated kits by universities and government and non-profit organizations" (FAA 2018, p. 35).

And three, an ongoing commercial build-up of new satellite constellations due to faster and flexible deployments of smaller satellites at reduced costs. Amazon for example plans to launch 3236 satellites into orbit as part of its Internet-from-space Kuiper constellation (Etherington 2020b). SpaceX is busy constructing Starlink – a mega-constellation of an initial 12,000 satellites – to provide satellite Internet access to the world (Sheetz 2020). And OneWeb – despite undergoing restructuring after filing for bankruptcy in March 2020 – is continuing its build-up of a constellation of up to 48,000 satellites to compete in the global satellite Internet broadband race (Reuters 2020b).

In contrast to old satellite broadband system – such as the one maintained by Hughes since the 1990s – which relied on assets in geostationary orbit at an altitude of roughly 35,700 km, the new constellations are launched into low-Earth orbit (LEO) at an altitude of only 2,000 kilometers or less (Hughes 2014). The difference in the distance to Earth significantly reduces latency in data transfer. However, in contrast to geostationary assets that stay fixed above a specific point on Earth, low-Earth orbit satellites circle the Earth every 90 to 120 minutes (Estes 2020). To avoid a loss of broadband connection when one satellite is out of reach, companies have to create a moving mash of satellites that at any point in time provide global coverage. As a result, companies are launching thousands of satellites into LEO to create their own satellite webs. As of this writing, SpaceX has launched 835 Starlink satellites into orbit, OneWeb has launched 74 satellites, and Amazon has not yet commenced any satellite deployments (Etherington 2020c).

Note: Given the persistence of the COVID-19 pandemic and the focus on home office and resilient Internet connectivity, the build-up of satellite Internet broadband has gained renewed urgency and political attention (Estes 2020).

Innovation pressures also increased in 2004 when US President Bush initiated the termination of the very expensive and accident-prone space shuttle program by

[1] The author would like to thank the CSIS Aerospace Security Project and the Swiss Department of Defense (VBS) for opportunities to cross-reference the dataset.

2011. The move forced NASA to rethink and financially reconceptualize how it will conduct future space missions and uphold its cargo deliveries to the International Space Station (Georgiou 2020). In 2006, the agency kicked off the Commercial Orbital Transportation Services (COTS) Program in an effort to push the private sector toward developing spacecraft and rockets that can carry cargo – and people – to the ISS and beyond. In October 2012, SpaceX conducted its first operational cargo flight to the ISS under COTS (NASA 2012). In September 2013, Orbital ATK followed – now part of Northrop Grumman (Northrop Grumman 2013). And in May 2020, SpaceX completed NASA's first manned commercial spaceflight (Etherington 2020a).

1.1 Critical Infrastructure Designation

Despite this new space race, several fundamental issues remain unanswered.

For example: While the major US defense and aerospace powerhouses are already considered existing critical infrastructure (CI), as designated by the US Department of Homeland Security (DHS), the new commercial space players coming out of Silicon Valley and beyond do currently not explicitly fall into any of DHS' 16 critical infrastructure sectors. For more than a year, industry has been lobbying the Trump administration – specifically the Cybersecurity and Infrastructure Security Agency (CISA) within DHS – to create a new CI sector specifically devoted to commercial space systems. Yet, if DHS creates such a sector, it will also have to make the difficult call on deciding what is within and what is outside its bounds.

To make inroads, an industry group consisting of currently 19 members launched a Space Information Sharing and Analysis Center (ISAC) in April 2019. According to its brochure, the Space ISAC "is the only all-threats security information source for the public and private space sector" (Space ISAC, n.d.). Despite the Space ISAC's existence, the designation of a US critical infrastructure sector for the space industry is nonetheless critical, as it would legally allow companies to share information among them without violating antitrust laws and incentivize companies to openly share information with government agencies without the threat of incurring fines or penalties for regulatory infractions (Werner 2020). Similarly, a designation as critical infrastructure sector would also allow the government to adopt formal information pathways and processes, to push for the implementation of cybersecurity standards, rules, and frameworks as outlined by the US National Institute for Standards and Technology (NIST) (NIST 2018). Some analysts additionally believe that designating the space industry as critical infrastructure will deter adversaries from targeting said companies. While this might hold true in a theoretical legal and normative sense, the persistent targeting of US defense industrial base companies clearly indicates that critical infrastructure designations alone do little to shape the strategic calculus of adversaries and stave off malicious activity.

In Europe, meanwhile, the issue is even more complex. On the one hand, EU member states are free to designate their own critical infrastructure sectors and are only guided by the minimum sectoral requirements for operators of essential services, as set out in the 2016 EU Network and Information Security (NIS) Directive, and the procedures to identify and designate critical infrastructures in the transport and energy sectors as outlined in the 2008 European Critical Infrastructure Directive (European Union 2008; European Union 2016). As a result, space as its own CI sector has only been designated as such by three of the 27 EU member states (Belgium, France, and Spain), in addition to the steps taken by the Netherlands – which explicitly identifies GNSS as a subcategory in its infrastructure and water management sector. All other EU members either do not have a significant national space industry that might warrant a CI designation, or scatter different parts of their space infrastructure and related space services across different CI sectors.

The problem is compounded by the absence of any designated 'European critical infrastructures' that span across the EU. Back in 2006 and 2013, the European Commission's (EC) European Programme for Critical Infrastructure Protection (EPCIP) tried to lay the groundwork for such a formal designation, but was in the end unsuccessful. Since 2013, the EU's approach toward critical infrastructure protection has thus been rather fragmented, with initiatives popping up in the area of civil protection, energy, foreign direct investment, network information security, and transportation. For instance, in regard to GALILEO and the European Geostationary Navigation Overlay Service (EGNOS), the European Union passed responsibilities to the member states in 2013 to "take all measures to ensure the good functioning" of the two systems, and "ensure the protection of the ground stations established on their territories" (European Union 2013, Chapter VI, Art. 28).

Over the years, the Commission has come to realize that the EU's approach has become increasingly inadequate in tackling the growing sectoral interdependencies, evolving risks of cascading effects, and diverging national implementations and obligations to secure these cross-EU critical infrastructures adequately. In mid-June 2020, the Commission finally commenced another initiative to explore several policy options to better protect these systems from disruption by natural disasters and man-made threats – including cyberattacks – and to tackle the problem on the EU level rather than by the member states alone. In the initiative's 2020 Inception Impact Assessment, the

Commission explicitly identifies “space services” as the one example of critical infrastructure that provides essential services across the entire EU (EC 2020, p.3). The initiative’s feedback period was closed on 7 August 2020, and it remains to be seen if, when, and what kind of legislative proposal the Commission will create out of the feedback it received.

1.2 Terrestrial Assets

From an adversarial nation state’s point of view, the most attractive and direct attack vector are intrusions into ground stations (or footholds from where an attacker may pivot into ground stations and ground control stations over time). In the case of the US government, this would include any asset ranging from systems at NASA's Goddard Space Flight Center (Maryland) and the agency’s Mission Control Center in Houston (Texas) on the civilian-end, to the GPS master control station at Falcon Air Force Base (Colorado), the satellite ground stations at RAF Menwith Hill (Harrogate, United Kingdom), or the Joint Defense Facility at Pine Gap (Alice Springs, Australia) on the signal intelligence and military end.

While past studies on the topic of cybersecurity in space have generally pointed out the central importance of ground control stations, they have also generally ignored the wide variety of stations and their differences in both security levels (physical, network, and electronic) and connections to the outside world. Clearly, it is miles easier to phish any of the 10,000 civil servants and contractors working at NASA’s Goddard Space Flight Center or to carry a USB stick onto the premises and plug it into any of the hundreds of unobserved terminals, than it would be to pull the same stunts to gain an initial network foothold at a highly secured defense facility, such as Pine Gap or Menwith Hill.

1.2.1 **Geo-dispersion**

On the commercial side, by contrast, the attractiveness of access to ground control stations from an adversarial nation state’s point of view is not necessarily that clear-cut. Take for example OneWeb. While the company’s satellite operation centers are located in London (UK) and McLean (Virginia, USA), OneWeb is also constructing 40 to 60 satellite network portals (SNPs) across the globe to provide “support operation[s] and handoff of high-speed user traffic to and from the [low Earth orbit] satellite” (GMV 2016; OneWeb 2020; Shuman 2017, slide 14). Meaning, these SNPs will be physically located in the markets that OneWeb seeks to supply, including China, Russia, India, Kazakhstan, South Africa, and Australia (OneWeb, n.d., slide 12). Naturally, OneWeb is cooperating with local partners to smoothly enter and expand its services in those markets. In February 2019, a Russian joint venture bought a majority stake in OneWeb operations over Russia – the first step to allow the company to enter the Russian market and build portals on Russian soil. The company is also currently negotiating with the Chinese government and China Telecom to build up to three of OneWeb’s SNPs in China alone (Forrester 2019; Shuiyu 2019). In early-June, the UK government eventually purchased a 20 per cent stake (400 million GBP) in OneWeb as part of its plan to replace Galileo and rescue UK-headquartered OneWeb from bankruptcy (Lyons 2020).

What complicates matters further is that some of OneWeb’s SNPs are operated by non-host country companies or contracted out. For example, OneWeb entered into a strategic partnership with the Swedish Space Corporation (SSC) to assemble, install, and host a OneWeb SNP at the SSC’s ground station in Clewiston (Florida, USA) (White 2019). Curiously, the SSC has also helped the Chinese government to operate Chinese weather and Earth-monitoring satellites from the SSC’s ground stations in Sweden, Chile, and Australia since at least 2011. In late-September 2020, the SSC announced that it will not renew its contract with Beijing due to changes in the geopolitical situation (Reuters 2020a).

While it is perfectly possible for a nation-state adversary to gain a foothold in OneWeb’s satellite operations centers, the unanswered question is: for what purpose? If it is intelligence collection or data manipulation, then directly hooking into national SNPs or sitting in any of OneWeb’s data centers is a relatively easier task to pull off. Similarly, if satellite destruction or collision is the objective, then any other satellite, whose company is not globally entangled with multiple national governments, will do perfectly fine.

This logic however does not mean that commercial entanglement is creating a discernable deterrence effect. The opposite might actually be true. Meaning, because OneWeb is entangled globally, the incentive for advanced persistent threat actors (APTs) to penetrate and sit on OneWeb’s in-country infrastructure is almost guaranteed. From there it is only a few hops to siphon data from OneWeb’s data centers abroad, satellite up- and downlink stations, or even go through the simplest route and send an official government delegation to OneWeb’s satellite operation centers in the UK and the US to receive briefings on their cybersecurity posture - under the umbrella of safeguarding government investments and ensuring that OneWeb does not allow government backdoors or is penetrated by other APTs.

Please also note that because the number of satellite ground control stations is rather small in general, and each usually have their own security operations center (SOC) attached, they are difficult targets to breach and complex systems to persistently surveil, map, and navigate in while remaining undiscovered.

For nation-state adversaries on whose territory OneWeb does not offer any services, all bets are off. This particularly applies to North Korean APTs who could potentially develop an interest over time in OneWeb's satellites for a multitude of reasons. Motivations are difficult to grasp in the cyber domain, and any APT interests to penetrate OneWeb's infrastructure could merely mask an alternative approach to facilitate other more important campaigns.

Geo-dispersion in conjunction with military terrestrial assets has probably been most impactful in the area of drone warfare. Through a combination of military communication satellites and GPS tracking the US Air Force is able to host their pilots at Creech AFB in Nevada, while their Reaper drones loiter over Afghan airspace 7,000 miles away (Fabio 2019; Trevithick & Rogoway 2018). Geo-dispersion also plays a role in systems such as the Automatic Dependent Surveillance – Broadcast (ADS-B) – whose on-board transponders in conjunction with GPS are picked up by air traffic controllers to determine the position, speed, and identity of an aircraft.

Security concerns in ADS-B have been raised almost every year since 2006, when the system came online (Thurber 2012). Given that ADS-B signals are both unencrypted and unauthenticated, anyone can track (eavesdrop on) the steadily increasing number of ADS-B equipped aircrafts in the sky – that is literally what open-source aircraft tracking websites, such as the Swiss-based OpenSky-network, do (OpenSky, n.d.). Can ADS-B signals be jammed and spoofed? Definitely (Kujur et al. 2020). Does this mean anyone determined enough can create armies of ghost aircrafts in the sky? Yes (Costin & Fancillon 2012). So why has this not happened yet on a massive scale?

To analyze the question of security as such, we have to go back to the basics of discerning between vulnerabilities, threats, and risks. To make it simple: A vulnerability is a weakness in an asset that an adversary could exploit. A threat requires an adversary to have the motivation, resources, and intent to exploit said vulnerability. The resulting risk is the potential for the loss or damage of the asset when an adversary actively exploits the vulnerability (Bejtlich 2005).

In the case of ADS-B, there are certainly multiple vulnerabilities, but there is no directed, persistent threat over time and as a result a low risk of exploitation. There are also mitigation procedures on the air traffic controller and pilot end to verify and validate received data which makes the ghost fleet scenario rather unattractive to an adversary. Thus, even though ADS-B is unencrypted and unauthenticated, the risks can be minimized to such an extent that these vulnerabilities become almost irrelevant in day-to-day civilian operations. It is a bit different when military aircraft are concerned. Since at least 2008, DoD has expressed concern about the possibility "to identify and potentially compromise DoD aircraft conducting sensitive missions in the United States due to ADS-B Out technology" (GAO 2018, p. 1). A US Government Accountability Office (GAO) report raised the issue in January 2018 (including threats of cyberattacks), but so far the preferred DoD solution has been to allow aircraft on sensitive missions to simply turn off their ADS-B transponders (GAO 2018; Bellamy III 2019).

In the context of drone warfare, the oft-cited example of unencrypted and classified live video drone feeds throughout much of 2012-2014 is running into the same vulnerability-threat-risk misinterpretation (Shachtman & Axe 2012). Just because an unencrypted video feed can be picked up by an adversary does not necessarily translate into an actionable threat and an unmanageable risk to the drone's mission. Similarly, if traffic is encrypted, on-foot ground assets would have to carry special equipment to view the feed. Said equipment could be lost or captured by an adversary, which would then require changing the encryption keys or recovering the lost asset. Against non-state actors that are limited in their operational range and slow to mobilize (such as the Taliban) unencrypted drone video feeds present a low risk to the drone's health.[2] However, if we are dealing with a major power or peer-adversary, any vulnerability within contested airspace will most likely be immediately exploited to gain a discernable advantage on the battlefield. Thus, unencrypted video feeds will present a very high risk – if not certainty - for the drone to be detected, shot down, or captured.

Managing and explaining these varying risks in an environment of breaking news stories and heightened public attention on cybersecurity concerns is an ongoing challenge for both military and civilian operators.

1.2.2 Supply Chain Fragmentation

The global fragmentation of technology supply chains has gathered sometimes more, sometimes less attention than a persistent cybersecurity threat. Bloomberg's very questionable – if not entirely false – reporting in late-2018 on "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies" has probably spurred more public interested in hardware supply chain security than any other story since the discovery of Stuxnet in 2010 (Robertson & Riley 2018; Kaspersky 2011). On the software end, recognizable examples of supply chain

[2] Note: For domestic drone missions (i.e., unarmed surveillance missions), the vulnerability-threat-risk equation is very different.

infections are in fact more numerous, including the deployment of NotPetya in M.E. Doc's update server in 2017, and APT10 breaching multiple managed service providers (MSPs) during Operation CloudHopper to move laterally onto client networks and exfiltrate their data (Greenberg 2018; PWC & BAE Systems 2017, p. 8).

In the context of the space economy, supply chain fragmentation is the norm, as specialized manufacturers and alternative suppliers are few and far between. Take for example OneWeb's global supply chain. On the satellite end, Airbus and OneWeb created a joint venture in 2016 called OneWeb Satellites to oversee the creation of hundreds of satellites for the OneWeb constellation. OneWeb Satellites maintains two assembly lines: one factory in Toulouse (France) and one in Merritt Island (Florida, USA) (OWS, 'Our Factories'). Swiss component supplier RUAG also specifically opened a factory in Titusville (Florida, USA) to churn out satellite components for OneWeb (RUAG 2017). In fact, among OneWeb's roughly 40 global suppliers, Switzerland's RUAG Space stands out (OWS, 'About Us'). It custom-builds the satellite dispenser – which is able to deposit up to 36 OneWeb satellites into space – manufactures the satellite panels, and also produces the satellites' multi-layered thermal insulation (RUAG 2019). To deliver OneWeb's satellites into space, the company relies on the European multinational Arianespace and to some degree also on US-headquartered Virgin Orbit. Although Arianespace has its main launching hub in French Guiana, it also conducts Soyuz launches out of Kazakhstan's Baikonur spaceport. On 21 March 2020, OneWeb successfully deposited 34 of its satellites in orbit on a Soyuz launch from Baikonur (OneWeb 2020b).

Among the companies competing in the race to establish low-orbit satellite Internet constellations, OneWeb's supply chain is the most Euro-centric and Swiss-entangled. When OneWeb unsuccessfully tried to raise additional funding from its then owners – led by the Japanese conglomerate SoftBank – it had to file for bankruptcy on 27 March 2020. Consequentially, numerous European suppliers that expanded their manufacturing capabilities, tried to repurpose their investments – by approaching SpaceX or Amazon – or significantly slowed down their production output. While the large suppliers were certainly not solely dependent upon OneWeb, many smaller suppliers did not have that same flexibility. Chris Quilty, president of Quilty Analytics, noted back in April 2020 that "the big concern that we've identified is we've already got a fairly fragile supplier base here […] Many of them are single-sourced to Airbus" (Henry 2020a). The subsequent injection of liquidity by the UK government and Indian telecom operator Bharti Global on 3 July –each of which announced to put forward 500 million USD to purchase OneWeb – relaxed the supply chain concerns (Henry 2020b). OneWeb resumed its satellite deployments under a modified 16-launch contract with Arianespace. On December 18, 36 OneWeb satellites were deployed into orbit aboard a Soyuz taking off from Russia's Vostochny Cosmodrome (Foust 2020).

In terms of cybersecurity concerns in the space economy, there is actually very little open-source intelligence available to paint a worrying and complete picture. So far, nation-state actors have been primarily interested in utilizing suppliers and contractors as beach-heads to move laterally into larger defense and aeronautics companies. In 2019 for example, four Airbus suppliers – among them French technology consultancy Expleo, British engine maker Rolls-Royce, and a British subsidiary of the company Assystem – were penetrated within a few months' time by the same threat actor (CERT-EU 2019; France24 2019). According to a TLP white memo released by CERT-EU, the likely Chinese threat actors compromised the suppliers by "breach[ing] its VPN connection to Airbus, and penetrat[ing] into Airbus systems using access rights granted to suppliers" (CERT-EU 2019). Open source information is unclear as to whether the intrusions led to any data breaches or impacted Airbus operations at all (Reuters 2019).

Large defense and aeronautic companies are naturally also directly targeted by nation-state adversaries. RUAG, for example, had been compromised by Russian threat actor Turla at least as early as September 2014. On 21 January 2016, RUAG – in cooperation with Switzerland's GovCERT – opened a major incident investigation in the case. The task force subsequently recovered logs, identified C&C servers, and started to closely monitor RUAG network activities. On 4 May 2016, the press started to report on the incident, which according to GovCERT undermined the ongoing investigation and rendered the monitoring of RUAG's network useless (GovCERT.ch 2016, p.2). On 27 August 2018, the Swiss Attorney General's Office closed the criminal investigation in the case. Overall, an approximated total of 23 GBs of data was exfiltrated. Officially the "authors [of the attack] and their location remain unknown" (Swissinfo 2018). Open source reporting is unclear as to whether RUAG Space was affected in any way.

In terms of hardware manipulation in the space industry, one potential case is repeatedly referenced in other research papers. Luca del Monte, senior strategist at the European Space Agency (ESA), mentioned the incident when speaking to Reuters in 2015 at the International Astronautical Congress in Israel. According to del Monte, ESA "received microcircuits made of material whose composition, under the microscope, was found to have been tampered with at a fundamental level. Had the attack not been detected, it would have interfered with a random number generator in a way that would have helped hackers to access the satellite, with worrying repercussion" (Rabinovitch 2015). Based on Reuters reporting, it is unclear whether the manipulation was deliberate or a manufacturing mishap. As of this writing, ESA has not replied to freedom of information requests submitted by the author for document access to ESA's incident investigation in the case.[3]

Notably, in August 2018, the Pentagon's Office of the Inspector General (OIG) audited US Air Force Space Command (AFSC) on whether it had implemented an "adequate supply chain risk management program for four critical strategic system" (including the Air Force Satellite Control Network and the Global Positioning System) (DoDIG 2018, p. i). Among other items, the OIG discovered that AFSC had "not take[n] the steps and establish[ed] the controls and oversight necessary to: conduct a thorough criticality analysis and identify all critical components and associated suppliers to manage risks to the system throughout its lifecycle; [and] submit complete and accurate requests to conduct threat assessments of critical component suppliers" (DoDiG 2018, p. i). As a result, the IG concluded that "an adversary has opportunity to infiltrate the Air Force Space Command supply chain and sabotage, maliciously introduce an unwanted function, or otherwise compromise the design or integrity of the critical hardware, software, and firmware" (DoDIG 2018, p. ii).

It is important to note in this context that adversarial nation states face the same, if not more extensive supply chain risks – as the Iranians learned first-hand through the deployment of Stuxnet. One can only speculate to what degree adversarial space industry supply chains have been targeted in the past, and are compromised today, to for example enable pin-point sabotage or facilitate continuous intelligence collection efforts.

However, David Sanger's 2017 New York Times story on US Cyber Command conducting supply chain attacks against North Korea's missile program should be a vivid reminder to everyone that correlation is not causality, and that misinterpreting data leads to bad analysis. First, just because US Cyber Command maintains a program that is interested in North Korea's missile program does not mean that its operations have actually been successful in penetrating the most reclusive state on Earth. And second, just because a few of North Korea's newest missile systems have failed at a higher rate (which one would expect) does not signal the existence of a clandestine supply chain infection campaign. As arms control wonk Jeffrey Lewis from the Middlebury Institute put it bluntly: "North Korea's missile launches aren't failing because we are hacking them; they are failing because Pyongyang is developing a wide array of new liquid- and solid-fueled ballistic missiles" (Lewis 2017).

1.3 Space-based Assets

Dividing space-based assets along the lines of military and civilian systems is the simplest way as it glances over the entire field of dual-purpose, dual-operator, and dual-user distinction. On the military end, there are four asset categories: Satellites for Space Situational Awareness (SSA), Intelligence, Surveillance, and Reconnaissance (ISR), Military Satellite Communications (MIL-SATCOM), and Position, Navigation, and Timing (PNT).

According to the UCS satellite database, out of the 2,787 satellites currently orbiting Earth, 509 are used for military purposes. This includes satellites whose users are part of the military/commercial space (such as Israel's Space-Communication Ltd.) and military/civilian space (as for example the Defence Science and Technology Group at the University of New South Wales). Military-to-military cooperation in space is fairly advanced, including:

(1) *Satellite co-ownership* – Athena-Fidus, for example, is a French-Italian telecommunication satellite that since 2014 provides dual-use broadband communication services to both the French and the Italian Armed Forces (Leonardo, 'Athena-Fidus'). The satellite was built by France's Thales and Italy's Leonardo.

(2) *Imagery access rights* – The French Helios satellite constellation (currently consisting of two old Helios satellites, two new Composante Spatiale Optique (CSO) satellites, and one CSO satellite in production) is used by Germany, Italy, Spain, and Belgium. In 2015, Germany paid the French government 210 million EUR to receive imagery access to three new CSO satellites. While the German government hailed the deal as another example of French-German cooperation, German military officials, politicians, and aeronautic experts viewed it as a "medium-sized disaster" (Greive & Jungholt 2015). Not only did the buy-in create crucial dependencies on the French, but for the same financial burden the Germans could have built their own satellites with German know-how and German suppliers. All three CSO satellites are manufactured by Airbus in Toulouse with primarily French components (Ingenieur.de 2015).

(3) *Voluntary imagery sharing* – According to a 2018 report by Sueddeutsche Zeitung, Germany's Federal Intelligence Service (BND) and the German army have liaison officers stationed at the National Geospatial Agency in Springfield, VA (USA). The paper notes that the US-side provides them with imagery copies, but only in coarser resolution, and only when the US government considers it advantageous (Bierman & Stark 2018).[4] This lack of cooperation stands in stark contrast to how the Five Eyes countries (the US, the UK, Canada, New

[3] Email sent to ESA on 18 September 2020.

[4] Note: The BND will get its own electro-optical satellite system, dubbed "Georg" in 2022 (Geheimes Elektro-Optisches Reconnaissance System Germany), see: DW 2016.

Zealand, and Australia) cooperate on geospatial intelligence sharing.

(4) *Coordinating* of *space operations* – At the Combined Space Operations Center (CSpOC) located within US Space Command at Vandenberg AFB (CA, USA), the US cooperates with its Five Eyes partners, as well as Germany and France, to "synchroniz[e] and execut[e] space operations; provid[e] tailored space effects on demand to support combatant commanders; and accomplish national security objectives" (USSPACECOM 2019). This essentially means that CSpOC coordinates and tracks the movements of military satellites.

Apart from mil-to-mil relations, government agencies, such as the US National Reconnaissance Agency (NRO), are also specifically tasked to purchase commercial satellite imagery to augment government intelligence (Hitchens 2020).

The overall point is that particularly military satellite systems owned by Western nations are not always single-use or single-owned – and can pivot if necessary, to commercial satellite services to bridge short-term redundancy gaps. An adversary who – for example – is interested in disrupting German geo-spatial satellite intelligence capabilities would have to disrupt a host of allied satellite systems as well as commercial satellite services to achieve a tangible and persistent effect over time. Even in the area of satellite communications, substantial disruptions and adversarial capabilities would have to be mounted to degrade Germany's military satellite communication coverage. In the case of Switzerland, it is even more complicated for an adversary. Not only does the Swiss military not own any satellite systems itself – as it buys those capabilities from partner nations and civilian operators – but it relies primarily on non-satellite communications as its armed forces are to a large extent focused on homeland defense (RTS 2020).[5] The downside of the Swiss dependencies is that in times of conflict, commercial service providers and partner nations might be reluctant to share military intelligence or partially deny commercial satellite services to the Swiss military.

Which brings us to the civilian/commercial space assets. According to the UCS satellite database, out of the 2,787 satellites orbiting Earth, 1,780 fall into this category. This includes satellites whose uses are purely commercial (such as Gazprom's Yamal-202, which provides communications for gas corporation operations throughout the Eurasian continent), government/civilian (such as ESA's EUMETSAT), and government/commercial assets (ex. China Satcom). USC distinguishes between five categories of civilian/commercial satellites: communication satellites, and those used for Earth observation, navigation, space science, and technology development.

The data and services of the vast majority of these satellites serve a multitude of companies and government agencies back on Earth. Meaning, even if an adversary is aiming to harm Gazprom operations in Eurasia by hacking into Yamal-202, the repercussions of Yamal's service disruptions will traverse throughout the region and effect numerous companies in varies countries. Particularly in the context of computer network attacks (CNA), cascading effects are not a desirable outcome due to their uncontrollable and public nature, and the inherent uncertainty of eliciting political or even military countermeasures. The spread of NotPetya is probably the most notable CNA campaign that most likely went way beyond its intended target.[6] In essence, civilian/commercial satellites are sub-optimal CNA targets during times of war and peace.

On the other hand, computer network operations whose aim is to solely undermine data integrity, would be most persistent if run directly on the satellite where the data is generated – rather than on the data collection backend (i.e., data centers). That being said, computer network exploitation (CNE) operations, whose goal it is to syphon data for the purpose of intelligence gathering, should preferably run on the data collection backend, rather than on the satellite itself, due to limited satellite bandwidth and exfiltration channels.

One important point to raise, which surprisingly is rarely touched upon in the context of securing space-based assets, is the quantitative end. Most studies – as this study also does – commence with the argument that space is getting more crowded. Which is true. The same studies then entirely avoid touching upon the issue of manageability. 2,787 satellites in orbit, that are controlled, maintained, serviced, and secured by a limited number of companies and government agencies is a manageable undertaking. By contrast, controlling, maintaining, servicing, and securing seven billion IoT devices scattered among thousands of companies back on Earth is certainly not.

1.3.1 Legacy Systems

Given the inherent costs and not entirely risk-free efforts to launch an asset into Earth's orbit, the life span of a satellite should desirably meet or exceed its design life. Meaning, a satellite designed to operate for at least 12 years in space, should not fail in year four. The good news is that according to a large n-study by Kristen

[5] Exceptions to the homeland defense focus include: Peace support operations, foreign protection missions, or special forces operations.

[6] Note: As with all CNA operations, adversarial motivations are difficult to grasp. For example, NotPetya could have been a targeted campaign primarily aimed at affecting Ukrainian companies, but it could also have been intended to primarily harm international companies doing business in Ukraine.

Ferrone at Aerospace, "~87% of U.S. military and civil satellites and ~75% of commercial satellites met or exceeded their design life" (Ferrone 2019). The bad news is that commercial satellite owners and government operators differ greatly on whether longer or shorter design lives are the way to go.

Speaking at Space Tech Expo in 2018, David Davis, chief systems engineer for the US Air Force Space and Missile Systems Center (SMC) noted that "the U.S. Air Force wants to update its technology in orbit more frequently by moving from satellites designed to last 10 to 15 years to satellites built to operate for three to five years" (Werner 2018). A similar thought resides in the US Space Force, which is primarily interested in distributing architecture in space across far more smaller satellites as the US currently does, to create redundancies, increased resilience, and make it harder for an adversary to target specific capabilities (Erwin 2020).

Meanwhile, Jean-Luc Froeliger, vice president for satellite operations and engineering at Intelsat, would like satellites to function indefinitely, based on the logic that even as an older satellite "may not bring in the same type of revenue it did at the beginning, [but] the satellite and launch are paid for and operation costs are minimum" (Werner 2020).

To reconcile both views, one can either acknowledge that different satellite classes, designs, and mission profiles will inherently determine a satellite's design live – meaning there is no common ground to be sought, which is bad news from a cybersecurity point of view, as higher life spans on the commercial end directly translate into exacerbating the hard- and software legacy challenges in space. While there is certainly interest within the industry to bringing the life span of satellites down to create higher refresh rates, the current obstacle is not so much launch costs but the satellite manufacturing costs itself (NSR 2018). The obvious work-around to that would be to build off-the-shelf, plug-and-play satellites which would naturally expand the attack surface.

Or one could take DARPAs approach which seeks – in cooperation with the SMC – to demonstrate how DoD can use primarily commercially-based technologies to build low Earth orbit satellite constellations. Essentially creating co-orbiting patches of military-commercial satellite webs that will take advantage of the ongoing space race between OneWeb, SpaceX (Starlink), and Amazon (Kuiper) (Forbes, n.d.).[7] According to DARPA this hybrid satellite battle architecture could enable one- to two-year technology refresh cycles compared to the current ten years (Hitchens 2019). Apart from the reduced life-cycle, DARPA will also have to ensure that connecting military satellites to commercial space assets will not introduce vulnerabilities into this hybrid constellation. Meaning, commercial satellites will have to fulfill certain cybersecurity requirements, including trusted hard- and software to "collect, generate, store, process, transmit and receive national security information," as well as end-to-end encryption and secure networking to establish secure communication links among multiple satellites (Leonard 2018).

Note: If DARPA's approach moves from fiction to reality, we might also see a rapidly increasing interest to find ways to conduct satellite-to-satellite breaches in orbit. So far however, there are no publicly known instances of satellite-to-satellite hacks ever having occurred (Falco 2020).

While NASA and several aerospace companies are in the process of exploring on-orbit satellite servicing solution – i.e., platforms that can hook themselves onto a satellite in orbit for maintenance purposes - the reality is that physical access to a satellite in orbit is currently not possible (NASA 2010b). As a result, system legacy problems in space are much more pronounced than they are back on Earth. In orbit, satellite hardware cannot be upgraded nor is it possible to entirely overhaul a satellite's firmware and other software components. The parameters of what can be changed in space systems is indeed rather narrow, which is both good and bad news for cybersecurity.

In the very old days, space operating systems were custom-built for their missions. But in 1987 a US company called WindRiver introduced VxWorks, the first off-the-shelf real-time operating systems (RTOS), which together with ESA's RTEMS, ECos, open-source Linux RTOS solutions, and numerous other space OS systems are today used in a wide-range of satellites. RTOS systems work differently than Windows 10 does, as it adds strictly specified deadlines to each computational task. If the computational deadline is not met, then the task is considered failed and is subsequently terminated (i.e., bounded response time).

For space systems this is of particular importance as Jacek Krywko, writing for ArsTechnica, explains: "A missed deadline quite often means your spacecraft has already turned into a fireball or strayed into an incorrect orbit. There's no point in processing such tasks any further; things must adhere to a very precise clock" (Krywko 2020).

Another aspect of RTOS systems is that they go through incremental changes over a longer period of time, rather than significant platform overhauls in a few years like Microsoft Windows. Maria Hernek, head of flight software systems at ESA, explained this neatly by noting that "we don't play with new space software because we think it's fun. We always have good reasons to do it. It's always either that the software we have

[7] Note: Military satellites are solely launched from the homeland or allied space ports. This stands in stark contrast to commercial satellite launches, which are largely driven by pricing, on-board space, launch vehicle thrust, and launch vehicle availability.

available does not solve our problems, that it causes some problems, or something like that" (Krywko 2020).

VxWorks' OS maturity does however not mean that all versions of VxWorks and other space OS are free from security vulnerabilities. Back in mid-2019, enterprise security firm Armis discovered a group of vulnerabilities in VxWorks' TCP/IP network protocols it collectively dubbed Urgent/11 (Armis 2019). Because VxWorks is not solely used in space systems, but is also widely deployed in critical infrastructure back on Earth, including "elevator and industrial controllers, patient monitors and MRI machines, as well as firewalls, routers, modems, VOIP phones and printers," Urgent/11 was approximately affecting 200 million devices (Armis 2019; Hay Newman 2019). As Ben Seri, vice president of research at Armis, succinctly summarized, "finding a vulnerability in the network layer means it would affect any device that is using this operating system and that has networking capabilities. It's like the holy grail of vulnerability research finding something in that layer" (Hay Newman 2019). One major problem in fixing a VxWorks vulnerability at scale is – as Wired's Lily Hay Newman correctly pointed out – that these assets "typically run continuously, and often depend on customized software that requires a tailored patching process" (Hay Newman 2019).

Although Armis noted back in mid-2019 that they found no indicators that Urgent/11 vulnerabilities were exploited in the wild, open source information is unclear as to whether this still holds true for 2020. As with critical infrastructure vulnerabilities in general, most industrial system will not get patched at all – de facto turning Urgent/11 into forever-day vulnerabilities (Goodin 2012).

As of this writing it is unclear whether any satellite systems were running the affected VxWorks versions and whether those affected were patched – or could be patched – as a result of Armis' disclosure (dpaonthenet 2010).

The bottom line is that cybersecurity lessons learned in space are not very much different from the best practices back on Earth. Space-based assets should be able to perform software updates; they should be able to respond to incidents remotely; and they should always maintain or be able to recover positive control – meaning to only execute commands transmitted by an authorized source, in the proper order, at the intended time. For space-based assets those requirements are significantly more pronounced than they are on Earth, as physical access is impossible to gain to a satellite maintaining an orbital speed of between 7,000 and 28,000 km/h. The White House's Memorandum on Space Policy Directive 5 from 4 September 2020, covering cybersecurity principles for space systems, stresses these exact requirements in an effort to "further define best practices, establish cybersecurity-informed norms, and promote improved cybersecurity behaviors throughout the Nation's industrial base for space systems" (WhiteHouse 2020).

1.3.2 Data Centers in Space?

Currently there are no data centers in space, and satellites are certainly not akin to anything remotely close to floating servers. Thus, while the cloud-revolution expanded rapidly on the terrestrial surface over the past decade – and is now making inroads into the maritime domain – not a lot of data is actually hosted in space at any point in time. The reasons for this lack of data hosting does not stem from the space environment itself. In fact, deploying cloud servers in space would be to a certain degree ideal, as they can be powered by the Sun and cooled by the icy vacuum of space – which in turn reduces equipment failure and enables higher processing speeds. Similar to Microsoft experimenting with cloud servers deployed underwater, cloud servers in space would also self-manage in a so called 'lights-out' state of play – which is free from human access and comfort, and solely optimized for computing efficiency (Donoghue 2017).

The major hurdle that currently stands in the way of the data colonization of space is the sheer cost of launching server rackets into space. Which is not necessarily a hurdle that will persist for very long, as SpaceX and other commercial launch services are likely to significantly push down prices over the next decade.

In late-2018, the Los Angeles-based satellite start-up Cloud Constellation closed a 100 million USD round of funding to build Space Belt – a network of data centers built on satellites in orbit (Sheetz 2019). One of the selling points that Cloud Constellation CEO Cliff Beek stressed was "global data protection that leverages commercial space" at a time when cyberattacks and data breaches are on the rise (Sheetz 2019). Whether Cloud Constellation can fulfill its lofty promise remains to be seen, but if the data center experience back on Earth is any indication, Space Belt is going to become a very attractive target for nation-state adversaries, cybercriminals, and script kiddies alike. And do not forget the lawyers and law enforcement agencies that will want to gain access or close down access to data hosted in space.

The so-called "Weltraumtheorie" (space theory) put forward by Germany's foreign intelligence service (BND) in August 2013, in the aftermath of the Snowden Affair, should be a warning sign for things to come (Biermann 2016). The BND tried to argue that, because satellites are located outside of national sovereign territory, satellite communication data links are consequentially not protected by any national laws. Similarly, because the BND collects data from foreign satellites – which themselves collect data that does not fall under German jurisdiction – the data harnessed from those foreign satellites by the BND is also outside the purview of German law (Biselli 2016). In effect, the Weltraumtheorie tried to totally disconnect data collection from space from the legal realities back on Earth. In the end, the BND failed with its creative legal interpretation as Germany's Federal Constitutional Court ruled in May 2020 that the BND's actions are bound by Germany's Basic Law and are not limited to actions occurring solely on German sovereign territory (BVerfG 2020).

In similar vein, the mirroring of Earth-based infrastructure in space is going to create synergies in the area of software and hardware overlaps that for a long time have shielded space-based infrastructure from non-state adversaries. Meaning, if Windows servers are deployed in space, they are likely going to be equally targeted and equally vulnerable as Windows servers back on Earth. With the infrastructure gap between space and Earth vanishing, the cyber threat landscape in space will naturally expand, and so will the risk to other space-based assets that will become reachable.

1.4 Up- and Downlink

In a strict sense of terminology, up- and downlink data streams from a satellite to a ground station, and vice versa, are located in the electromagnetic spectrum – the so called "space in-between". As outlined in the introduction, this paper will not venture into the area of jamming and spoofing; but it will look at signal interception – which partially falls into the cyber domain (think data fusion and data relay).

There are five basic satellite orbits: low-, medium-, and high Earth (LEO, MEO, HEO), as well as polar, and geostationary orbits (GEO). To a degree, we can generalize what kind of satellites are located in what orbit. LEO is preferably used by Earth observation satellites (approximately 2,000 km altitude or less), MEO is home to navigation satellite systems (such as GPS at an altitude of around 20,000 km), and HEO is populated by early-warning satellites (over 36,000 km altitude). A satellite in lower orbits is generally better positioned (i.e., closer to Earth) to obtain high-quality remote-sensing data and imagery than a satellite in higher orbits. Similarly, a satellite in higher orbits has a far larger satellite area coverage/footprint than a satellite in lower orbits (Johnson 1996). A satellite's area coverage/footprint can be approximately determined by both its distance from Earth, its signal strength, and the frequency bands it is operating on.

Satellites in geostationary orbit (around 35,780 km above the equator) move synchronous to Earth's rotation. Meaning, a ground station that services a geostationary satellite does not have to readjust its antenna constantly, because the satellite hovers always at the same approximate altitude above it. This is particularly useful for communication and weather satellites. By contrast, ground stations that service the vast number of non-geosynchronous satellites have to wait until the satellite either rotates into their field of vision (i.e., makes a pass) – data is meanwhile stored aboard the satellite until it is downloaded – or can maintain contact if the satellite's download link is relayed through other satellites in orbit (Fritz 2013, p. 23). The latter, however, is rather rare, and there are currently no industry standards established for sat-to-sat communications (Strout 2020).

When a ground station wants to connect to a communication satellite, it does so through a transmitter whose radio waves are received by the satellite's transponder(s) in orbit (uplink) during a pass. In the reverse scenario, the satellite's transmitter beams down radio waves to Earth which are picked up by the ground station's or a user's satellite dish/antenna (downlink). Depending on the strength and frequency of the signal, a satellite dish has to vary in size and must be deployed at the correct angle toward the satellite to capture the signal adequately. Satellite passes in LEO orbit only take around five to ten minutes, in which satellite contact can be established to transmit and receive data – because LEO satellites are moving at a speed of 28,000 km/h. Meanwhile, a satellite in geostationary orbit can maintain constant contact with a ground station, but because it is so far out in space, a signal from a GEO satellite takes a quarter of a second to arrive on Earth (one hop), and half a second for a round-trip (two hops).

In the context of up- and downlinks, we also have to distinguish between spot beams (or pencil beams) and wide beams. Spot and wide beams are in themselves relative terms. Meaning, a satellite beam that covers the entirety of Swiss territory can be considered a spot beam when contrasted to a wide beam that covers the entirety of continental Europe. Relatively speaking, spot beams are more concentrated in power and cover a narrower area than wide beams, which (a) reduces the risk of interference with other transmissions on the same frequency, and (b) lowers the risk of adversarial and third-party interception (Bliley 2017). Spot beams are usually utilized in satellite communication up- and downlinks between a specific transponder. Multiple spot beams from a single satellite can also be used to connect to several ground stations, in an effort to overcome rain fade or to compensate for a degraded signal (Bliley 2017).[8]

[8] Rain fade or attenuation: Atmospheric rain, snow, and ice absorb microwave radio frequency signals, which can lead to a degraded or lost signal on the receiver's end. They are the major environmental causes of satellite communication system outages.

Generally speaking, to intercept satellite communication signals an adversary has to be either located within the satellite's footprint on Earth (downlink interception), somewhere in-between the satellite and the transmitter(s)/receiver(s) on Earth (uplink interception), or in-between two satellites to intercept sat-to-sat downlink relays in orbit.[9]

Because LEO satellites are so close to Earth, their signals can be picked up by amateur ham-radios. The International Space Station, for example, has one on board that lets the crew make random radio contact with Earth-bound ham-radio amateurs and students alike (ARISS, n.d.). Iridium communication satellites – which are also located in LEO – and used for unencrypted pager traffic, satellite phone calls, and other data communications can also be picked up fairly easily. At CCCamp 2015, Germany's Chaos Computer Club handed out 4,500 rad1o badges (i.e., software defined radios) that were sensitive enough to intercept Iridium communications (Porup 2015).

It should be noted that the Iridium communication network consists of 66 satellites that were put into orbit between 1997 to 2002, with a life expectancy of eight years. No satellites were launched between 2002 and 2017, which puts the constellation way past its expiry date. Please also note that it is one thing to intercept satellite communications and quite another to reverse-engineer and inject meaningful messages back into the data stream to achieve a discernable effect (i.e., to reroute a postal package to a different location).

1.4.1 **FORNSAT**

According to a 2004 document in the Snowden leaks, the collection from foreign communication satellites (FORNSAT) was "the source of over 30 percent of NSA and U.S. Field reporting […] 46 percent of arms proliferation reporting, 30 percent of counter narcotics reporting, and 29 percent of counterterrorism reporting […]" (USN 2004).

This brings us to Menwith Hill Station (MHS) – the largest NSA eavesdropping outpost on British soil. Located in North Yorkshire, the 605 acres large compound hosts 37 radomes (so-called gulf balls, i.e., weatherproof structural enclosures that protect a radar dish/antenna), and is staffed by approximately 1,400-2,200 NSA and GCHQ staff (BBC 2019). According to the Intercept, MHS's FORNSAT mission (codename MOONPENNY) "was monitoring 163 different satellite links" back in 2009, "storing phone calls, text messages, emails, internet browsing histories, and other data" (Gallagher 2016).[10]

Among other items, MHS also supported GCHQ in the aftermath of the London bombing on 7 July 2005, by "tracking phone, GSM, SMS, and high-powered cordless phone signals" (MHS 2005b). Documents in the Snowden Leaks also note that this "included putting nine U.K. cities under mass surveillance by monitoring satellite phones via 'VOICESAIL.' NSA analysts also found a certain area in Pakistan with a high density of calls to the U.K. […]" (MHS 2005b). MHS also runs/ran XKEYSCORE's Deep-Dive Packet Analysis called QUANTUMTHEORY, for "real-time packet inject in response to passive collection of target communications" (MHS, n.d.). In essence, a CNO man-on-the-side (MOTS) operation that "inspects each packet, one at a time, for a set of keywords that determine if the packet originated from a CNE target and if a modified response to that packet might result in exploitation of the client computer" (MHS, n.d.).[11] MHS even ran an operation that targeted World of Warcraft (WoW) by fusing FORNSAT packet data with other systems and databases to spot entities per their WoW logon events and "by identifying accounts, characters, and guilds related to Islamic Extremist Groups, Nuclear Proliferation and Arms Dealing" (MHS 2008).

The Snowden Files also revealed that MHS maintains access to US and British military communication satellites in orbit. Which allows it to quickly accrue data to, for example, aid in identifying the location of a distress signal in Afghanistan to guide Combat Search and Rescue (CSAR) operations, or to intercept mobile phone signals across the African continent to track and trace individuals for capture or kill missions (MHS 2005b; USG 2005). Much still remains secret about the activities at MHS – but one thing is certainly sure: like Pine Gap in Australia, Bad Aibling in Germany, and Misawa in Japan, Menwith Hill Station is part of an extensive network of NSA eavesdropping posts that play a fundamental role in the defense of the United States and its allies across the globe.

In contrast to well-established intelligence operations to gain FORNSAT access, some APT threat actors – such as Russia's Turla – have explored ways to use satellites as command-and-control nodes in their campaigns. According to Kaspersky, Turla has been leveraging "satlink hijacking" since around 2007. As Kaspersky explained it in 2015, "to attack satellite-based Internet

[9] Other examples include: Satellite communications intercepted by third parties and transmitted to us; satellite communications intercepted in on-Earth routing (i.e., at satellite signal relay stations or by tapping into data cables); and satellite signals intercepted by mirroring legitimate ground station up- and downlink streams (i.e., broken encryption codes). One can also intercept satellite communications by pointing a dish at the Moon and listen to the radio signals that bounce off it (also known as Earth-Moon-Earth or EME).

[10] MHS was most notably also part of the Five Eyes' project ECHELON, see: Schmid 2001.

[11] Note: MOTS are similar to man-in-the middle attacks (MITM). The main difference being that "with MITM, the attacker is present on infrastructure the traffic is traversing and can tamper with it […]. With MOTS, the attacker has sufficient access to observe and inject traffic which through timing/bandwidth is consumed by the victim before the legitimate reply arrives." See: Vijayan 2019.

connections, both the legitimate users of these links as well as the attackers' own satellite dishes point to the specific satellite that is broadcasting the traffic. The attackers abuse the fact that the packets are unencrypted. Once an IP address that is routed through the satellite's downstream link is identified, the attackers start listening for packets coming from the Internet to this specific IP. When such a packet is identified, […] they identify the source and spoof a reply packet back to the source using a conventional Internet line" (Tanase 2015). The downside to this technique is that satellite Internet has been rather slow and unstable in the past, which is why "Satellite Turla" has been rarely observed in the wild. However, this might change when SpaceX, Amazon, and OneWeb succeed in their global satellite Internet plans.

Back in 2017, The Intercept got their hands on a classified presentation by Canada's signal intelligence agency, the Communication Security Establishment (CSE), covering a Russian state-supported threat actor they named MAKERMARK – which conducted the same satlink hijacking that Turla does. While it is still unclear whether MAKERSMARK is synonymous to Turla, the presentation was rather dismissive of MAKERSMARK's skills. On one slide, the CSE criticized that MAKERMARK is not following CNE best practices by live testing new implant protocols. On another, it highlighted that the C&C servers were used for personal browsing (i.e., checking Vkontakt and .ru email accounts). All in all, CSE summarized MAKERSMARK with the words "designed by geniuses, implemented by morons" (CSE, n.d., p. 6). While this assessment certainly diminished the achievements of the Russian group, one has to be careful to dismiss an early experimental approach to "test things," with one that will mature over time and close operational security gaps. Time will tell how threat actors will evolve and attach themselves to the new possibilities of vast satellite Internet infrastructure and data centers being deployed in space.

Please note that this report was unable to investigate the issue of up- and downlink encryption of data traffic in a sensible manner. The primary reasons being, (a) a lack of comprehensive open-source data, (b) the general variety of encryption algorithms used, and (c) the use, sporadic use, or non-use in various parts of the data transmission chain. In the absence of an initial mapping of the use of encryption for data-at-rest in space and data-in-transit through space, no sensible evaluation – nor general analysis – can be made as to the state-of-play of encryption use in space.

2 Terra Calling

Within the larger objective of securing and defending the space economy, two organizations/agencies take center stage in Europe and on the other side of the Atlantic: NASA and ESA.

To highlight their roles and shortfalls in the cyber domain, this section takes a closer look at two short case studies. The first peeks into the history of persistent cybersecurity problems at NASA, the functioning of the NASA Security Operation Center, and the work of NASA's Office of the Inspector General.

The second short case study takes apart the unprecedented seven-day outage of Galileo in July 2019. While much is still unknown about the incident, open sources are pretty clear on the impact, the slow incident response, and how the failure played out among Galileo's user base.

Both case studies will hopefully help the reader to understand and pinpoint why cyber and cyber-related issues are so persistent and difficult to address.

2.1 Case-study NASA

Testifying back in June 2003 before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, then NASA inspector general (IG) Robert W. Cobb explained that, "IT security activities at NASA have historically been carried out on a decentralized basis [as agency systems are distributed across various locations throughout the US]. This has resulted in a lack of synchronization in development efforts and a lack of full interoperability among the systems developed. We have reported on issues including inadequate security training for system administrators, an inconsistently applied program for ensuring security of sensitive systems, inadequate implementation of NASA's host and network security policies and procedures, inadequate security plans for NASA's IT systems, and an inadequate incident response capability" (Cobb 2003, p. 2).

Unsurprisingly, the 2004 Federal Information Security Management Act (FISMA) report subsequently noted that the NASA IG evaluated the quality of agency certification and accreditation processes at NASA as poor – on par with the evaluation of his IG colleagues at DoD, DHS, the Department of Commerce, the Department of Energy and others (OMB 2005, p. 9).

Throughout the years, NASA has incrementally implemented various solutions to improve its IT security posture. Yet by fiscal year 2007, NASA's Administrator, who heads the agency, noted that IT security is still a "material weakness," that could potentially compromise the "integrity, availability, and confidentially of mission-critical data. The operational efficiency of the agency is also hampered by the inconsistent application of security solutions at different NASA Centers. If this weakness continues, mission resources may have to be reallocated to bring the agency's IT systems into compliance" (NASA 2007, p. 20).

During the fiscal years 2007 and 2008, NASA reported a total of 839 security incidents to US-CERT that resulted in the installation of malicious code on its systems and 209 cases of unauthorized access to sensitive information (GAO 2009, p. 32). According to GAO, the number of malicious code installations was “the highest experienced by any of the federal agencies, which accounted for over one-quarter of the total number of malicious code attacks directed at federal agencies during this period” (GAO 2009, p. 33).

While NASA has maintained an Incident Response Center (NASIRC) since 1993, that was supposed to provide “an agency-wide computer and network systems incident response and coordination capability,” the reality was that the various NASA Centers were “not submitting all required reports on IT security incidents to the NASIRC” (Thomas 1995; Cobb 2003, p. 5). Similarly, “information in the NASIRC incident database was unreliable for a variety of reasons, and the NASIRC could not produce accurate, complete, and meaningful analyses and reports” (Cobb 2003, p. 6).

In November 2008, the NASIRC eventually transitioned into a full-fledged SOC located at Ames Research Center (NASA CIO 2008).

In 2011, NASA’s OIG performed a rudimental vulnerability test on computers connected to NASA’s agency-wide mission computer network. Among the 190 IT systems and projects identified on the network (176,000 IPs), eight IT projects were Internet-accessible (54 IPs). According to the OIG, “these servers were associated with moderate- and high-impact NASA IT projects used to control spacecraft or process critical data” (NASA OIG 2011, p. 3). In six of the eight projects, the OIG also found that “encryption keys, encrypted passwords, and user account lists were exposed to potential attackers” (NASA OIG 2011, p. 5). One server even leaked “sensitive account data for all its authorized users” (NASA OIG 2011, p. 5).

Skipping forward to 2018, the OIG audited the NASA Security Operations Center for the first time. According to the report, the SOC is staffed by ten NASA civil service personnel and 36 contractors (NASA OIG 2018, p. 2).

The OIG’s report came to devastating conclusions, as it found several institutional obstacles to meaningful progress. First, the report notes that “since its inception a decade ago, the SOC has fallen short of its original intent to serve as NASA’s cybersecurity nerve center. Due in part to the agency’s failure to develop an effective IT governance structure, the lack of necessary authorities, and frequent turnover in the Office of the Chief Information Officer (OCIO) leadership, these shortcomings have detrimentally affected SOC operations, limiting its ability to coordinate the agency’s IT security oversight and develop new capabilities to address emerging cyber threats. In sum, the SOC lacks the key structural building blocks necessary to effectively meet its IT security responsibilities” (NASA OIG 2018, p. 10). While it is industry best practice to sign a charter together with stakeholders to outline authorities and responsibilities, the OIG highlights that, “in addition to lacking a charter, the SOC has no roadmap or plan for continual service improvement to address its strategic vision or overall goals” (NASA OIG 2018, p. 11). In terms of leadership overhaul, the OIG found that “since the SOC’s establishment in 2008, nine different individuals have served as [Senior Agency Information Security Officer] SAISO, six of whom have served in an “acting” capacity, including the current SAISO” (NASA OIG 2018, p. 4).

If this were not devastating enough, the OIG addressed the challenges head-on by criticizing that, “while the SOC’s original intent was to provide end-to-end monitoring, incident detection, and response services for the entirety of NASA’s network and systems footprint, the reality is that a series of challenges prevent the SOC from meeting this enterprise-wide goal. Ten years after its creation, the SOC continues to lack visibility into the majority of NASA’s Mission systems even while it bears significant responsibility for protecting those systems” (NASA OIG 2018, p. 2).

The major reasons for this lack of visibility are two-fold. On the one hand, NASA’s high- and moderate-impact systems reside within mission networks – whose incidents are the sole responsibility of the system owner or designated IT security staff (i.e., incident response team). As the report notes, the individual NASA Centers “may perform mitigation and prevention actions in response to a particular incident, if the SOC determines that these actions need to be performed agency-wide, it will coordinate a response at the agency level. The SOC does not perform remediation actions itself but instead relies on Center or Mission Directorate staff who have the authority and capability to block specific internet data” (NASA OIG 2018, p. 6).

On the other hand, the decentralized nature of NASA’s operations has prevented the SOC from “developing a complete network map of NASA’s enterprise infrastructure to identify the physical connectivity of all agency networks and devices” (NASA OIG 2018, p. 16). As a result, the SOC has to painstakingly figure out manually where certain systems and devices are physically and logically located, and is unable to more efficiently allocate resources to high-value assets that reside within the network.

As the OIG correctly summarizes, “the lack of complete network mapping coupled with the SOC’s lack of visibility into mission networks means the SOC is unable to identify and protect many critical assets in the NASA architecture because they do not know they exist” (NASA OIG 2018, p. 17).

According to the OIG’s latest report of June 2020, “NASA continued to make limited progress in securing its networks and information systems" (NASA OIG 2020, p. 14).

Please note that, as a federal agency and the law enforcement arm of NASA, the OIG has also been at the forefront of fighting cybercrime. According to Krebs, the agency was instrumental in the investigation into McColo, 3FN, and was even successful – during a lengthy investigation into the cyber theft of sensitive technical data from NASA systems – to get Chinese authorities to detain a Chinese national in China for violations of China's Administrative Law in December 2010 (Krebs 2015). The OIG also led the investigation into the alleged first-ever cybercrime committed in space – with NASA Astronaut Anne McClain being accused in August 2019 by her estranged spouse of improperly accessing a bank account while serving aboard the International Space Station (Baker 2019). In April 2020, McClain was cleared of wrongdoing and her former spouse was charged with lying to federal investigators (Baker 2020).

2.2 Case-study Galileo

The European Global Navigation System (GNSS) – known as Galileo – achieved its initial live services capability in December 2016, providing users worldwide with position, navigation, and timing information. As of this writing, Galileo comprises 26 satellites deployed in three MEO orbital planes (22 usable, 2 in testing, 1 not usable, 1 not available) (GSA, 'Constellation Information'). Initial plans foresaw the completion of the constellation for a total of 30 satellites in orbit by the end of 2020 (GSA, 'Galileo Initial Services'). To date, one launch has been preliminarily scheduled for mid-2021, to bring Galileo satellite 27 and 28 into orbit aboard a Soyuz taking off from the Guiana Space Center in South America (Spaceflight Now, 'Launch Schedule').

During a system upgrade on 10 July 2019, a service incident occurred in the Galileo ground infrastructure – which went publicly unreported until 14 July, when the European Global Navigation Satellite System Agency posted on its website that Galileo is "currently affected by a technical incident related to its ground infrastructure" (GSA 2019). While Galileo's Search and Rescue (SAR) service was unaffected, the incident did lead to a "temporary interruption of the Galileo initial navigation and timing services" (GSA 2019). GSA assured users that "experts are working to restore the situation as soon as possible" (GSA 2019). For seven days straight the outage persisted, with all 22 of Galileo's previously usable satellites being flagged as "not usable" or in "testing." The incident was indeed unprecedented as "billions of organizations, individuals, phones, and apps from across the globe simply stopped listening to Galileo" and automatically switched to the US-operated GPS as a backup (this is also why most end users did not take notice of the outage) (McCarthy 2019; Porter 2019).

While end users seemed unburdened or were entirely unaware of the outage, the community that was most heavily invested in Galileo – such as application entrepreneurs, design engineers, system integrators, and service providers – did feel the impact. The general situation was one of confusion, as "the official Notice Advisories (NAGUs) posted on the European GNSS Service Centre website were slow to appear and provided little detail. Meanwhile, no voice was heard, no face was seen, no representative of the program was available for an official comment" (IG 2019).

According to Inside GNSS – an outlet covering GNSS engineering, policy, and design – one industry executive noted that "it's inexcusable how long it took after the failure occurred until the user base was informed. Even worse the SIS/health flag showed no problems until the very end. I was surprised. A total constellation failure should not be happening in the modern world of testing and simulation. The reaction was slow and until this day has been very secretive and political. As there has been no official communication, all my theories [concerning the technical cause of the failure] are derived from Inside GNSS!" (IG 2019).

Indeed, one major communication problem Galileo faced during the incident was the sheer organizational complexity of making decisions within an EU-non-EU hybrid organization that encompasses the EU Commission, the EU GNSS Agency, ESA (all EU countries + Canada, Norway, and Switzerland), GMV (the private company responsible for developing and maintaining the ground control segment of Galileo satellites), and others. The Register thus rightly noted that "no one in the satellite of organizations around Galileo felt they were authorized to talk about what was going on, leaving it up to [European Commission] officials – none of whom knew what was going on either. In other words, a classic clusterfuck of communication" (McCarthy 2019).

On 17 July, the incident was finally fixed and Galileo went back online. However, while a full public account on what exactly led to the incident is still unavailable, GNSS industry representatives were invited in September 2019 to a "Galileo post mortem" event. It is unclear from open-source material whether this event is the same as the 2019 ION Conference in Miami at which a presentation was given on the Galileo service recovery (ION 2019).

The Register pieced together the sparse information available from the ION slides and combined them with details dug out by entrepreneur and software developer Bert Hubert, who became intrigued by the Galileo failure and set up an independent resource to monitor the system (Hubert 2019).

According to The Register, the actual Galileo satellites themselves were working fine and were indeed in their expected positions, but the software that kept the atomic clocks on the satellites in sync was not. “There was some kind of anomaly in the reference time system while it was being upgraded – which is where the operator error came in – and that sent the whole system spinning,” as the Register explains it (McCarthy 2019). Additionally, the backup systems were not available for some reason during the upgrade, meaning “it wasn't possible to simply rollback to the previous version. As a result, things got more and more inaccurate” (McCarthy 2019). On top of that, the system was somehow not configured normally, which is why the engineers were not able to put things back together. In the end, the decision was made to reboot the entire system, which – due to its complexity – took several days to complete.

Overall, The Register concluded that “there remains precious little information about how and why it all went so wrong in the first place and why adequate recovery systems weren't in place” (McCarthy 2019).

In the aftermath of the incident, the EU Commission set up an Independent Inquiry Board in September 2019 (EC 2019a). The Board’s final report still remains EU classified, and only four of its very general recommendations were published on the Commission’s website in November 2019 (EC 2019b). Even more disturbing than this level of secrecy was that the seven-day outage did not even have much of an impact in Galileo’s quarterly performance report. In fact, the report noted that “during this quarterly reporting period, the measured Galileo Initial Open Service performance figures exceed the Minimum Performance Level (MPL) targets specified in the [OS-SDD], with the exception of the UTC availability MPLs in July” (GSC, n.d., p. 4). As The Register rightly quipped, “yes, despite the entire system going offline and being unusable for a week, the European Global Navigation Satellite Systems Agency (GSA) is proud to report that it has hit all its targets so you can keep sending the cash” (McCarthy 2020).

The reason for this surprisingly favorable assessment stems from Galileo still being considered to be in its initial services phase – and not yet fully operational. Meaning, the Minimum Performance Level target is set to a mere 77 per cent availability per month (IG 2020). In the month of July, Galileo availability reached 81 per cent. By contrast, the months of August and September recorded 99 per cent availability.

Time will tell whether another outage of this proportion or even an adversarial operation can and will occur once Galileo reaches its full operational capability. As Hubert correctly notes, “if a major outage needed many things to go wrong at the same time, that means it was not theoretically an accident waiting to happen” (Hubert 2019). So it might have been good news that the outage occurred when it did and how it did.

3 Threat Reality and Fiction

This section takes apart the most referenced examples in the context of satellite hacking and incidents related to the space economy. An overwhelming number of mainstream articles written on satellite hacking mentions at least one of the incidents outlined – which in itself is deeply troublesome – because the evidentiary basis for most of these incidents is shaky at best and non-existent at worst.

This section therefore seeks to readjust the reality of satellite hacking and serve as reference point, to appropriately contextualize and to fact-check reporting on these incidents for readers. Separating reality from fiction and questioning sensationalist reporting on past cyber incidents is elemental if we aim to gauge the actual threat landscape and avoid that policy priorities are influenced by stories that baselessly exude fear, uncertainty, and doubt (FUD).

Misleading narratives propelled by such unsubstantiated reporting have been held up and disseminated far and wide. This section seeks to set the record straight.

3.1 1997 Jay Dyson and H4GiS

We embark on our journey by taking apart one campaign from the late-1990s that does not really fit into the picture of what we usually consider a cybersecurity incident in the space economy. The reason for mentioning this case first is to highlight the human element in the cyber domain. Already in the old days of the Internet, once things got personal, they tended to escalate with the potential to spur malicious actors into a campaign that could destroy a person’s life and livelihood. Remembering these effects helps us understand and recall that adversarial campaigns can spill over into the personal space, and subsequently result in severe psychological effects on the human side. Guarding against these threats should be on the priority list of every academic institution, company, and government agency alike.

The story begins at 10 a.m. on 5 March 1997, when Jay Dyson – at the time a security engineer at NASA’s Jet Propulsion Laboratory (JPL) – discovered that the Hackers Against Geeks in Snowsuits (aka H4GiS) had gained root level access on some of NASA’s computers, and deployed password sniffers and backdoors across the network. H4GiS also defaced NASA’s website in the process with the slogan that “all who profit from the misuse of the Internet will fall victim to our upcoming reign of digital terrorism […] The commercialization of the Internet stops here” (Penenberg 2000).

The story could have ended with the JPL team ejecting H4GiS from its network and patching the security holes, but it did not. As Adam Penenberg at Forbes put it, “Dyson took this all too personally. Then he made his first mistake: He bashed Hagis online, posting the attack on his own Web site. ‘You are just a bunch of lame kids,’ he wrote” (Penenberg 2000). The second mistake Dyson made was to challenge H4GiS by arguing that this was not “what real hacking is about” and dared them to breach a commercial site.

The quip was enough to turn the whole episode personal for two of H4GiS’s members, known as "u4ea" (Euphoria) and "tr0ut” (Trout). H4GiS was the para-military arm of a hacker group known as the Brotherhood of Warez (BoW), and u4ea was their “founder, president, and dictator for life” (Coleman 2014, p. 37). Gabriella Coleman introduces u4ea in her book ‘Hacker, Hoaxer, Whistleblower, Spy,” with the words: “When I interview hackers who were active in the 1990s about their trolling activities, the conversation inevitably turns toward a discussion of the most feared hacker/troll of the era: “u4ea” […]. So terrifying was this troll’s reign that every time I utter u4ea to one of his contemporaries, their demeanor blackens and proceedings assume an unmatched seriousness” (Coleman 2014, p. 37). Tr0ut on the other hand was not equally prolific. The only other campaign he was provably involved in was – according to written testimony by then FBI director Louis J. Freeh in March 2000 – the 1996 intrusion into the National Oceanic and Atmospheric Administration (NOAA) (US Senate 2000). Together with the NASA breach, the FBI assessed at the time that tr0ut caused damage exceeding 40,000 USD – other sources put the figure closer to 70,000 USD and 200-man hours for repair (WHiTe VaMPiRe 1999).

Instead of u4ea and tr0ut turning their eyes to a commercial site as Dyson suggested, they defaced Dyson’s personal website and took down Internet company Nyx, which provided Dyson’s access, by deleting everything on their network. Nyx subsequently shut down for two weeks to restore its operations.

After a cool-down period of around three months, H4GiS called up Dyson’s phone company and got them to disconnect his home and home-business phones. They then targeted Dyson’s wife Kathleen by breaching her online account and barraging her with threatening messages to the point that she was crying for hours. In January 1998, H4GiS also breached PacificNet, which hosted Dyson’s web design business site, and deleted all his files.

Eventually, Dyson reported the incidents to NASA but was ordered to ignore H4GiS and stand down. NASA’s own Computer Crimes Division could also not help him, as the campaign was not deemed an agency matter. Instead, the only advice he got was to call the FBI. H4GiS’s campaign paired with Dyson’s obsession to call them out eventually swept away his marriage. In June 1998, Kathleen and Jay separated and later divorced. As Dyson put it, “my wife wanted to run and hide, and I wanted to fight” (Penenberg 2000). The fight also took a toll on Dyson himself. He started to smoke and lost 50 pounds in five months. As one of his colleagues at NASA observantly put it, “Jay kept kicking at this beehive, then wondering why he kept getting stung” (Penenberg 2000).

On 1 April 1998, the Canadian Royal Mounted Police (RCMP) arrested 22-year-old unemployed former part-time computer science student Jason Mewhiney aka tr0ut, in Val Caron, Ontario (Reuters 1998). They also raided the homes of his divorced parents in Sudbury and seized numerous documents, diskettes, and his computers. According to CNET, the FBI got to Jason by tracing telephone numbers to the Sudbury area and then tipped off RCMP (CNET 1998). Jason initially faced up to 100 charges for breaching the computer systems at NASA, NOAA, Hughes STC, and several computers at universities in Canada and the US (CBC 1998). He pleaded guilty to 12 counts and served six months in jail.

U4ea on the other hand was never caught and his real identity is still unknown to this day. Some say that u4ea was an FBI informant, but the FBI has strenuously denied this. Open sources allow for no definitive conclusion as to whether u4ea continued to target Dyson after tr0ut’s arrest.

What we do know is that in 2000, Dyson believed that he had traced u4ea’s identity to a man in the Washington area but refused to share any information with the FBI. As Adam Penenberg put it, “Dyson wants to exact his own revenge. ‘I have no intention of dragging u4ea to the authorities,’ he says, fingering his .45. ‘This is strictly between him and me. I will do whatever it takes to see this end come about’" (Penenberg 2000). Jay Dyson passed away on 21 December 2011, with u4ea still at large (XSoldier, ‘Jay Dyson’).

Reflecting on the feud between Jay Dyson and H4GiS, Gabriella Coleman interviewed a former BoW member who explained that “there were massive hacker wars that went on that nobody knew about. […] I mean, this was a time when hackers didn’t want attention, people who talked to the press were mediawh0res. We were a genuine subculture, our own news, our own celebrities, our own slang, our own culture.” “And your own wars,” Gabriella pointedly added (Coleman 2014, p. 38).

Since the Dyson episode, the hacking community has steadily gone mainstream and with it hacker wars have largely become a thing of the past. Nowadays, u4ea and t0out’s campaign would fall into the intersection of social engineering and information warfare; two issues that are gaining more and more prominence in the context of cybersecurity. Ignoring these attack vectors and their tactical evolution and cascading impact comes at its own peril. Yet, to this date it remains unknown whether social engineering and information warfare campaigns have been specifically run against the space economy, and what trajectory the future might hold. More research is needed to figure out whether Jay Dyson's experience is an outlier case, or whether it is part of a series of incidents that have and are targeting the space economy on an individual and private level. As militaries around the globe are increasingly attracted to the idea of running information warfare campaigns to create persistent psychological effects within a population or target workforce, maintaining and caring for the mental health of network defenders will highly likely become a priority for government agencies and the private sector alike.

3.2 1998 ROSAT Satellite

The 1998 ROSAT incident is probably the most famous story passed down over the last two decades that is being repeatedly referenced in discussions about cybersecurity in space. Major outlets such as Wired, Bloomberg, FastCompany, as well as numerous research papers and cybersecurity talks at various high-profile conferences mention the incident as proof of the first-ever destructive cyberattack against a satellite (Scoles 2020; Akoto 2020; Malik 2019).

According to the story as it is commonly told, a threat actor hacked into NASA's Goddard Space Flight Center in Maryland and pivoted into a satellite control system. The threat actor then proceeded to send commands to a US-German satellite X-ray telescope, known as ROSAT (short for the German: *Röntgensatellit*), instructing it to aim its solar panels directly at the Sun. The panels and the satellite's batteries subsequently burned up, which rendered ROSAT inoperable. Eventually, the out-of-control satellite crashed back to Earth.

Parts of the story are real, parts of the story are based on assumptions, and parts of the story are pure fiction – pieces that need to be clearly distinguished and labeled as such.

ROSAT was a US-German satellite X-ray telescope that had been launched from Cape Canaveral into LEO orbit on 1 June 1990.[12] The satellite was designed for a mere 12-month long mission but had a life-span of up to five years (MPE 2011). ROSAT eventually continued to operate for eight years, when in April 1998 an equipment failure occurred in the primary star tracker, which led to pointing errors. According to the Goddard Space Flight Center, "ROSAT engineers in April lost control of the satellite's navigational system, which had deteriorated after eight years in space" (NASA 1999). The secondary star tracker – attached to the Wide Field Camera – was used as a backup option, but it severely restricted the control and tracking of ROSAT (Englhauser 1998). Sometime in September 1998, the satellite's Attitude Measuring and Control System (AMCS) was stuck in safe mode/degraded pointing mode, most likely because the camera "suffered irreversible damage to its collecting plate after accidentally scanning too closely to the sun" (Englhauser 1998; NASA 1999). Any attempts to recover ROSAT failed and thus by 12 February 1999, the satellite was switched off. On 23 October 2011, ROSAT re-entered Earth's atmosphere – partially burned up – and crashed into the Bay of Bengal (MPE 2011).

The hacking part of the story is revealed ten years after ROSAT's malfunction, when in 2008, Keith Epstein from Bloomberg's BusinessWeek, got his hands on a still classified 26-page long network intrusion threat advisory titled "Russian Domain Attacks Against NASA Network Systems," written by then NASA OIG senior investigator Thomas J. Talleur in January 1999.

Going back to events occurring in May 1997, Talleur connects several intrusions over time into various systems at the Goddard Center to paint the picture of a coordinated APT campaign. For example, in May 1997 someone gained access to computers in the X-ray Astrophysics Section of a building on Goddard campus to exfiltrate data that deal with the "design, testing, and transferring of satellite package command-and-control codes" (Epstein & Elgin 2008). In July 1998, another breach occurred at Goddard, which was followed up by the FBI and the Air Force Office of Special Investigations (AFOSI). The trail eventually led investigators to cybercriminals with dozens of IP addresses associated with computers near Moscow. According to Epstein, AFOSI discovered that "the cyber-crime ring had connections to a Russian electronic spy agency known by the initials FAPSI [Federal Agency of Government Communications and Information]“ (Epstein & Elgin 2008). Yet as Epstein also explains, "none of this has ever been made public, and BusinessWeek could not independently corroborate the Russian ties" (Epstein & Elgin 2008).

When ROSAT was stuck in safe mode in September 1998, Talleur noted that this accident coincided with the intrusions into the Goddard systems controlling it. In other words, he believed that the previous breaches were conducted for intelligence gathering purposes and the targeting of ROSAT was the mission's culmination. According to Epstein, Talleur's advisory stated that "operational characteristics and commanding of the ROSAT were sufficiently similar to other space assets to provide intruders with valuable information about how

[12] X-ray telescopes are designed to observe, detect, and resolve X-rays from sources outside Earth's atmosphere.

such platforms are commanded" (Epstein & Elgin 2008). As Epstein explains, "put differently, manipulating ROSAT could teach an adversary how to toy with just about anything the U.S. put in the sky" (Epstein & Elgin 2008).

With Talleur's report still classified, we are unable to grasp whether the connections he drew make technical sense or whether they are purely speculative. As such, many questions remain unanswered, such as: Did the adversary gain access to Goddard in September to take over the satellite flight controls? Or did they send a command to the satellite from outside Goddard, by cloning the signal (i.e., cracked encryption)? Similarly, how does ROSAT's earlier malfunction in April fit into Talleur's analysis? Was there a breach at Goddard in April?

Time will tell whether we will ever get to know whether an adversary (the "Russians") successfully repurposed breached NASA data to gain control over ROSAT, or whether the intrusions and the satellite's malfunctions were entirely unrelated.

Until then, it might not be very prudent to hold up ROSAT as an example of a destructive cyberattack against a satellite, without also including an explanation on the uncertainties and assumptions surrounding the case.

3.3 1999 Skynet Ransom

Sometime in late-February 1999, the Sunday Business – a Sunday newspaper in the UK – broke the news that one of Skynet's military communication satellites belonging to the UK Ministry of Defense was supposedly hacked and held for ransom. According to the story, the British aerospace authorities had noticed an irregularity in the position of one of Skynet's satellites two weeks earlier. Shortly thereafter, an anonymous ransom message was received (by someone somewhere), that demanded money to stop the interference with the satellite. Sunday Business went on to quote several anonymous sources, including an "intelligence source" and a "security source" who noted that "this is a nightmare scenario" and that "this is not just a case of computer nerds mucking about. This is very, very serious, and the blackmail threat has made it even more serious" (Chicago Tribune 1999).

The incident is referenced in numerous research papers and tech talks on satellite security, but did it actually happen?

While the author of this report was unable to locate the original Sunday Business article – they went out of business in 2006 and are not digitalized in the British Newspaper Archive – there was enough detail picked up by other news organizations such as Reuters and the Chicago Tribune – that reference the Sunday Business article – to roughly piece it together (Reuters 1999; Chicago Tribune 1999). At a minimum we do know that the article did exist.

We also know what followed thereafter. The BBC picked up the report on 2 March 1999, quoting an MoD official saying that, "the story is complete nonsense. All our satellites are where they should be and doing what they should be doing. It's all systems go" (BBC 1999). CNET reported on it on 3 March, quoting a UK MoD spokeswoman – who declined to give her name – stating that, "the satellite system has not been hacked into and the satellite has not changed course […]. And, the security levels make it extremely difficult, if not impossible, to hack into the system" (Grice 1999).

The New Scientist also cites an MoD spokesman in its reporting on 6 March, saying that "all our satellites are on course and we've had no problems at all" (The New Scientist 1999).

The clue that might help unravel the story is most likely found on the law enforcement side. The New Scientist reached out to Scotland Yard who confirmed that "officers from the Metropolitan Police Force Fraud Squad are investigating an allegation of a hacker who is believed to be targeting several different international sites some of which may include military installations" (The New Scientist). In fact, ZDNet's Jane Wakefield cites an MoD spokesman in her 1 March article that "believes the story has been confused with a current Scotland Yard investigation" (Wakefield 1999). The MoD spokesman goes on to note that "the Fraud Squad are investigating a hacker who is accessing international sites but it has nothing to do with the MOD" (Wakefield 1999).

According to ZDNet, the Hacker News Network reported that the Sunday Business story should be treated as "extremely suspect until it can be verified by a second source" (Wakefield 1999).

Despite the responsible reporting by some outlets at the time, the Sunday Business story is still being referenced by academics, journalists, and policymaker 20 years later, as if a Skynet satellite was actually held for ransom.

3.4 International Space Station

From time to time, systems on the International Space Station do get infected by malware.

In 2008 for example, the W32.Gammima.AG worm was detected on one laptop, which was most likely infected by a digital camera storage card brought onto the station (Keizer 2008). According to NASA' daily status reports, ISS personnel regularly runs anti-virus checks on USB drives and the various station laptops (such as payload laptops and Auxiliary Computer System laptops) (NASA 2013; NASA 2018; NASA 2020). According to NASA spokesman Kelly Humphries, the worm "was never a threat to any command-and-control or operations computer" (Keizer 2008). Graham Cluley, then senior technology consultant at Sophos, put the Gammima infection into perspective by stating that, “[i]f there is any good news at all, it's that the malware was designed to steal usernames and passwords from computer game players, not something that orbiting astronauts are likely to be spending a lot of time doing” (Cluley 2008).

In 2010, NASA provided the ISS with access to the Internet via a satellite link that connects to a computer in Houston in remote desktop mode. As NASA explains it, “the crew will view the desktop of the ground computer using an onboard laptop and interact remotely with their keyboard touchpad” (NASA 2010a). As Kaspersky’s Igor Kuksov correctly notes, “it is safer that way: even if a malicious link or file is opened by an ISS crew member, only the ground computer will be compromised” (Kuksov 2019).

According to TASS, the Russian segment of the ISS will get its own separate Internet connection by the end of 2020 (TASS 2020). The Russians will use their Luch relay satellites to connect to a broadband communication channel on Earth (TASS 2020). Open-source reporting is unclear whether they will also connect to a remote desktop, or whether this will be a direct feed. Time will tell whether, and when, the first malware product will worm its way from the open Internet aboard the ISS.

In 2013, Eugene Kaspersky made a few waves during his presentation at the Canberra Press Club by noting that “scientists, from time to time, they are coming to space with USBs which are infected. I'm not kidding. I was talking to a Russian space guys and they said from time to time there are virus epidemics in the space station” (Leyden 2013). Several journalists not only jumped on the virus epidemic bandwagon, but also misunderstood Kaspersky’s comments when he brought up Stuxnet. Several media outlets, including Vice, The Atlantic, Extreme Tech, and the Times of Israel, started churning out headlines such as “Stuxnet, America's Nuclear Plant-Attacking Virus, Has Apparently Infected the International Space Station" (Wagenseil 2013). As Paul Wagenseil correctly clarified, “Kaspersky never said Stuxnet had infected the International Space Station (ISS). Rather, he offered two separate and unrelated anecdotes” (Wagenseil 2013). Similarly the Atlantic published a correction saying “this article originally said the ISS was infected with Stuxnet. Upon further review of Kaspersky's statements, that's not the case. We're sorry for the confusion” (Simpson 2013).

In this context it is worth noting that the Mir space station also faced its fair share of computer viruses – and it has not always been the Russians’ fault. In October 1997, NASA inadvertently spread a macro virus (think MS Office products) from “Houston to Moscow, and infected the workstations that are used for Mir space station ground control including daily communication with the Mir Crew” (Perillo 1998). According to Jeffrey Cardenas, then NASA’s Mir operations and training manager, the virus was not caught by anti-virus software in the US or Russia, and subsequently corrupted several e-mail messages (Harreld 1997). Out of fear of spreading the virus further, Houston and Moscow avoided the use of e-mail attachments and switched to using fax. On 17 October, the virus was purged from all systems. Henry Hertzfeld, then senior research scientist at George Washington University's Space Policy Institute, noted that this may be one of the first examples of a mishap of American origin associated with the Mir mission (Harreld 1997).

3.5 2007/08 US Gov. Satellite Hack

In 2011, the annual report of the Congressional U.S.-China Economic and Security Review Commission, disclosed for the first time two separate incidents in 2007 and 2008 as examples of malicious cyber activities directed against US satellites (USCC 2011, p. 216).

According to the report, the Landsat-7 US earth observation satellite “experienced 12 or more minutes of interference” on 20 October 2007. Nine months later, the same satellite again “experienced 12 or more minutes of interference” on July 23 2008. According to the Commission, the “responsible party did not achieve all steps required to command the satellite” (USCC 2011, p. 216).

In contrast, on 20 June 2008, the Terra EOS AM-1 US Earth observation satellite experienced “two or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands.” Four months later, Terra EOS AM-1 experienced “nine or more minutes of interference. The responsible party achieved all steps required to command the satellite but did not issue commands” (USCC 2011, p. 216).

While the Commission did note that authoritative Chinese military writings advocated for exploitations or attacks against ground-based infrastructure, space-based systems, or the communications links between the two, it did not explicitly attribute the satellite incidents to the Chinese. However, subsequent media coverage on the report glanced over these discrepancies, with even Reuters running the headline “China key suspect in U.S. satellite hacks” (Wolf 2011). Kim Zetter, reporting for Wired, on the other hand put things into context by highlighting that, “the report, as is typical of ones published by the U.S.-China commission, suggests that China is behind the attacks but provides little evidence to support this, other than noting that Chinese military writings have advocated disabling ‘ground-based infrastructure, such as satellite control facilities’” (Zetter 2011).

The curious part is, that the Commission's draft report – whose excerpts were circulated to journalists – included a reference that the hackers gained access to the two satellites through the Svalbard Satellite Station (SvalSat) in Spitzbergen, Norway, which "routinely relies on the Internet for data access and file transfers" (Zetter 2011; Wolf 2011). Although the SvalSat reference is absent in the final report, John Leyden from The Register followed up on the clue by reaching out to Kongsberg Satellite Services (KSAT), which runs SvalSat (KSAT, n.d.).

According KSAT's statement, "KSAT has not experienced any attempt to enter into the company's systems from outside sources. Furthermore, KSAT does not have any indication that hacking of satellites using the KSAT Svalbard station has taken place. A careful screening of our security systems has not indicated any attempts to access SvalSat from unauthorized sources. We have not received any message from NASA that their satellites were hacked. To our knowledge, NASA has not observed any external, unauthorized access to their satellites" (Leyden 2011). Additionally, a KSAT spokesman noted that the hacking allegations were "unsubstantiated and no evidence has been found" (Leyden 2011). And speaking to Reuters, KSAT president Rolf Skatteboe stated that "our systems indicate nothing […] we don't understand where this is coming from" (Wolf 2011).

3.6 2014 NOAA Webserver

Back in late-September 2014, a (suspected Chinese) threat actor breached a server that hosted four websites belonging to the National Weather Service (NWS) (Flaherty et al. 2014). The NWS is part of the National Oceanic Atmospheric Administration (NOAA), which in turn is part of the US Commerce Department. In violation of the Commerce Department's policy, NOAA did not report the security incident within two days of discovery. Instead, under the cover of "unscheduled maintenance," NOAA tried to mitigate the incident by taking the National Ice Center offline for over a week, as well as shutting down other satellite-based weather data feeds – whose application is used for tracking storms, temperature, and other weather systems across the globe to inform disaster planning, aviation weather forecasts, maritime shipping navigation, and other crucial tasks (Osborne 2014).

On 4 November, NOAA finally informed the Commerce Department. One week later, the Washington Post reported on the incident, stating that "NOAA officials would not say whether the attack removed material or inserted malicious software in its system, which is used by civilian and military forecasters in the United States and also feeds weather models at the main centers for Europe and Canada" (Flaherty et al. 2014).

In a statement to Business Insider, NOAA spokesperson Scott Mullen noted that "NOAA staff detected the attacks and incident response began immediately. Unscheduled maintenance was performed by NOAA to mitigate the attacks. The unscheduled maintenance impacts were temporary and all services have been fully restored. These effects did not prevent us from delivering forecasts to the public" (Loria 2014).

The last point does not necessarily reflect the whole truth as CNN, for example, quoted climatologist David Robinson over at Rutgers Global Snow Lab saying that, "we were shut out entirely. That's our one source of data" (Pagliery 2014). Equally, the Washington Post interviewed Stephen English, head of the satellite section at the European Center for Medium-Range Weather Forecasts in the UK, saying that "all the operational data sent via NOAA, which is normally an excellent service, was lost" (Flaherty et al. 2014). Commercial entities were also affected by the "unscheduled maintenance." According to Delta Airlines spokesperson Morgan Durrant, Delta overcame the loss of data – which it normally incorporates into pilot briefings on aviation hazards – by relying on its own meteorologists and information technology specialists, who used alternative sources of information (The Day 2014).

On top of all this, the NOAA incident also included a murky attribution claim that remains unsubstantiated to this day. According to the Washington Post, "NOAA confirmed to Rep. Frank Wolf (R-Va.) that China was behind the attack" (Flaherty et al. 2014). As Rep. Wolf put it, "NOAA told me it was a hack and it was China" (Flaherty et al. 2014). However, no other member of Congress nor any other US government agency has since come forward to support NOAA's purported attribution to China.

Furthermore, the cybersecurity problems at NOAA did not fall from the sky. In fact, the Department of Commerce's OIG released a report in mid-July 2014, which highlighted numerous significant security deficiencies in NOAA's information systems. Among other items, the OIG pointed out that, "specifically, our review of each system's vulnerability scans found that: The [Polar-orbiting Operational Environmental Satellites] POES, [Geostationary Operational Environmental Satellites] GOES, and [Environmental Satellite Processing Center] ESPC have thousands of vulnerabilities, where some of the vulnerabilities in the software have been publicly disclosed for as long as 13 years. […] ESPC and POES have not remediated 24 percent and 50 percent, respectively, of the high-risk vulnerabilities identified by the OIG's FY 2010 vulnerability scans" (OIG DoC 2014, p. 10).

The four National Environmental Satellite, Data, and Information Service (NESDIS) systems did also not enforce the Department's prohibited use of personal computers for remotely accessing information systems. According to the OIG, in FY2013 "an attacker exfiltrated data from a NESDIS system to a suspicious external IP address via the remote connection established with a personal computer. The NOAA Computer Incident Response Team determined that the personal computer was likely infected with malware, but NOAA could not pursue the investigation because it involved a personal device, not government equipment (i.e., the owner of the personal computer, even though a NESDIS contractor, did not give NOAA permission to perform forensic activities on the personal computer)" (OIG DoC 2014, p. 12).

Even more curious was the OIG's finding that POES is "actually interwoven with U.S. Air Force's (USAF) Defense Meteorological Satellite Program (DMSP) to the point where they are virtually one system" (OIG DoC 2014, p. 3). The OIG goes on to note that "unfortunately, because USAF and NOAA disputed for several years (from 2006 to 2010) who was responsible for DMSP's security, neither organization conducted security assessments of DMSP. Ultimately, USAF and NOAA determined in 2010 that USAF was responsible for DMSP. However, USAF has yet to fulfill its responsibilities by determining DMSP's security posture and ensuring that the system meets the Department's security requirements" (OIG DoC 2014, p. 3).

Five of the six examples listed in this section have outlined the problems in reporting about cyber incidents and subsequently getting a firm grasp of the cyber threat landscape pertaining to various satellites, the ISS, and webservers back on Earth. Incidents are naturally complex and have moving parts that cannot be fully covered and understood when they occur. As such, going back to separating fiction from reality is a necessity to fully comprehend what kind of incidents have and have not (yet) occurred.

While this does not mean that similar threats and incidents cannot emerge in the future, it does reveal that the most-referenced cyber incidents affecting space system have either not occurred at all, are based on a series of assumptions, or did not occur in the manner they were initially reported.

To outline how difficult it is to actually hack and maintain control over a satellite, the next section looks at DEFCON's 2020 hack-a-sat challenge.

4 DEFCON Hack-A-Sat 2020

Following the success of last year's DEFCON Aviation village, which allowed outside hackers for the first-time ever to probe for weaknesses in a fourth-generation jet fighter's Trusted Aircraft Information Download Station (known as TADS), the USAF, in cooperation with the Defense Digital Service (DDS), upped their game for DEFCON 2020 (Pawlyk 2019). While the persistence of the coronavirus pandemic forced the Aviation Village to be held remotely, the Space Security Challenge aka Hack-A-Sat that the DDS and USAF conceived, provided the hacker community with access to a satellite in a way that they never had before.

To qualify for Hack-A-Sat, the 2,213 teams (around 6,000 competitors) that registered for the challenge had to score points across 32 capture the flag exercises that tested their knowledge and persistence on everything from orbital mechanics, star tracking, and navigation, to flight software and hacking satellite applications over message buses (Hackasat 2020a; Hackasat 2020b; Hackasat 2020c).

The eight highest-scoring teams were invited to the main event on 7 August, which included six challenges. Five of those challenges revolved around a FlatSat carousel mock-up located in Florida that was accessible to the teams via VPN. A FlatSat is essentially a rudimental motherboard tabletop on which hardware and software components are installed upon as if they were inside of a real satellite in orbit. The last challenge consisted of an on-orbit challenge, the most accurate solution to which was submitted to an actual satellite in space.

To provide more context to the challenge's evolving story and complexity, it is worth quoting the narratives for each challenge in full.

Challenge 0: "An adversary has obtained access to the satellite's ground station. Once they have obtained access, they kick us out. The challenge: Teams must obtain network access to the ground station" (AFResearch Lab 2020a).

Challenge 1: "Having access to the ground station means we can attempt communication, but the satellite is spinning out of control, which complicates everything. The challenge: Teams must regain communication with the satellite" (AFResearch Lab 2020b).

Challenge 2: "The satellite is spinning out of control because the guidance, navigation, and control system or GNC is inoperable. We suspect sabotage. The challenge: Teams must repair the GNC system as quickly as possible to stop the dangerous spinning" (AFResearch Lab 2020c).

Challenge 3: "With the repair complete on the GNC, the satellite has stopped spinning. But we can't still communicate with the payload module or operate the imager. We have to ask ourselves, 'what else did they damage on this satellite?' The challenge: Teams must restore communication with the payload module so we can get it working again" (AFResearch Lab 2020d).

Challenge 4: "We restored communication with the payload module, but we still can't operate it. The Challenge: Now teams must restore normal operations of the payload module so we can access the imager" (AFResearch Lab 2020e).

Challenge 5: "We've done our best work and it seems we have regained control over the satellite. But how do we know for sure? The challenge: Teams must prove that we are fully in control of the satellite system by imaging the Moon" (AFResearch Lab 2020f).

For the fifth challenge – the on-orbit challenge – teams had to come up with a mission plan that fulfilled three key criteria. First, the commands had to be generated in the correct order and within the specified period. Second, the image capture angle of the Moon is within specifications. And third, the team's negative Z-axis is pointed as close to the Earth's center as possible without affecting the camera-to-Moon pointing error.

The on-orbit challenge was the most complex as it brought together all necessary steps to hack, control, and keep a satellite secure. As Hack-A-Sat explains, "the on-orbit challenge was completed with full thrust. Our satellites rely on data and sensors from multiple sources in order to complete an objective. The [two-line element set] that was provided relied on data from the satellite and ground stations.[13] Authenticated communications were required to upload the proper command sequence. Trusted execution was required to process sensor and actuary data to close control loop. [And] secure onboard communications were required to carry out operations in orbit" (AFResearch Lab 2020g).

In the end, team PFS came out on top, while Team 'Poland can into space' delivered the most accurate solution for the on-orbit challenge (AFResearch Lab 2020h). This was a rather amazing outcome for PFS, as some of their members had no knowledge about how much infrastructure was unique to satellites before they signed up to the challenge. Interviewed by Wired, PFS member Cyrus Malekpour, for example, explained how he parsed archival NASA white papers to figure out what a "star tracker" actually was. Similarly, PFS member Demarcus Williams noted that "the space part threw a wrench in stuff […] I wasn't familiar with the terminology, the math required" (Scoles 2020).

Overall, Hack-A-Sat was all about learning from each other and building new relationships. The DEFCON community gained first-hand experience in the vast special knowledge required to hack and control a satellite and its ground infrastructure, while the Pentagon learned how to better secure its satellites as they are being designed. Time will tell what the next Aviation Village at DEFCON 2021 will bring and whether the community's interest in satellite hacking will gain traction in the months and years ahead.[14] For the moment though, Hack-A-Sat was an unprecedented opportunity for the hacking community that might serve as a starting point to spur the thinking on cybersecurity in space within DoD and elsewhere around the world.

5 Implications for Switzerland

From the perspective of the Swiss National Cybersecurity Strategy 2018-2022, the space economy at large and Swiss dependencies on space-based infrastructure are of vital interest to the federal government and the 26 cantons. Yet, similarly to the problems faced by the EU on European critical infrastructure, and the US on creating a dedicated CI sector for the space industry (section 1.1), the fragmented nature of Swiss space industries and the absence of space-based assets owned by Switzerland have so far prevented the emergence of a holistic cybersecurity approach for the Swiss space economy.

For such a policy to take root, the federal government would be well-advised to first comprehensively map out current Swiss space dependencies and available redundancies across the existing nine CI sectors and 27 sub-sectors identified by the Federal Council (BABS, n.d.).[15] Second, it would do well to also map the reverse logic and look at hypothetical cyber incidents occurring outside of Swiss territory that might cascade and touch Swiss CI in the event that one or several satellites were to fail (e.g., ROSAT), ground stations exhibit persistent communication problems (e.g., Galileo), or web servers that disseminate crucial space data go offline for a longer period of time (as was the case with NOAA).

Once this mapping has been completed, the answer as to whether Swiss dependencies on space infrastructure and services are exposed to a major risk or a minor one will become much clearer.

[13] A two-line element set, or TLE, is "a data format that contains information about an objects position and velocity at a specific point in time. It is used to calculate where a satellite will be at some point in the future – with increasing uncertainty the further out in time." See: AFResearch Lab 2020g @ 0:06-0:20.

[14] If Will Roper, Assistant Secretary of the Air Force for Acquisition, Technology and Logistics, picks up on his other plan from 2019, DoD might bring hackers to Nellis or Creech Air Force Base where they can probe systems in a military plane (or drone?). See: Marks 2019.

[15] This mapping exercise could also include small and medium enterprises that are part of the space economy but do not fulfill the criteria to be considered critical infrastructure.

Apart from mapping out dependencies and cascading effects, the federal government would also be well-advised to follow the EU debate on European critical infrastructure – pertaining to the space sector – as it will most likely affect ESA and Galileo to one degree or another. It might even be prudent for the federal government to proactively seek out engagement with the European Commission and coordinate with other ESA members on this very subject. Maybe such a Swiss initiative might be able to shape and align EU standards and procedures with Swiss interests, particularly when it comes to securing, reporting, and mitigating incidents in European critical infrastructure. Similarly, the federal government ought to keep an eye on the US debate on a CI sector dedicated to the space economy, as it might envelop RUAG and other Swiss companies within the US space sector supply chain.

In the event of a clash between the regulatory approaches of the EU and the US, the fallout could make things difficult for Swiss and other third-country companies.

In the context of the European Space Agency, the Swiss government and other member state governments would do well to open up the debate on the Agency's cybersecurity posture and threat environment. Currently, very little is known as to what major cybersecurity incidents the Agency has been dealing with in the past and what the outcomes were of ESA's investigations. As the case of the potential hardware manipulation (p.10) and the handling of the Galileo outage (p.20) have shown, a lack of communication and transparency can result in the spread of rumors and a discernable reduction in trust in the Agency.

Given that ESA does not have federal agents like NASA's OIG that actively hunt down cybercriminals and other threat actors across the globe, it might be prudent to think about whether standing up a joint cyber task force – comprising law enforcement, intelligence, and military officers from the various ESA member countries – would be an appropriate tool to proactively tackle incidents affecting the Agency as the space race is heating up.

On the subject of whether the Swiss Defense Department ought to build its own satellites, the federal government has to decide whether a solely fiscal point of view can adequately take into account the increasingly political uncertainties in times of great power rivalry and the ongoing space race to saturate Earth's orbits (RTS 2018). In the opinion of this author, independent satellite capabilities and available third-party redundancies are the cornerstone of a prudent defense policy to keep Switzerland safe on the journey ahead.

Swiss government departments and companies might also want to closely follow the European Commission's plan on exploring the build-up of a European satellite communication system. On 23 December 2020, the Commission made the crucial step of selecting a consortium of European satellite manufacturers, operators and service providers, telco operators, and launch service providers to study the design, development, and launch of such a European-owned space-based communication system (Airbus 2020). The consortium members are: Airbus, Arianespace, Eutelsat, Hispasat, OHB, Orange, SES, Telespazio, and Thales Alenia Space. As of this writing, it is unclear whether Swiss companies will be able to feed into the study and/or join the consortium at a later stage. It is also unclear whether the Swiss government can become a partner nation in this process, given that the system will be built upon the EU's GOVSAT program, which is specifically aimed at "providing secure and cost-efficient communications capabilities to security and safety critical missions and operations managed by the European Union and its Member States, including national security actors and EU Agencies and institutions" (GSA, 'GOVSATCOM').

Overall, however, Switzerland is not well positioned to significantly steer the debate on securing the fragmented space economy by itself. It needs to engage like-minded partners and insert relevant policy ideas and technical know-how into the ensuing debates in Europe and the US to stake out its political aims and vision for the future in space and cyberspace.

One approach to do so would be for Switzerland – particularly the Defense Department, RUAG, and Armasuisse – to partner up with selected European or US counterparts to pick up on the success of Hack-A-Sat and advance a series of hacking challenges pertaining to the space economy across Europe and the US. This way, Switzerland can help secure third-party space infrastructure it currently depends on, and it will be able to engage the European and US hacking community, as well as learn about attack methodologies and how to better secure satellite infrastructure now and in the future.

Another approach would be to insert a much-needed reality check on the threat landscape facing the space economy. If done well, the mapping exercise mentioned previously in this section could serve as a blue print for other nations to adopt and help map out their risk exposure and available redundancies. Similarly, Switzerland might want to serve as a neutral arbiter that collects information and investigative reports about past cases affecting the space economy to paint a realistic picture of what actually occurred (excluding attribution claims). As outlined in section 3, the current gap between reality and fiction is particularly wide when it comes to cyber incidents affecting satellites, ground stations, and web servers. A comprehensive and structured revisiting of past cases by a Swiss government department will most likely also spur a reflection on how past incidents were covered by the media and were able to proliferate throughout the information security and policy community, at times relatively unchallenged. Particularly in light of the media coverage of the 2016 RUAG incident, which undermined government investigative procedures in the case, such a public reflection is much-needed so it does not happen the next time around.

Switzerland should also keep an eye out on the legal debates that have and will increasingly occur when it comes to the interception of satellite communications by intelligence agencies and the legal status of data transmitted and hosted in space. The BND's Weltraumtheorie (p.15) was not necessarily as outlandish as the German media portrayed it to be, and it might be picked up by other governments in the years ahead that do not share the same privacy concerns and intelligence collection constraints as imposed by Germany's Federal Constitutional Court.

5.1 Horizon Scanning

In terms of horizon scanning, the discernable lack of publicly available research papers on cybersecurity and the space sector, as well as the absence of public interest in Europe in the future trajectory of the space domain is a serious shortcoming for a healthy strategic debate on how to position Switzerland (and Europe) for the future.

Based on the findings of this report, we can outline three broad trends that will define the space domain and attach it at the hip to the evolution of cyberspace for the years to come.

First, given the accelerating space race, the build-up of satellite Internet broadband constellations will most likely become an essential extension – if not even a dominating part – of cyberspace as we know it. Depending on future user experiences, pricing, and legal challenges, it might well be that Starlink, OneWeb, and Amazon will capture a significant market share currently held by Earth-based broadband vendors. Once this occurs, actors from across the threat spectrum will turn their eyes sky-ward to explore a new promised land.

According to Reddit user Wandering-Coder, who was fortunate enough to beta-test Starlink, "streaming, low-latency video conferencing, and gaming are all completely accessible with this service. Even for the beta, it appears as though they've under-estimated Starlink's capabilities, so I am excited to see it mature" (Brodkin 2020).

Combined with the promise of deploying data centers in space, this could be a game changer that few analysts and governments have even begun to comprehend. Regulatory questions, legal questions, an expanding threat landscape, new vendors with little cybersecurity experience, and a focus on the electromagnetic spectrum will catapult space onto the priority list of governments and the hacking community alike. Planning ahead now, and gaming through various scenarios on the expansion of cyberspace to space, is not only a prudent choice but a fundamental requirement for sensible space and cyber policies to emerge.

Second, the private sector drive to saturate Earth's orbits will force militaries and intelligence agencies around the globe to attach themselves to these new constellations (hybridization) and/or create their own high-refresh rate satellite infrastructure in space (i.e., splitting up functionalities across multiple smaller satellites). While this evolution will likely strengthen resilience in space, it will also make commercial constellations a much more attractive target for nation-state adversaries and will most likely enable the targeting of small high-refresh rate satellites without incurring the same military or political response as targeting a large low-refresh rate satellite would have theoretically elicited in the past.

Time will tell how these targeting dynamics will play out on the nation-state level and to what degree and when exactly non-US commercial entities will start making their move to compete in space.

In the improbable instance of US companies successfully maintaining their dominance in space, the world could experience a repeat of the early days of the Internet and US regulatory and policy dominance on satellite broadband Internet for decades to come. If the trio of US space broadband giants exert their dominance in space, the continental Europeans will be boxed out of yet another area of technological competition and most likely be forced to turn to a regulatory approach to carve out opportunities for European companies. An approach that will be seen by many in Washington as another example of European companies being unable to compete in the digital realm without government intervention.

Third, the build-up of space infrastructure will also have consequences for the data backend on Earth (think data centers, ground stations, SNPs, etc.). With more and more data being generated and transmitted through space-based infrastructure, the sheer data volume and realignment of information streams will open up new attractive targets on Earth and new attack vectors that have so far not been on the priority list of many adversaries. This trend will most likely also affect supply chains and will kick off a discussion on reliable suppliers in the long run.

6 Conclusion

This report has taken the reader on a journey starting from the vastness of the policy space surrounding critical infrastructure, to the logics of targeting ground stations, data centers, and assets in space, to the cybersecurity problems at NASA, and numerous satellite hacking incidents frequently referenced that actually never occurred as often publicly described. It ended on the high note of the Hack-A-Sat challenge – which will hopefully provide a blueprint for other government agencies and countries to practically engage their hacking communities – and the recommendations for Switzerland.

This report has also shown that there are no quick and easy solutions to defending and securing the space economy. New commercial players with bold visions are currently reshaping the architecture and assets deployed in space. State and non-state actors will adapt to this new environment for better or worse. And with it all comes the inherent uncertainty of what will happen next in this evolutionary transformation of space itself and international politics back on Earth.

This report has tried – and hopefully succeeded – to enlighten the reader on the past, outline the challenges of the present, and open a glimpse to the future ahead.

7 Abbreviations

ADS-B	Automatic Dependent Surveillance – Broadcast
AFB	Air Force Base
AFOSI	US Air Force Office of Special Investigations
AFSC	US Air Force Space Command
AMCS	Attitude Measuring and Control System
APT	Advanced Persistent Threat
BND	Bundesnachrichtendienst (German foreign intelligence service)
BoW	Brotherhood of Warez
C&C	Command and Control
CERT-EU	Computer Emergency Response Team – European Union
CI	Critical Infrastructure
CISA	US Cybersecurity and Infrastructure Security Agency
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CNO	Computer Network Operation
COTS	Commercial Orbital Transportation Services
CSAR	Combat Search and Rescue
CSE	Canada’s Communication Security Establishment
CSO	Composante Spatiale Optique
CSpOC	Combined Space Operations Center
DARPA	Defense Advanced Research Projects Agency
DDS	Defense Digital Service
DHS	US Department of Homeland Security
DMSP	Defense Meteorological Satellite Program
DoD	US Department of Defense
EC	European Commission
EGNOS	European Geostationary Navigation Overlay Service
EPCIP	European Programme for Critical Infrastructure Protection
ESA	European Space Agency
ESPC	Environmental Satellite Processing Center
FAA	US Federal Aviation Administration
FAPSI	Russia’s Federal Agency of Government Communications and Information
FBI	US Federal Bureau of Investigations
FISMA	Federal Information Security Management Act
FORNSAT	Foreign Communication Satellite
FUD	Fear, Uncertainty, and Doubt
GAO	US Government Accountability Office
GCHQ	UK Government Communications Headquarters
GEO	Geostationary/synchronous Earth Orbit
GNSS	Global Navigation Satellite System
GOES	Geostationary Operational Environmental Satellites
GovCERT.ch	Swiss Government Computer Emergency Response Team
GPS	Global Positioning System
GSA	European GNSS Agency
GSM	Global System for Mobile Communication
GSS	Global Sensor Station
H4GiS	Hackers Against Geeks in Snowsuits
HEO	High Earth Orbit
IG	Inspector General
ISAC	Information Sharing and Analysis Center
ISR	Intelligence, Surveillance, and Reconnaissance
ISS	International Space Station

JPL	Jet Propulsion Laboratory
KSAT	Kongsberg Satellite Services
LEO	Low Earth Orbit
MEO	Medium Earth Orbit
MHS	Menwith Hill Station
MIL-SATCOM	Military Satellite Communications
MoD	Ministry of Defense
MOTS	Man-on-the-side
MPL	Minimum Performance Level
MRI	Magnetic Resonance Imaging
MSP	Managed Service Provider
NAGU	Notice Advisories
NASA	National Aeronautics and Space Administration
NASIRC	NASA Incident Response Center
NESDIS	National Environmental Satellite, Data, and Information Service
NIS	Network Information Security (Directive)
NIST	US National Institute of Standards and Technology
NOAA	the National Oceanic and Atmospheric Administration
NRO	US National Reconnaissance Agency
NSA	US National Security Agency
NWS	US National Weather Service
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OS	Operating System
PNT	Position, Navigation, and Timing
POES	Polar-orbiting Operational Environmental Satellites
RCMP	Canadian Royal Mounted Police
RTOS	Real-Time Operating System
SCADA	Supervisory Control and Data Acquisition
SMC	US Air Force Space and Missile Systems Center
SMS	Short Message Service
SNP	Satellite Network Portal
SOC	Security Operations Center
SSA	Space Situational Awareness
SSC	Swedish Space Corporation
TADS	Trusted Aircraft Information Download Station
TT&C	Telemetry, Tracking & Control
ULS	Up-link Station
USAF	United States Air Force
US-CERT	US Computer Emergency Response Team
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network

8 Bibliography

AFResearch Lab. 'Hack A Sat Challenge 0'. Youtube, August 7, 2020a. https://youtu.be/No76f6g9TlA.

AFResearch Lab. 'Hack A Sat Challenge 1'. Youtube, August 7, 2020b. https://youtu.be/rP59xrh9e_I.

AFResearch Lab. 'Hack A Sat Challenge 2'. Youtube, August 7, 2020c. https://youtu.be/Ji3M_oUeTL8.

AFResearch Lab. 'Hack A Sat Challenge 3'. Youtube, August 8, 2020d. https://youtu.be/tMp3UdNtRFk.

AFResearch Lab. 'Hack A Sat Challenge 4'. Youtube, August 8, 2020e. https://youtu.be/5XmFWec1nB0.

AFResearch Lab. 'Hack A Sat Challenge 5'. Youtube, August 8, 2020f. https://youtu.be/qkUOE2ZQyy4.

AFResearch Lab. 'Hack-A-Sat Final Event Closing Ceremony'. Youtube, August 9, 2020h. https://youtu.be/AcgDDuBP2Zw.

AFResearch Lab. 'Hack-A-Sat On Orbit Challenge Explained'. Youtube, August 8, 2020g. https://youtu.be/uJ6T1Bvq1Mc.

Airbus. 'European Space and Digital Players to Study Build of EU's Satellite-Based Connectivity System'. Airbus, 23 December 2020. https://www.airbus.com/newsroom/press-releases/en/2020/12/european-space-and-digital-players-to-study-build-of-eus-satellitebased-connectivity-system.html.

Akoto, William. 'What Happens When All the Tiny Satellites We're Shooting into Space Get Hacked?' FastCompany, 15 February 2020. https://www.fastcompany.com/90464666/what-happens-when-all-the-tiny-satellites-were-shooting-into-space-get-hacked.

ARISS. 'Contact the ISS'. Amateur Radio on the International Space Station, n.d. https://www.ariss.org/contact-the-iss.html.

Armis. 'Urgent/11'. Armis, 2019. https://www.armis.com/urgent11/.

BABS. 'Die Kritischen Infrastrukturen'. Swiss Federal Office for Civil Protection, n.d. https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html.

Baker, Mike. 'NASA Astronaut Anne McClain Accused by Spouse of Crime in Space'. The New York Times, 23 August 2019. https://www.nytimes.com/2019/08/23/us/astronaut-space-investigation.html.

Baker, Mike. 'Space Crime Allegation Leads to Charges Against Astronaut's Ex-Wife'. The New York Times, 6 April 2020. https://www.nytimes.com/2020/04/06/us/space-crime-allegation-indictment.html.

BBC. 'RAF Menwith Hill: Spy Base Radar Antenna Shelters Approved'. BBC News, 14 August 2019. https://www.bbc.com/news/uk-england-york-north-yorkshire-49348848.

BBC. 'Satellite Hijack "Impossible"'. BBC News, 2 March 1999. http://news.bbc.co.uk/2/hi/science/nature/288965.stm

Bejtlich, Richard. 'SANS Confuses Threats with Vulnerabilities'. TaoSecurity Blog, 26 January 2005. https://taosecurity.blogspot.com/2005/01/sans-confuses-threats-with.html.

Bellamy III, Woodrow. 'New Rule Allows Military Aircraft to Turn Off ADS-B Transmissions'. Aviation Today, 23 July 2019. https://www.aviationtoday.com/2019/07/23/new-rule-allows-military-aircraft-turn-ads-b-transmissions-off/.

Biermann, Kai. 'Eine Vertuschung Namens Weltraumtheorie'. Zeit Online, 24 February 2016. https://www.zeit.de/politik/deutschland/2016-02/bnd-nsa-bad-aibling-weltraumtheorie.

Biermann, Kai, and Holger Stark. 'Merkels Fliegende Augen'. Zeit Online, 14 February 2018. https://www.zeit.de/2018/08/ueberwachung-bnd-satelliten/seite-2.

Biselli, Anna. 'Interne Dokumente Zur Weltraumtheorie: Wie Sich BND Und Kanzleramt Vor Der Öffentlichkeit Fürchteten'. Netzpolitik, 23 May 2016. https://netzpolitik.org/2016/interne-dokumente-zur-weltraumtheorie-wie-sich-bnd-und-kanzleramt-vor-der-oeffentlichkeit-fuerchteten/.

Bliley. 'Spot Beams vs. Wide Beams for Satellite Communications'. Bliley Technologies, 31 October 2017. https://blog.bliley.com/spot-beams-wide-beams-satellite-communications.

Brodkin, Jon. 'SpaceX Starlink Users Provide First Impressions and Unboxing Pictures'. ArsTechnica, 2 November 2020. https://arstechnica.com/information-technology/2020/11/spacex-starlink-beta-tester-takes-user-terminal-into-forest-gets-120mbps/.

BVerfG. 'Leitsätze Zum Urteil Des Ersten Senats Vom 19. Mai 2020 (1 BvR 2835/17)'. Bundesverfassungsgericht, 19 May 2020. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html.

CBC. 'Hacker Charged with Cracking Major U.S. Codes Social Sharing'. CBC News, 4 June 1998. https://www.cbc.ca/news/canada/hacker-charged-with-cracking-major-u-s-codes-1.158980.

CERT-EU. 'Airbus Supply Chain Hacked in a Cyberespionage Campaign - Memo TLP:White'. CERT-EU, 27 September 2019.

https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190927-2.pdf.

Chicago Tribune. 'Hackers Reportedly Seize Control of Military Satellite'. Chicago Tribune, 1 March 1999. https://www.chicagotribune.com/news/ct-xpm-1999-03-01-9903010180-story.html.

Cluley, Graham. 'Computer Worm Strikes International Space Station'. Sophos - Naked Security, 27 August 2008. https://nakedsecurity.sophos.com/2008/08/27/computer-worm-strikes-international-space-station/.

CNET. 'Suspected NASA Hacker Nabbed'. Phrack - Issue 53, 6 April 1998. http://phrack.org/issues/53/14.html.

Cobb, Robert W. 'Cyber Security: The Status of Information Security and the Effects of the Federal Information Security Management Act (FISMA) at NASA - Testimony by the Honorable Robert W. Cobb, Inspector General National Aeronautics and Space Administration, before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census'. US House of Representatives, n.d. https://oig.nasa.gov/congressional/testimony062403.doc.

Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy – The Many Faces of Anonymous*. Verso, 2014.

Costin, Andrei, and Aurelien Francillon. 'Ghost in the Air(Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices'. Blackhat US, 2012. https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf.

CSE. 'Hackers Are Humans Too - Cyber Leads to CI Leads'. Communications Security Establishment Canada, n.d. https://www.documentcloud.org/documents/3911739-Hackers-Are-Humans-Too-Partial-Redacted.html.

DoDIG. 'Air Force Space Command Supply Chain Risk Management of Strategic Capabilities'. US Department of Defense, 14 August 2018. https://media.defense.gov/2018/Aug/16/2001955109/-1/-1/1/DODIG-2018-143_REDACTED.PDF.

Donoghue, Andrew. 'Beyond Lights-Out: Future Data Centers Will Be Human-Free'. DataCenter Knowledge, 19 September 2017. https://www.datacenterknowledge.com/design/beyond-lights-out-future-data-centers-will-be-human-free.

dpaonthenet. 'Wind River Embedded RTOS Chosen for Key Element of European Satellite Navigation System'. Design products & applications, 18 June 2010. http://www.dpaonthenet.net/article/34512/Wind-River-embedded-RTOS-chosen-for-key-element-of-European-satellite-navigation-system.aspx.

DW. 'German Spy Agency BND to Get Its Own Satellite'. Deutsche Welle, 10 November 2016. https://www.dw.com/en/german-spy-agency-bnd-to-get-its-own-satellite/a-36350903.

EC. 'Galileo Incident of July 2019: Independent Inquiry Board Provides Final Recommendations'. European Commission, November 19, 2019b. https://ec.europa.eu/growth/content/galileo-incident-july-2019-independent-inquiry-board-provides-final-recommendations_en.

EC. 'Kick-off of the Independent Inquiry Board on Galileo'. European Commission, September 6, 2019a. https://ec.europa.eu/growth/content/kick-independent-inquiry-board-galileo_en.

EC. 'Protecting Critical Infrastructure in the EU – New Rules'. European Commission, 2020. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Enhancement-of-European-policy-on-critical-infrastructure-protection.

Englhauser, Jakob. 'ROSAT S/C Status 1998-08-31 ... 1998-12-03'. Max Planck Institute for Extraterrestrial Physics, 1998. https://web.archive.org/web/20110511215945/http://www.xray.mpe.mpg.de/~jer/rosat/status/status-980830.html.

Epstein, Keith, and Ben Elgin. 'Network Security Breaches Plague NASA'. Bloomberg BusinessWeek, 20 November 2008. https://www.cs.clemson.edu/course/cpsc420/material/Papers/NASA.pdf.

Erwin, Sandra. 'Space Force Plans Big Reveals on Its First Anniversary'. SpaceNews, 16 October 2020. https://spacenews.com/space-force-plans-big-reveals-on-its-first-anniversary/.

Estes, Adam Clark. 'The Pandemic Is Speeding up the Space Internet Race'. Vox Recode, 26 September 2020. https://www.vox.com/recode/2020/9/26/21457530/elon-musk-spacex-starlink-satellite-broadband-amazon-project-kuiper-viasat.

Etherington, Darrell. 'Amazon Gains FCC Approval for Kuiper Internet Satellite Constellation and Commits $10 Billion to the Project'. TechCrunch, July 31, 2020b. https://techcrunch.com/2020/07/31/amazon-gains-fcc-approval-for-kuiper-internet-satellite-constellation-and-commits-10-billion-to-the-project/.

Etherington, Darrell. 'SpaceX Makes History with Successful First Human Space Launch'. TechCrunch, May 30, 2020a. https://techcrunch.com/2020/05/30/spacex-makes-history-with-successful-first-human-space-launch/.

Etherington, Darrell. 'SpaceX Successfully Launches 60 More Starlink Satellites, Bringing Total Delivered to Orbit to More than 800'. TechCrunch, October 19, 2020c. https://techcrunch.com/2020/10/19/spacex-successfully-launches-60-more-starlink-satellites-bringing-total-delivered-to-orbit-to-more-than-800/?tpcc=ECTW2020.

European Union. ‘Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection’. Official Journal of the European Union, 8 December 2008. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG.

European Union. ‘Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union’. Official Journal of the European Union, 19 July 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

European Union. ‘Regulation (EU) No 1285/2013 of the European Parliament and of the Council of 11 December 2013 on the Implementation and Exploitation of European Satellite Navigation Systems and Repealing Council Regulation (EC) No 876/2002 and Regulation (EC) No 683/2008 of the European Parliament and of the Council’. Official Journal of the European Union, 20 December 2013. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R1285.

FAA. ‘The Annual Compendium of Commercial Space Transportation: 2012’. US Federal Aviation Administration, February 2013. https://www.faa.gov/about/office_org/headquarters_offices/ast/media/Annual_Compendium_of_Commercial_Space_Transportation_2012_February_2013.pdf.

FAA. ‘The Annual Compendium of Commercial Space Transportation: 2018’. US Federal Aviation Administration, January 2018. https://www.faa.gov/about/office_org/headquarters_offices/ast/media/2018_AST_Compendium.pdf.

Fabio, Adam. ‘GPS and ADS-B Problems Cause Cancelled Flights’. Hackaday, 9 June 2019. https://hackaday.com/2019/06/09/gps-and-ads-b-problems-cause-cancelled-flights/.

Falco, Gregory. ‘When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience’. ResearchGate, November 2020. https://www.researchgate.net/publication/340335070_When_Satellites_Attack_Satellite-to-Satellite_Cyber_Attack_Defense_and_Resilience.

Ferrone, Kristine. ‘Majority of Satellites Exceed Design Life’. Aerospace, 6 December 2019. https://aerospace.org/getting-it-right/dec-2019/satellite-design-life.

Flaherty, Mary Pat, Jason Samenow, and Lisa Rein. ‘Chinese Hack U.S. Weather Systems, Satellite Network’. The Washington Post, 12 November 2014. https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.

Forbes, Stephen. ‘Blackjack’. DARPA, n.d. https://www.darpa.mil/program/blackjack.

Forrester, Chris. ‘Russia Buys into OneWeb’. Advanced Television, 26 February 2019. https://advanced-television.com/2019/02/26/russia-buys-into-oneweb/.

Foust, Jeff. ‘OneWeb resumes satellite deployment with Soyuz launch’. SpaceNews, 18 December 2020. https://spacenews.com/oneweb-resumes-satellite-deployment-with-soyuz-launch/.

France24. ‘Airbus Hit by Series of Cyber Attacks on Suppliers’. France24, 26 September 2019. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers.

Fritz, Jason. ‘Satellite Hacking: A Guide for the Perplexed’. *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies* 10, no. 1 (December 2012): 21–59.

Gallagher, Ryan. ‘Inside Menwith Hill’. The Intercept, 6 September 2016. https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/.

GAO. ‘Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks’. US Government Accountability Office, October 2009. https://www.gao.gov/assets/300/296854.pdf.

———. ‘Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft’. US Government Accountability Office, January 2018. https://www.gao.gov/assets/690/689478.pdf.

Georgiou, Aristos. ‘Why Did the Space Shuttle Program End?’ Newsweek, 21 May 2020. https://www.newsweek.com/why-space-shuttle-program-end-1505594.

GMV. ‘OneWeb Awards GMV the Contract to Develop OneWeb’s Satellite Constellation Command and Control’. GMV, 19 December 2016. https://www.gmv.com/en/Company/Communication/News/2016/12/satelites_oneweb.html.

Goodin, Dan. ‘Rise of “Forever Day” Bugs in Industrial Systems Threatens Critical Infrastructure’. ArsTechnica, 10 April 2012. https://arstechnica.com/information-technology/2012/04/rise-of-ics-forever-day-vulnerabiliities-threaten-critical-infrastructure/.

GovCERT.ch. ‘APT Case RUAG – Technical Report’. 23 May 2016. https://www.govcert.ch/downloads/whitepapers/Report_Ruag-Espionage-Case.pdf.

Greenberg, Andy. ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’. Wired, 22 August 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greive, Martin, and Thorsten Jungholt. ‘Von Der Leyens „katastrophaler“ Satelliten-Deal’. Welt, 5 April

2015. https://www.welt.de/politik/deutschland/article139136852/Von-der-Leyens-katastrophaler-Satelliten-Deal.html.

Grice, Corey. 'Satellite Hack Raises Security Questions'. cnet, 3 March 1999. https://www.cnet.com/news/satellite-hack-raises-security-questions/.

GSA. 'Constellation Information'. European Global Navigation Satellite Systems Agency, n.d. https://www.gsc-europa.eu/system-service-status/constellation-information.

GSA. 'Galileo Initial Services'. European Global Navigation Satellite Systems Agency, 30 October 2018. https://www.gsa.europa.eu/galileo/services/initial-services.

GSA. 'GOVSATCOM'. European Global Navigation Satellite Systems Agency, n.d. https://www.gsa.europa.eu/govsatcom.

GSA. 'Update on the Availability of Some Galileo Initial Services'. European Global Navigation Satellite Systems Agency, 14 July 2019. https://www.gsa.europa.eu/newsroom/news/update-availability-some-galileo-initial-services.

GSC. 'European GNSS (Galileo) Initial Services - Open Service Quarterly Performance Report July - September 2019'. European GNSS Sevice Center, n.d. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo-IS-OS-Quarterly-Performance_Report-Q3-2019.pdf.

Hackasat. 'All Challenges'. Hackasat, 2020a. https://quals.2020.hackasat.com/challenges.html.

Hackasat. 'Stat Dump for Space Security Challenge 2020: Hack-A-Sat Qualifiers'. Hackasat, 2020b. https://quals.2020.hackasat.com/teams.htm.

Hackasat. 'FAQs'. Hackasat, September 9, 2020c. https://www.hackasat.com/faqs#qual-event.

Harreld, Heather. 'Virus Infects Communications with Mir'. FCW, 19 October 1997. https://fcw.com/articles/1997/10/19/virus-infects-communications-with-mir.aspx.

Hay Newman, Lily. 'An Operating System Bug Exposes 200 Million Critical Devices'. Wired, 29 July 2019. https://www.wired.com/story/vxworks-vulnerabilities-urgent11/.

Henry, Caleb. 'After Bankruptcy, OneWeb's Supply Chain Looking for New Ways to Keep Busy'. SpaceNews, April 20, 2020a. https://spacenews.com/after-bankruptcy-onewebs-supply-chain-looking-for-new-ways-to-keep-busy/.

Henry, Caleb. 'British Government and Bharti Global Buy OneWeb, Plan $1 Billion Investment to Revive Company'. SpaceNews, July 3, 2020b. https://spacenews.com/british-government-and-bharti-global-buy-oneweb-plan-1-billion-investment-to-revive-company/.

Hitchens, Theresa. 'Securing The Space Cloud: It's Really Hard'. BreakingDefense, 10 May 2019. https://breakingdefense.com/2019/05/securing-the-space-cloud-its-really-hard/.

Hitchens, Theresa. 'Under Senate's Eye, NRO, NGA Stress Commercial Imagery Plans'. BreakingDefense, 9 July 2020. https://breakingdefense.com/2020/07/under-senates-eye-nro-nga-stress-commercial-imagery-plans/.

Hubert, Bert. 'The July Galileo Outage: What Happened and Why'. berthub.eu, 7 November 2019. https://berthub.eu/articles/posts/galileo-accident/.

Hughes. 'Hughes Becomes First Satellite Internet Provider to Surpass One Million Active Users'. Hughes, 8 September 2014. https://www.hughes.com/resources/press-releases/hughes-becomes-first-satellite-internet-provider-surpass-one-million.

IG. 'Galileo Issues Q3 2019 Performance Report Covering Outage Period'. Inside GNSS, 31 January 2020. https://insidegnss.com/galileo-issues-q3-2019-performance-report-covering-outage-period/.

IG. 'Lessons to Be Learned from Galileo Signal Outage'. Inside GNSS, 1 October 2019. https://insidegnss.com/lessons-to-be-learned-from-galileo-signal-outage/.

Ingenieur.de. 'Deutschland Beteiligt Sich Doch an Französischen Spionagesatelliten'. Ingenieur.de, 31 March 2015. https://www.ingenieur.de/technik/fachbereiche/ittk/deutschland-beteiligt-an-franzoesischen-spionagesatelliten/.

ION. '2019 – Galileo Programme Update'. Institute of Navigation, 2019. https://www.ion.org/publications/abstract.cfm?articleID=16900.

JAXA. 'JEM Small Satellite Orbital Deployer (J-SSOD)', n.d. https://iss.jaxa.jp/en/kiboexp/jssod/.

Johnson, David B. 'Satellite Coverages and Orbits'. National Center for Atmospheric Research, 6 July 1996. https://ral.ucar.edu/~djohnson/satellite/coverage.html

Kaspersky, Eugene. 'The Man Who Found Stuxnet – Sergey Ulasen in the Spotlight'. Kaspersky, 2 November 2011. https://eugene.kaspersky.com/2011/11/02/the-man-who-found-stuxnet-sergey-ulasen-in-the-spotlight/.

Keizer, Gregg. 'Malware Infects International Space Station (ISS) Laptops'. CIO, 28 August 2008. https://www.cio.com/article/2434006/malware-infects-international-space-station--iss--laptops.html.

Krebs, Brian. 'Arrest of Chinese Hackers Not a First for U.S.' KrebsonSecurity, 13 October 2015. https://krebsonsecurity.com/2015/10/arrest-of-chinese-hackers-not-a-first-for-u-s/.

Krywko, Jacek. 'Definitely Not Windows 95: What Operating Systems Keep Things Running in Space?' ArsTechnica, 2 November 2020. https://arstechnica.com/features/2020/10/the-space-operating-systems-booting-up-where-no-one-has-gone-before/.

KSAT. ‘Ground Station Services’. Kongsberg Satellite Services, n.d. https://www.ksat.no/services/ground-station-services/.

Kujur, Birendra, Samer Khanafseh, and Boris Pervan. ‘Detecting GNSS Spoofing of ADS-B Equipped Aircraft Using INS’. IEEE Xplore, 8 June 2020. https://ieeexplore.ieee.org/abstract/document/9109966.

Kuksov, Igor. ‘Internet in Space: Is There Net on Mars?’ Kaspersky, 13 September 2019. https://www.kaspersky.com/blog/internet-in-space/28267/.

Leonard, Matt. ‘DARPA Looks for Better Satellite Security’. Defense Systems, 27 April 2018. https://defensesystems.com/articles/2018/04/27/darpa-satellite-communications-encryption.aspx.

Leonardo. ‘Athena-Fidus’. Leonardo, n.a. https://www.leonardocompany.com/en/products/athena-fidus.

Lewis, Jeffrey. ‘Is the United States Really Blowing Up North Korea’s Missiles?’ Foreign Policy, 19 April 2017. https://foreignpolicy.com/2017/04/19/the-united-states-isnt-hacking-north-koreas-missile-launches/.

Leyden, John. ‘Inside the Mysterious US Satellite Hacking Case’. The Register, 21 November 2011. https://www.theregister.com/2011/11/21/us_sat_hack_mystery/.

———. ‘The Truth about Mystery Trojan Found in Space’. The Register, 13 November 2013. https://www.theregister.com/2013/11/13/space_station_malware_not_stuxnet/.

Loria, Kevin. ‘Report: China Hacked America’s Weather Satellites And Threatened Vital Data’. Business Insider, 12 November 2014. https://www.businessinsider.com/china-hacked-americas-weather-satellites-2014-11?r=US&IR=T.

Lyons, Kim. ‘UK Government Takes $500 Million Stake in Space Exploration Firm OneWeb’. The Verge, 3 July 2020. https://www.theverge.com/2020/7/3/21312456/uk-oneweb-500-million-space.

Malik, William J. ‘Attack Vectors in Orbit: The Need for IoT and Satellite Security’. RSA Conference 2019, March 2019. https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/13692/MBS-W03-Attack-Vectors-in-Orbit-The-Need-for-IoT-and-Satellite-Security.pdf.

Marks, Joseph. ‘The Cybersecurity 202: Hackers Just Found Serious Vulnerabilities in a U.S. Military Fighter Jet’. The Washington Post, 14 August 2019. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/08/14/the-cybersecurity-202-hackers-just-found-serious-vulnerabilities-in-a-u-s-military-fighter-jet/.

Mazareanu, Elena. ‘Number of satellites launched from 1957 to 2019’. Statista, 23 June 2020. https://www.statista.com/statistics/896699/number-of-satellites-launched-by-year/.

McCarthy, Kieren. ‘One Man’s Mistake, Missing Backups and Complete Reboot: The Tale of Europe’s Galileo Satellites Going Dark’. The Register, 8 November 2019. https://www.theregister.com/2019/11/08/galileo_satellites_outage.

McCarthy, Kieren. ‘Remember When Europe’s Entire Galileo Satellite System Fell over Last Summer? No You Don’t. The Official Stats Reveal It Never Happened’. The Register, 29 January 2020. https://www.theregister.com/2020/01/29/galileo_satellite_outage/.

MHS. ‘Combat Search and Rescue: Menwith Hill Station’s Role in Saving Lives’. SID Today, March 23, 2005a. https://edwardsnowden.com/docs/doc/2005-03-23-SIDToday-Combat-Search-and-Rescue-Menwith-Hill-Stations-Role-in-Saving-Lives.pdf.

MHS. ‘MHS and GCHQ “Get in the Game” with Target Development for World of Warcraft Online Gaming’. Edwardsnowden.com, 1 January 2008. https://edwardsnowden.com/docs/doc/First.pdf.

MHS. ‘MHS Lends a Hand in the Aftermath of the London Bombings’. SID Today, August 25, 2005b. https://edwardsnowden.com/docs/doc/2005-08-24-SIDToday-MHS-Lends-a-Hand-in-the-Aftermath-of-the-London-Bombings.pdf.

MHS ‘MHS Leverages XKS for QUANTUM against Yahoo and Hotmail’. Edwardsnowden.com, n.d. https://edwardsnowden.com/docs/doc/menwith-hill-station-leverages-xkeyscore-for.pdf.

MPE. ‘ROSAT – the End of an Exceptional Satellite (1.June 1990 – 23. October 2011)’. Max Planck Institute for Extraterrestrial Physics, 14 November 2011. https://www.mpe.mpg.de/229897/News_20111114.

Nanosats. ‘Present Status of Launched Nanosatellites’, 5 November 2020. https://www.nanosats.eu/img/fig/Nanosats_status_2020-10-05_large.png.

NASA. ‘Agency Financial Report - Fiscal Year 2007’. National Aeronautics and Space Administration, 15 November 2007. https://www.nasa.gov/pdf/202960main_NASA_FY07_Financial_Report.pdf.

NASA. ‘CubeSat 101 - Basic Concepts and Processes for First-Time CubeSat Developers’, October 2017. https://www.nasa.gov/sites/default/files/atoms/files/nasa_csli_cubesat_101_508.pdf.

NASA. ‘First Contracted SpaceX Resupply Mission Launches with NASA Cargo to Space Station’. NASA, 7 October 2012. https://www.nasa.gov/home/hqnews/2012/oct/HQ_12-355_SpaceX_CRS-1_Launch.html.

NASA. 'ISS Daily Summary Report – 7/21/2020'. NASA - ISS On-Orbit Status Report, 21 July 2020. https://blogs.nasa.gov/stationreport/2020/07/21/.

NASA. 'ISS Daily Summary Report – 07/30/13'. NASA - ISS On-Orbit Status Report, 30 July 2013. https://blogs.nasa.gov/stationreport/category/2013/july/page/2/.

NASA. 'ISS Daily Summary Report – 11/08/2018'. NASA - ISS On-Orbit Status Report, 8 November 2018. https://blogs.nasa.gov/stationreport/2018/11/08/iss-daily-summary-report-11082018/.

NASA. 'NASA Extends the World Wide Web Out Into Space'. National Aeronautics and Space Administration, January 22, 2010a. https://www.nasa.gov/home/hqnews/2010/jan/HQ_M10-012_ISS_Web.html.

NASA. 'On-Orbit Satellite Servicing Study Project Report'. NASA Goddard Space Flight Center, October 2010b. https://nexis.gsfc.nasa.gov/images/NASA_Satellite%20Servicing_Project_Report_0511.pdf.

NASA. 'ROSAT Wrap-Up - ROSAT X-Ray Telescope Mission Comes to an End'. NASA Goddard Space Flight Center, 13 September 1999. https://heasarc.gsfc.nasa.gov/docs/rosat/taps.html.

NASA CIO. 'NASA Security Operations Center Operations and NASIRC Transition'. National Aeronautics and Space Administration, 29 October 2008. https://www.nasa.gov/pdf/322746main_10_29_08-NASA-Security-Operations-Center-Operations-and-NASIRC-Transition.pdf.

NASA OIG. 'Audit of NASA's Security Operations Center'. Office of Inspector General - National Aeronautics and Space Administration, 23 May 2018. https://oig.nasa.gov/docs/IG-18-020.pdf.

NASA OIG. 'Evaluation of NASA's Information Security Program under the Federal Information Security Modernization Act for Fiscal Year 2019'. Office of Inspector General - National Aeronautics and Space Administration, 25 June 2020. https://oig.nasa.gov/docs/IG-20-017.pdf.

NASA OIG. 'Inadequate Security Practices Expose Key NASA Network to Cyber Attack'. Office of Inspector General - National Aeronautics and Space Administration, 28 March 2011. https://oig.nasa.gov/docs/IG-11-017.pdf.

NASIC. 'Competing in Space'. US National Air and Space Intelligence Center, US Department of Defense, 16 January 2019. https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF.

NIST. 'Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1'. National Institute of Standards and Technology, 16 April 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Northrop Grumman. 'Orbital Sciences Corporation : Orbital Set to Launch COTS Demonstration Mission to International Space Station Tomorrow'. Northrop Grumman, 17 September 2013. https://news.northropgrumman.com/news/releases/orbital-sciences-corporation-orbital-set-to-launch-cots-demonstration-mission-to-international-space-station-tomorrow.

NSR. 'Satellite EOL: Not One Size Fits All'. Nothern Sky Research, 25 July 2018. https://www.nsr.com/satellite-eol-not-one-size-fits-all/.

OIG DoC. 'Significant Security Deficiencies in NOAA's Information Systems Create Risks in Its National Critical Mission - Final Report No. OIG-14-025-A'. Office of Inspector General - U.S. Department of Commerce, 15 July 2014. https://www.oig.doc.gov/OIGPublications/OIG-14-025-A.pdf.

OMB. 'Federal Information Security Management Act (FISMA) - 2004 Report to Congress'. Office of Management and Budget - Executive Office of the President of the United States, 1 March 2005. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/inforeg/2004_fisma_report.pdf.

OneWeb. 'Hughes and OneWeb Announce Global Distribution Partnership for Low Earth Orbit Satellite Service'. OneWeb, March 9, 2020a. https://www.oneweb.world/media-center/hughes-and-oneweb-announce-global-distribution-partnership-for-low-earth-orbit-satellite-service.

OneWeb. 'OneWeb'. OneWeb, n.d. https://trai.gov.in/sites/default/files/satrc/Presentation/SATRC_28_OneWeb.pdf.

OneWeb. 'OneWeb Successfully Launches 34 More Satellites into Orbit in Second Launch of 2020'. OneWeb, March 21, 2020b. https://www.oneweb.world/media-center/oneweb-successfully-launches-34-more-satellites-into-orbit-in-second-launch-of-2020.

OpenSky. 'About Us'. The OpenSky Network, n.d. https://opensky-network.org/about/about-us.

Osborne, Charlie. 'Feds "covered up" Chinese Hack on US Weather Systems'. ZDNet, 13 November 2014. https://www.zdnet.com/article/feds-covered-up-chinese-hack-on-us-weather-systems/.

OWS. 'About Us'. OneWeb Satellites, n.d. https://onewebsatellites.com/about-us/.

OWS. 'Our Factories'. OneWeb Satellites, n.d. https://onewebsatellites.com/factory/.

Pagliery, Jose. 'U.S. Weather System Hacked, Affecting Satellites'. CNN Business, 29 December 2014. https://money.cnn.com/2014/11/12/technology/security/weather-system-hacked/index.html.

Pawlyk, Oriana. 'Hackers Find Serious Vulnerabilities in an F-15 Fighter Jet System'. Military.com, 16 August 2019. https://www.military.com/daily-news/2019/08/16/hackers-find-serious-vulnerabilities-f-15-fighter-jet-system.html.

Penenberg, Adam. 'A Private Little Cyberwar'. Forbes, 21 February 2000. https://www.forbes.com/forbes/2000/0221/6504068a.html?sh=7ef879aa2661.

Perillo, Robert J. 'NASA to Be "Hacked" by DoD, and Macro Virus Infected Mir'. The Risks Digest - Volume 19, Issue 74, 16 May 1998. https://catless.ncl.ac.uk/Risks/19/74.

Porter, Jon. 'Europe's GPS Alternative Has Been Offline since Friday'. The Verge, 15 July 2019. https://www.theverge.com/2019/7/15/20694395/europe-galileo-satellite-navigation-system-offline-outage-technical-incident.

Porup, J.M. 'It's Surprisingly Simple to Hack a Satellite', 21 August 2015. https://www.vice.com/en/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite.

PWC & BAE Systems. 'Operation Cloud Hopper'. PWC UK, April 2017. https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

Rabinovitch, Ari. 'Space Age Perils: Hackers Find a New Battleground on the Final Frontier'. Reuters, 22 October 2015. https://www.reuters.com/article/us-space-risks/space-age-perils-hackers-find-a-new-battleground-on-the-final-frontier-idUSKCN0SG1Z420151022.

Reuters. 'British Satellite Firm OneWeb Emerges from Bankruptcy'. Reuters, November 20, 2020b. https://www.reuters.com/article/oneweb-bankruptcy/british-satellite-firm-oneweb-emerges-from-bankruptcy-idUSL4N2I63KF.

Reuters. 'Hackers Have Seized Control of One of Britain's Military Communication Satellites and Issued Blackmail Threats, The Sunday Business Newspaper Reported'. Rense.com, 2 March 1999. https://rense.com/ufo2/hackuk.htm.

Reuters. 'Hackers Tried to Steal Airbus Secrets via Contractors: AFP'. Reuters, 26 September 2019. https://www.reuters.com/article/us-airbus-cyberattack-report-idUSKBN1WB0U9.

Reuters. 'Mounties Get Their Hacker'. Wired, 4 June 1998. https://www.wired.com/1998/04/mounties-get-their-hacker/.

Reuters. 'Swedish Space Agency Halts New Business Helping China Operate Satellites'. Reuters, September 21, 2020a. https://www.reuters.com/article/china-space-australia-sweden-int/swedish-space-corporation-halts-new-business-with-china-idUSKCN26C1XU.

Robertson, Jordan, and Michael Riley. 'The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies'. Boomberg Businessweek, 4 October 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

RTS. 'La Suisse Veut Profiter Des Satellites d'observation Militaires Français'. RTS, 25 November 2020. https://www.rts.ch/info/suisse/11778327-la-suisse-veut-profiter-des-satellites-dobservation-militaires-francais.html.

RTS. 'L'armée Suisse a Envisagé d'acquérir Son Propre Satellite Espion'. RTS, 22 June 2018. https://www.rts.ch/info/suisse/9662564-larmee-suisse-a-envisage-dacquerir-son-propre-satellite-espion.html.

RUAG. 'Produktionsstart an Neuem Standort in Florida: RUAG Space Eröffnet Weitere US-Niederlassung'. RUAG, 12 July 2017. https://www.ruag.com/de/news/produktionsstart-neuem-standort-florida-ruag-space-eroeffnet-weitere-us-niederlassung.

RUAG. 'RUAG Space Is Key Supplier for Constellations'. RUAG, 14 March 2019. https://www.ruag.com/en/news/ruag-space-key-supplier-constellations.

Russkiy Mir. 'Russian Internet Connection Installed on ISS'. Russkiy Mir Foundation, 31 July 2020. https://russkiymir.ru/en/news/275572/.

Schmid, Gerhard. 'Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) (2001/2098(INI))'. European Parliament, 11 July 2001. https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN.

Scoles, Sarah. 'The Feds Want These Teams to Hack a Satellite - From Home'. Wired, 8 June 2020. https://www.wired.com/story/the-feds-want-these-teams-to-hack-a-satellite-from-home/.

Shachtman, Noah, and David Axe. 'Most U.S. Drones Openly Broadcast Secret Video Feeds'. Wired, 29 October 2012. https://www.wired.com/2012/10/hack-proof-drone/.

Sheetz, Michael. 'Satellite Start-up Raises $100 Million to Put Cloud Data Storage in Space'. CNBC, 27 February 2019. https://www.cnbc.com/2018/12/19/cloud-constellation-raises-100-million-to-store-cloud-data-in-space.html.

———. 'SpaceX Is Manufacturing 120 Starlink Internet Satellites per Month'. CNBC, 10 August 2020. https://www.cnbc.com/2020/08/10/spacex-starlink-satellte-production-now-120-per-month.html.

Shuiyu, Jing. 'OneWeb Plans 3 Satellite Ground Stations in China'. China Daily, 28 November 2019. https://www.chinadaily.com.cn/a/201911/28/WS5ddf8fb2a310cf3e3557ab4f.html.

Shuman, Mariah. 'The Dream of Affordable Internet Access for Everyone Is Getting Closer'. OneWeb/ITU, May 2017. https://www.itu.int/en/ITU-R/space/workshops/2017-Bariloche/Presentations/16%20-%20Mariah%20Shuman%20Oneweb.pdf.

Simpson, Connor. ‘Russian Cosmonauts Occasionally Infect the ISS with Malware’. The Atlantic, 11 November 2013. https://www.theatlantic.com/international/archive/2013/11/russian-cosmonaut-accidentally-infected-iss-stuxnet/355150/.

SoldierX. ‘Jay Dyson’. SoldierX.com, n.d. https://www.soldierx.com/hdb/Jay%20Dyson.

Space ISAC. ‘Space ISAC’. Space ISAC, n.a. https://s07f21n96ry3bgacl3z1pdi9-wpengine.netdna-ssl.com/wp-content/uploads/2020/08/SISAC_8x11_Email-rev1.5.pdf.

Spaceflight Now. ‘Launch Schedule’. Spaceflightnow.com, accessed January 7, 2021. https://spaceflightnow.com/launch-schedule/.

Spacewar. ‘Swedish Space Corporation to Cease Assisting Chinese Companies Operate Satellites’. Spacewar.com, 22 September 2020. https://www.spacewar.com/reports/Swedish_Space_Corporation_to_cease_assisting_Chinese_companies_operate_satellites_999.html.

Strout, Nathan. ‘The Pentagon Wants Help for Its Satellites to Talk to Each Other’. C4ISR Net, 16 January 2020. https://www.c4isrnet.com/battlefield-tech/c2-comms/2020/01/16/the-pentagon-wants-help-for-its-satellites-to-talk-to-each-other/.

Swissinfo. ‘Swiss Close Investigation into Cyber Attack on Defence Firm’. Swissinfo, 27 August 2018. https://www.swissinfo.ch/eng/ruag_swiss-close-investigation-into-cyber-attack-on-defence-firm/44352550.

Tanase, Stefan. ‘Satellite Turla: APT Command and Control in the Sky’. SecureList, 9 September 2015. https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.

TASS. ‘Russian Space Agency Ensures Secrecy of Vote for Cosmonauts at ISS’. TASS, 1 July 2020. https://tass.com/science/1173585.

The Day. ‘U.S. Weather Systems Hacked’. The Day, 13 November 2014. https://www.theday.com/article/20141113/NWS13/311139563.

The New Scientist. ‘Clear and Present Danger?’ The New Scientist, 6 March 1999. https://www.newscientist.com/article/mg16121761-300-clear-and-present-danger/.

Thomas, Valerie L. ‘NASIRC Receives NASA Group Award’. National Space Science Data Center, June 1995. https://nssdc.gsfc.nasa.gov/nssdc_news/june95/09_v_thomas_0695.html.

Thurber, Matt. ‘ADS-B Is Insecure and Easily Spoofed, Say Hackers’. AINonline, 3 September 2012. https://www.ainonline.com/aviation-news/aviation-international-news/2012-09-03/ads-b-insecure-and-easily-spoofed-say-hackers.

Trevithick, Joseph, and Tyler Rogoway. ‘Shedding Some Light On The Air Force’s Most Shadowy Drone Squadron’. The Drive, 25 April 2018. https://www.thedrive.com/the-war-zone/19318/uncovering-the-air-forces-most-mysterious-drone-squadron.

UCS. ‘Changes to the UCS Satellite Database’. Union of Concerned Scientists, April 2020b. https://www.ucsusa.org/sites/default/files/2020-05/changes%20to%20the%20database%204-1-20.pdf.

UCS. ‘UCS Satellite Database’. Union of Concerned Scientists, August 2020a. https://www.ucsusa.org/resources/satellite-database.

US Senate. ‘Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing - Hearing before the Senate Subcommittee on Technology, Terrorism, and Government Information’. US Government Printing Office, 28 March 2000. https://www.govinfo.gov/content/pkg/CHRG-106shrg69358/html/CHRG-106shrg69358.htm.

USCC. ‘2011 Report to Congress of the U.S.-China Economic and Security Review Commission’. U.S.-China Economic and Security Review Commission, November 2011. https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf.

USG. ‘Menwith Hill Satellite Classification-Guide’. The Intercept, 2005. https://www.documentcloud.org/documents/3089521-Menwith-satellite-classification-guide.html.

USN. ‘First COMSAT Advisory Board Proves Its Point (Repost)’. SID Today, 26 May 2004. https://edwardsnowden.com/docs/doc/2004-05-26-SIDToday-First-COMSAT-Advisory-Board-Proves-Its-Point-repost.pdf.

USSPACECOM. ‘USSPACECOM Expands Key Allied Space Partnerships through Multi-Nation Operations’. US Space Command, US Department of Defense, 27 December 2019. https://www.spacecom.mil/News/Article-Display/Article/2047780/usspacecom-expands-key-allied-space-partnerships-through-multi-nation-operations/.

Vijayan, Jai. ‘Russian Threat Group May Have Devised a “Man-on-the-Side” Attack’. Dark Reading, 25 July 2019. https://www.darkreading.com/attacks-breaches/russian-threat-group-may-have-devised-a-man-on-the-side-attack-/d/d-id/1335348.

Wagenseil, Paul. ‘No, Stuxnet Did Not Infect the International Space Station’. Yahoo News, 13 November 2013. https://news.yahoo.com/no-stuxnet-did-not-infect-international-space-station-002152419.html.

Wakefield, Jane. ‘Our Satellites Are Hack Proof’. ZDNet, 28 February 1999. https://www.zdnet.com/article/our-satellites-are-hack-proof/.

Werner, Debra. ‘Cyber Focus: Space’. Aerospace America, September 2020. https://aerospaceamerica.aiaa.org/features/cyber-focus-space/.

Werner, Debra. 'How Long Should a Satellite Last: Five Years, Ten Years, 15, 30?' SpaceNews, 14 May 2018. https://spacenews.com/how-long-should-a-satellite-last/

White, Dan. 'SSC Increases Capacity at Florida Ground Station – Eight New Antennas to Support OneWeb's Global Satellite Network'. SSC, 7 October 2019. https://www.sscspace.com/ssc-increases-capacity-at-florida-ground-station/.

White House. 'Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems'. White House, 4 September 2020. https://www.whitehouse.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/.

WHiTe VaMPiRe. 'Free the Fish'. Projectgamma.com, 6 April 1999. http://67.225.133.110/~gbpprorg/phrack/phrack.ru/old/blackhatbloc/jamba/040699-1741.html.

Wolf, Jim. 'China Key Suspect in U.S. Satellite Hacks: Commission'. Reuters, 28 October 2011. https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028.

Zetter, Kim. 'Hackers Targeted U.S. Government Satellites', 27 October 2011. https://www.wired.com/2011/10/hackers-attack-satellites/.

CSS

ETH Zürich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.