Technical Study

Satellite Cyberattacks and Security

July 2021

Prepared by: **Luke Shadbolt**

> HDI Global Specialty SE

Contents

Introduction

This report presents the output of a study made by HDI Global Specialty (UK) into the current state of knowledge surrounding satellite cyberattacks. At present none of the established insurers provide coverage against cyberattacks in their policies; however as the risk of cyberattacks is set to increase in future it is an area of growing concern for operators that merits further study.

Cyberattacks use software and network techniques to compromise, control, interfere, or destroy the data and computer systems linked to satellite operations. This report differentiates between these types of attack and those techniques referred to as ‘Electronic Warfare’ (EW) such as jamming or spoofing, where the aim is either to block or imitate the Radiofrequency (RF) signals that are transmitted between the satellite and ground stations [1] [2] [3]. EW attacks are not considered within the scope of this study, however current cyber coverage policy clauses may or may not choose to include them under their definition of cyberattack.

Section I of the report presents the main consequences of satellite cyberattack, ranging from service disruption to loss of satellite control and espionage. Common modes of attack are discussed in section II, while in section III several well publicised case studies are presented. Defence mechanisms are increasingly being incorporated into satellite design and operations, certain examples of which are described in section IV. The current state of industry efforts to address satellite cybersecurity is discussed in section V, and a review of the present insurance standpoint is given in section VI.

Introduction *continued*

Why are satellites a target?

Satellites are crucial for everyday life in our society, from navigation to TV broadcasts, phone and power networks, weather forecasts, climate monitoring, and military communications. The growing Internet-of-Things also relies on satellite communication. Space systems are of immense value and importance in each of these areas and represent a single point of failure, meaning that many of the above services would collapse without correct functioning of the space systems on which they rely. These factors make them attractive targets to different groups including industry competitors, criminals, hacking activists, nation states, or military forces [4].

In addition, cybersecurity standards for space assets are not regulated by any governing body and a lack of regulation means that satellites both lack common cybersecurity standards and may be used for cyberattacks with impunity / anonymity.

Satellite vulnerability

Satellites have a series of points of vulnerability since they are controlled from the ground and relay information to and from the ground, see Figure 1. As such, accessing their networks is generally easier than if there were only a single entry point to defend [4]. Three key points of access exist for a potential cyberattack [5]:

- The extended land-based infrastructure that sustains space-based assets including ground stations, terminals, related companies, and end-users.
- The satellites themselves.
- The supply chain.

The complexity of the supply chain is what makes this a key point of access – satellites require multiple manufacturers and a system integrator to compile all the components to function as one. The multiple vendors required provide various opportunities for a hacker to gain access [6].

Military satellites are generally less vulnerable to cyberattack than their civilian counterparts since greater effort is expended in their cybersecurity, for instance in utilising advanced encryption methods and ensuring physical infrastructure such as ground stations is well protected.

In the past only state actors were capable of attacking space-based assets, however today the technical barrier is much lower. It is possible to hack into computer systems and intercept communications using relatively cheap, easily available, and unsophisticated hardware. Therefore state-of-the-art monitoring and protection measures are now a must for space-based systems, just like any other IT systems that support critical infrastructure.

CYBER THREATS TO SPACE SYSTEMS

Space Segment
- Command Intrusion
- Payload Control
- Denial of Service
- Malware

User Segment
- Spoofing
- Denial of Service
- Malware

Link Segment
- Command Intrusion
- Spoofing
- Replay

Ground Segment
- Hacking
- Hijacking
- Malware

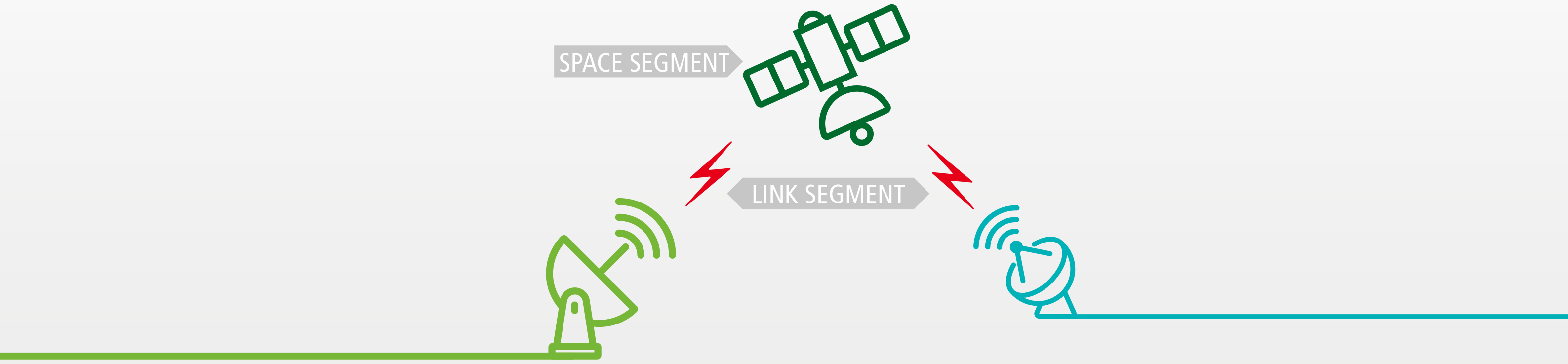


Figure 1 – Cyber threats across the four typical segments of a space system [7].

State vs Non-state actors

Cyberattacks on satellites may be conducted by a variety of different groups or organisations as described previously and these can be broadly categorised as either state or non-state actors.

State actors include the governments of nation states and/or their military forces. Several such actors have developed cyber warfare capabilities that could interfere with satellites. State actors may be motivated by the need to gather intelligence on their adversaries, as a response to confrontations, or as a way of demonstrating their technological prowess.

Non-state actors include all other groups capable of carrying out satellite cyberattacks including corporations, criminals, and hacking activists. Such groups may conduct attacks as a means of gaining an advantage over industry competitors (i.e. industrial espionage), to allow theft of data, to hold organisations to ransom, or in the pursuit of other economic or political goals.

One of the major challenges facing space asset organisations in responding to cyberattacks is referred to as the “Attribution Problem”, or the difficulty in identifying the source of a cyberattack. Since satellites rely on networks like the internet where communications are divided into packages that follow independent routes to the receiver (an approach referred to as ‘Packet Switching’), an attack can be made from virtually anywhere while leaving little trace of the origin of the attack [8]. This provides the actor with the ‘deniability factor’ and therefore makes cyberattacks a perfect way to create disruption and damage to space systems.

> Since satellites rely on networks like the internet where communications are divided into packages that follow independent routes to the receiver (an approach referred to as ‘Packet Switching’), an attack can be made from virtually anywhere while leaving little trace of the origin of the attack.

I. Cyberattack Consequences

Table 1 summarises the main types of cyberattack. Potential consequences of such attacks are described below in this section.

Table 1 – Types of Cyberattack [3]

	Cyber		
Types of Attack	Data Intercept or Monitoring	Data Corruption	Seizure of Control
Attribution	Limited or uncertain attribution	Limited or uncertain attribution	Limited or uncertain attribution
Reversibility	Reversible	Reversible	Irreversible or reversible, depending on mode of attack
Awareness	May or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public
Attacker Damage Assessment	Near-real time confirmation of success	Near-real time confirmation of success	Near-real time confirmation of success
Collateral Damage	None	None	Could leave target satellite disabled and uncontrollable

I.1 Service disruption

One of the most likely consequences of satellite cyberattack is service disruption or even complete service denial. Service disruption, even as a result of an attack on a single satellite, has the potential to cause an immediate and significant impact on large groups of people across a wide geographical area. For example, service disruption to Global Positioning System (GPS) satellites has the potential to impact not only the multitude of ground, sea, and air services that rely on their signals for accurate positioning, but also critical infrastructure such as financial institutions and utility companies that rely on them for precise timing.

Communications satellites comprise the majority of satellites in orbit and support global communications, complementing terrestrial communications networks. Disruption to the operation of these satellites can have wide-ranging impacts as was illustrated in 1998 when a U.S. communications satellite suffered a computer failure, leaving television stations unable to deliver programming amongst other impacts [2].

I.2 Loss of satellite control

In terms of severity, one of the worst potential consequences of satellite cyberattack is a loss of control of the satellite. If hackers are able to seize control of the satellite bus or payloads there is no limit to the damage that can be done. An attack could deliberately cause a satellite to manoeuvre, 'decaying' or lowering its orbit so that it re-enters the Earth's atmosphere and burns up. Alternatively a sophisticated attack could manoeuvre a satellite so that it collides with another satellite or space object [9]. In another scenario the attack could shut down all communications and permanently damage the satellite by expending its propellant supply or damaging its electronics and sensors [3]. States are actively developing these capabilities and examples of such attacks have been documented (see section III).

I.3 Extortion or ransom

Just as hackers are able to hold terrestrial computer systems to ransom through the use of ‘ransomware’, space systems also present the opportunity for such attacks. In this case a criminal actor might hijack some aspect of the satellite’s operation and demand the transfer of a financial payment from the operator, promising to return control on receipt of the payment. Submitting to such a demand is usually inadvisable given that the criminal actor may respond by simply increasing the sum demanded, however when critical services such as GPS navigation and communications are involved a response either to pay or not is likely to be costly.

There is some precedent for such attacks on satellites, with one unverified example being a ransomware attack on a British military satellite as reported in 1999 [10].

I.4 Espionage (state, industrial)

Espionage as a form of cyberattack refers to the act of obtaining secret or confidential information without the permission of the information owner (i.e. spying). Often associated with nation states or governmental actors, corporations may also commit espionage in order to steal competitors secrets and thereby gain an advantage (commonly referred to as ‘industrial espionage’). The data transmitted via space assets is particularly vulnerable to interception and monitoring given the highly connected nature of these systems. Although such a cyberattack may not damage the satellite or disrupt its service in any way, the interests of the organisations that operate and utilise the service may be compromised.

Some state actors have conducted comprehensive and sustained penetration and cyber-espionage operations against the U.S. defence and European satellite and aerospace industries since at least 2007 [5].

Other state actors with significant cyber espionage abilities have used satellite-based communication techniques since 2007 to help hide the location of their command servers [11]. Such techniques are inexpensive requiring only a satellite dish, some cable, and a satellite modem, all of which cost about $1,000.

II. Modes of Attack

Cyberattacks against space assets are similar to cyberattacks against non-space systems. They often involve attempts to feed information to a system that causes software to perform in unexpected ways, commonly known as "bugs". In some cases, bugs can be exploited to crash systems, run unauthorised code, and/or gain unauthorised access. Other common cyberattacks exploit the lack of, or faulty, authentication of users and commands. The more software features or components a system has, and the more types and channels of data it processes, the higher the attack surface of potential vulnerabilities that an attacker can exploit [5].

As explained previously, three key points of access exist for a potential satellite cyberattack: the extended land-based infrastructure (ground stations etc.), the satellites themselves, and the supply chain. The modes of attack via each of these points are discussed in this section.

II.1 Attacks via ground stations or other terrestrial infrastructure

Ground stations (or "tracking sites") are the terrestrial facilities used to communicate with satellites. They provide the ability to send data to (uplink) and receive data from (downlink) the satellite, and are connected via terrestrial networks (e.g. the internet) to a control centre from where commands to the spacecraft are issued, see Figure 2. All ground stations use computers which may exhibit software vulnerabilities that can be exploited by hackers. If hackers are able to infiltrate these computers they can send malicious commands to the satellites. A simple methodology used to achieve this could be as follows:

The hacker would first use open source intelligence gathering techniques (Google, LinkedIn, Facebook, etc.) to identify key personnel with privileged systems access at the ground station. He would then target them with a spear phishing campaign via email and social media in order to trick them into inadvertently providing access to their workstation and then onto satellite control systems. These systems could then be manipulated over the internet to control the satellites or gain access to sensitive data [12].

Attacks on ground-based internet-connected infrastructure that is operated by humans represents the easiest mode of attack via cyber means. Other techniques may include tapping internet or Ethernet cables, and piggybacking off of data relays. Examples of attacks using such methods include that of the satellite ROSAT (see section III.1) that was attacked via hacked computers at the Goddard Space Flight Center in 1998.

The recent implementation of cloud-based ground stations and satellite services acts to further increase the attack surface or range of vulnerabilities for an attacker to exploit. Services such as Amazon Web Services (AWS) and Microsoft's Azure Cloud Services enable satellite operators to manage the features and functions of their satellite from the comfort of their own home [13]. However these services equally bridge the gap for motivated adversaries to command attacks using the dynamic cloud platform.

In addition to ground stations other terrestrial infrastructure such as that responsible for processing space data is susceptible to attack. In 2014 attackers breached the National Oceanic and

The hacker would first use open source intelligence gathering techniques (Google, LinkedIn, Facebook, etc.) to identify key personnel with privileged systems access at the ground station. He would then target them with a spear phishing campaign via email and social media in order to trick them into inadvertently providing access to their workstation and then onto satellite control systems. These systems could then be manipulated over the internet to control the satellites or gain access to sensitive data [12].

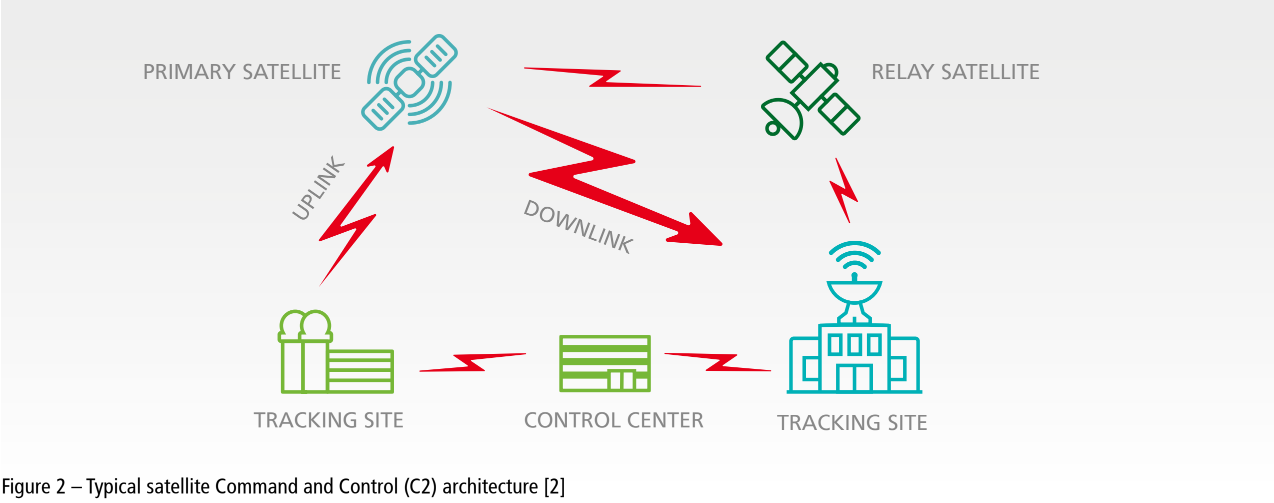


Figure 2 – Typical satellite Command and Control (C2) architecture [2]

Atmospheric Administration (NOAA) computer network, including systems used to manage and disseminate satellite weather data and products. Although the attack itself did not disrupt satellite data, NOAA stopped providing satellite images to the National Weather Service and public-facing services were taken offline for two days while the systems were cleaned [5].

II.2 Direct satellite / communication link attack

Some attacks may avoid ground-based infrastructure and attack satellites directly via their radiofrequency (RF) communication links. These links represent a significant weakness and one that is common to all satellites. Commercial satellite uplinks and downlinks are often transmitted through open (unencrypted) telecom network security protocols that are easily accessed by cyber criminals [14].

Attacks on these links are likely to be man-in-the-middle (MITM), an umbrella term that involves an attacker inserting themselves between the sender and receiver, and thus able to monitor information being passed (data interception) or perhaps even modify it (data corruption / modification). The ease with which data can be intercepted is largely mission dependent since a number of factors influence the communication link (orbit type, transmitter power, beam width, encryption etc.).

For example, satellites in Geostationary Earth Orbit have a relatively large downlink beam width resulting in a much more easily intercepted signal [15]. Interception of data may result in the loss of data confidentiality and data privacy if the data is not encrypted. As spacecraft move towards optical communications, data interception will become more difficult but not impossible. Data can also be corrupted by an attacker during its transmission to/from a spacecraft. This could result in service disruption or satellite loss if it results in no action when required or the wrong action being taken.

It is also possible - although often very difficult, to use a cyberattack against the command and control (C2) link to gain access to the satellite bus or payloads. This type of attack is made easier if the C2 system is unencrypted or does not properly authenticate commands.

Alleged instances of such attacks include that of the satellite Terra EOS AM-1 (see section III.3) whereby the attackers gained control for a period of several minutes in 2008. Although the attack initially appeared to have come via the Svalbard ground station the facility's owners saw no evidence of this and it may therefore have originated as a direct attack on the satellite communication link.

II.3 Supply chain (hardware + software) vulnerabilities

The multiple vendors required to supply components, assemble, and integrate a satellite provide various access points and opportunities for a hacker to compromise the hardware and/or software. For example, NASA purchases components from catalogues of approved vendors around the world. However the approval process for these vendors does not necessarily include cybersecurity vetting standards and instead prioritises physical quality control. This lack of insight introduces considerable cybersecurity risk. In addition to the vulnerability of the supply chain, space organisations generally work with several research centres who may possess their own vulnerabilities, and thus collaborations across multiple partners can exacerbate potential security issues [16]. As shown in Figure 3, the unique complexity of the development, management, use and ownership environment of space assets makes consolidated cybersecurity for such systems particularly challenging.

In particular, risks to global supply chain security are posed by the increasing use of faulty or counterfeit microelectronics and materials produced abroad.

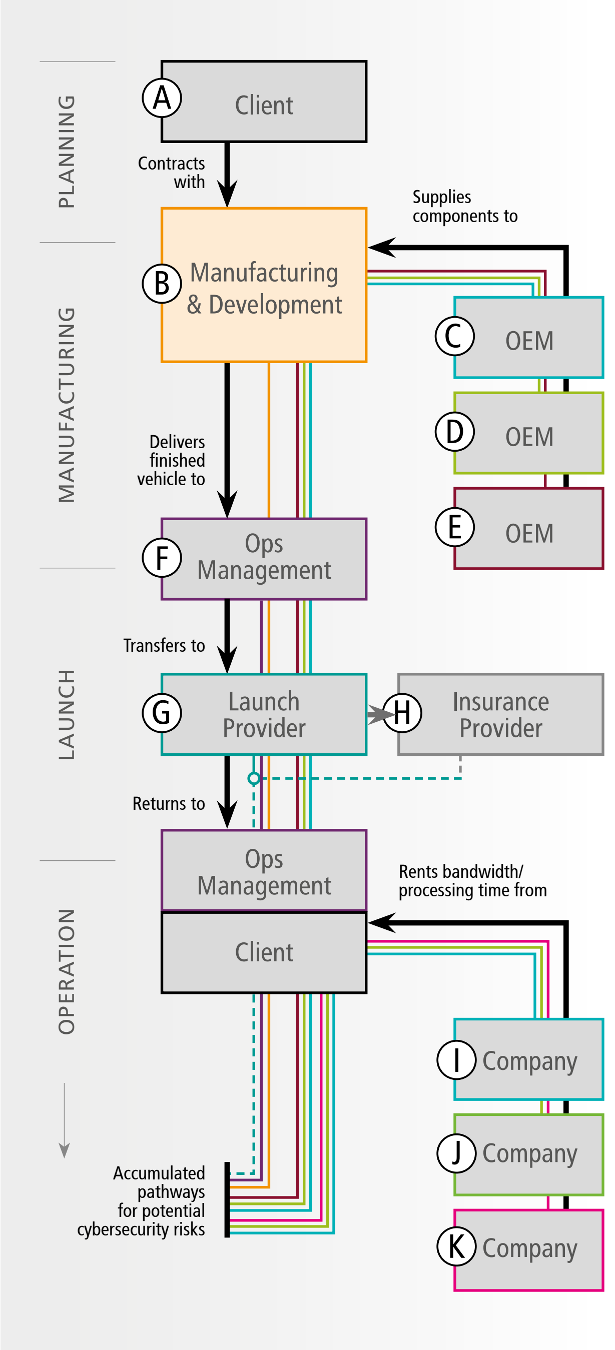


Figure 3 – Cybersecurity risks and responsibility pathways for an example satellite project [6].

Deliberate installation of hidden back doors in hardware or software products is another major threat in this area. Such cyberespionage operations can be directed against satellite manufacturers, parts suppliers, software brokers, launch service providers, and telecommunications companies. Physical infiltration, social engineering, and network exploitation of these targets can provide access to the design schematics, physical components, and software packages of a given satellite [5].

As shown in Figure 3, company A may commission the development of a satellite with company B that then assumes the cybersecurity responsibility of the satellite. Company B then outsources components of that satellite development to companies C, D, and E, who own their own component of the cybersecurity responsibility of the satellite. When company B completes the development of the satellite and delivers it to the owner (company A), company F is then contracted to manage the operations of the satellite (Company F then assumes operational cybersecurity responsibility of the satellite). Company F then commissions company G to launch the satellite into space. Company G assumes cybersecurity responsibility during the launch process. The liability for this cybersecurity responsibility is often shifted to an insurance provider company, H. Once the satellite is in orbit and operational, the management company (F) then resumes cybersecurity responsibility for the operations of the satellite. Often, the owner of the satellite (company A) will want to maximise the utility of the satellite to improve profitability and so will lease the use of bandwidth or processing on the satellite to other companies I, J, K, etc. Because of this complex ecosystem of owner, developer, operator and user cybersecurity responsibility, there are many opportunities for an adversary to gain access to the satellite.

This liability life cycle does not cover the role of cyber insurance during the operational life of the satellite, which is yet to become a major player for space asset cybersecurity [16].

II.4 Other modes of attack

In addition to those discussed above there are other modes of attack, some of which are only starting to emerge.

Cyberattacks against the user segment of the space system (see Figure 1) may involve the terminals or devices used to receive a satellite signal. In many cases, these attacks are very similar to cyberattacks against other types of computer equipment and focus on exploiting hardware or software vulnerabilities in the devices. Examples include techniques for modifying the data content of civil GPS signals and rebroadcasting them. When commercial GPS receivers try to decode these malicious GPS signals they can crash repeatedly, effectively succumbing to a denial-of-service attack [5].

Another category involves the exploitation of satellite links to facilitate hacking of other targets. Such techniques may hijack the IP addresses of legitimate satellite-based internet users, allowing the hackers to gain access to private networks and hide the location of their command servers.

Satellite-to-satellite cyberattacks whereby an attack is launched on one satellite from another have not yet been publicly documented, however the technical feasibility of such attacks has been studied and they are expected to become a threat in the coming decade. These attacks would target the sensors and subsystems of the victim satellite in close proximity or within line-of-sight. As such the offensive satellite would require special-purpose sensors and actuators that may not be typically resident on satellites [13]. These actuators would need to be controlled via a ground station (potentially hosted in the cloud) or using on-board decision making algorithms.

III. Case Studies

Actual evidence in the public domain of cyberattacks against space systems is limited. To date there have only been a few publicly-disclosed cyberattacks directly targeting space systems and even the information on these is incomplete. The most prominent examples are described in this section.

III.1 ROSAT (1998)

Hackers based in Russia took control of the U.S.-German X-ray science satellite ROSAT on 20/09/1998 in an example of an attack made via a satellite ground station. In this particular case, computers at the NASA Goddard Space Flight Center in Maryland were hacked before the hackers instructed the satellite to turn towards the sun. This effectively fried the satellite's batteries and optics, rendering the satellite useless [5] [17]. It was also reported that ROSAT data obtained in the attack was sent to Moscow [18].

III.2 Landsat 7 (2007, 2008)

On 20/10/2007 the U.S. earth observation satellite Landsat 7 jointly managed by NASA and the U.S. Geological Survey experienced 12 minutes of interference in an example of a direct attack on the satellite C2 link. The interference was only discovered following a similar event on 23/07/2008. Both attacks are thought to be attributable to China, however in both cases the responsible party did not achieve all the steps necessary to command and control the satellite [5] [16].

III.3 Terra EOS AM-1 (2008)

The NASA earth observation satellite Terra EOS AM-1 experienced 2 minutes of interference on 20/06/2008 and 9 minutes of interference on 22/10/2008. In both cases the responsible party achieved command and control of the satellite, however no commands were issued. The attacks were again attributed to China [16]. Although the attacks initially appeared to have come via the Kongsberg Satellite Services ground station at Svalbard, the facility's owners saw no evidence of this and it may therefore have originated as a direct attack on the satellite C2 link [5].

IV. Defence Mechanisms

The fundamental problem historically for space systems has been that they were designed assuming protection at their boundaries (i.e. outside the space segment, see Figure 1) would be enough. Little internal protection existed if the boundary was breached. Current and future space system designs must overcome the risk of an adversary breaching the boundary and operating unhindered inside the system using Defence in Depth (DID) principles. Both large traditional developments and more modern rapidly developed space systems (i.e. New Space) should ensure that they have a cyber-hardened design with such principles implemented throughout [7].

The backbone of a cyber-resilient spacecraft should be a robust Intrusion Detection System (IDS).

For a space system, a DID strategy relies on multiple layers of security to protect mission-critical assets. This approach encompasses acquisition, secure supply chains, space system hardening and monitoring, secure software development, intrusion detection and prevention, culture, people, etc. to create multiple layers as a security control. Recalling again Figure 1 and applying a DID strategy, security controls would need to be applied at the user segment, ground segment, link segment, and space segment to ensure the overall system has a robust security architecture. This section outlines how to apply defence mechanisms to the space segment only; focusing on encryption and authentication, on-board intrusion detection and prevention, cyber resilience testing, supply chain risk management, and on-board logging.

IV.1 Encryption and authentication

Encryption of the data sent to and from spacecraft may be considered as the first line of defence inside a space system, allowing private communications that are only visible to others with the cryptographic key. Encryption is effective in preventing loss of confidentiality when data is intercepted, denial-of-service style attacks, and unauthorised access to space systems [15]. On-board authentication of uplinked commands can help identify malicious interference and avoid loss of satellite control. Specifically, encryption of the C2 link is essential to secure the command and control of the satellite and avoid the potential consequences of a successful attack.

Although all military satellites use some form of encryption, it is unclear how many public and private satellites are using this security technique. The space asset community often applies security techniques the developers determine to be "relevant", which yields a variety of encryption practices. Some satellites are using NIST's (the National Institute of Standards and Technology) latest Advanced Encryption Standard (AES), whereas others roll out their own encryption standards. An example of a satellite using something other than the AES and pushing the boundaries of what is possible for space asset security is a Chinese satellite that uses Quantum Key Distribution (QKD) for encrypted communication [16]. QKD is a method of sending encryption keys using the peculiar quantum behaviours of subatomic particles (termed "entanglement"), and at least in theory is completely unhackable [19]. Several western companies including the British company ArQit are also pursuing this next-generation encryption. Its development is thought necessary to address the weaknesses of current encryption techniques in the face of rapidly increasing computing power. While this sophisticated encryption is unnecessary for many space assets, it is clear that such advanced security techniques are indeed possible for satellites.

IV.2 On-board intrusion detection and prevention

The backbone of a cyber-resilient spacecraft should be a robust Intrusion Detection System (IDS). The IDS should consist of continuous monitoring of telemetry, command sequences, command receiver status, shared bus traffic, and flight software configuration and operating states. From a telemetry monitoring perspective, several parameters exist that have the highest likelihood of indicating a cyberattack against a spacecraft and should be actively monitored on the ground and on-board the spacecraft with the IDS [7].

Responses to detected events may vary depending on the nature of the threat. Violating non-severe rules or crossing a low-scoring threshold will trigger an alert in telemetry to the ground operator with the violation, the raw data that caused it, and a recommended course of action. If a severe rules violation occurs or a higher threshold is crossed, the spacecraft's Intrusion Prevention System (IPS) will take automated actions, which may include swapping to a redundant side, quarantining command sequences, reloading flight software, and/or halting suspect units [7].

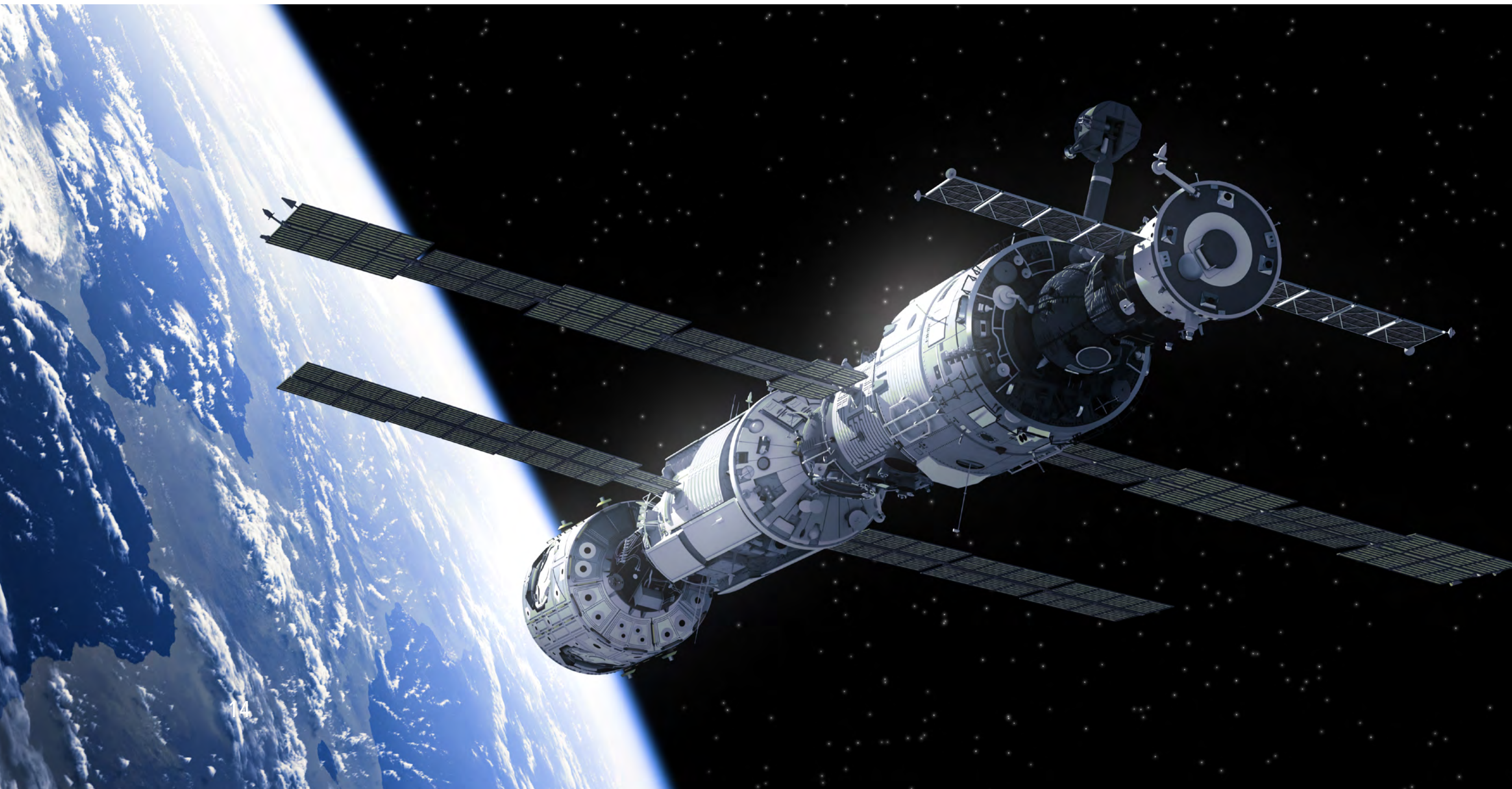
The IPS system should be integrated into the existing on-board spacecraft Fault Detection Isolation and Recovery system (FDIR) because the FDIR has its own fault detection and response system built in. Integrating the two systems ensures they do not take conflicting actions.

Finally, the spacecraft IPS and the ground should retain the ability to return critical systems on the spacecraft to a known cyber-safe mode. This is an operating mode during which all nonessential systems are shut down and the spacecraft is placed in a known good state using validated software and configuration settings. The default cyber-safe mode software should be stored on-board the spacecraft in memory with hardware-based controls and should not be modifiable [7].

IV.3 Cyberattack resilience testing

Spacecraft (and particularly their software) need to be designed from the outset for the appropriate level of security, and systems checked for cyber resilience before launch – not once they are in orbits from which there are no plausible recovery options.

Cyberattack resilience testing is a new approach towards achieving this goal, whereby developers precisely replicate their spacecraft, ground stations, and communication networks in a realistic environment so that they can be put through malicious cyberattacks and their vulnerability assessed by cyber experts. The company ManTech launched such a service in 2020 called Space Range [20]. Its testers are able to find hidden vulnerabilities, misconfigurations, and software bugs; giving developers the opportunity to harden their systems against cyberattack before they are launched and put into operation. In 2019 the European Space Agency (ESA) established a cyber training range at ESEC in Belgium which is planned to become a European reference centre for cyber security services. The range provides training



and testing for its own employees and partners, and aims to develop knowledge in awareness, detection, investigation, response and forensics to counter cyberattacks specific to space systems [21].

While the use of dedicated cybersecurity ranges may not be available to all spacecraft developers, if the space system's resilience against common forms of cyberattack is considered during the design phase this can act as an effective preventative measure, resulting in a more cyber-hardened system once in operation.

Software often leverages third-party code, which may introduce vulnerabilities into the system.

IV.4 Supply chain risk management

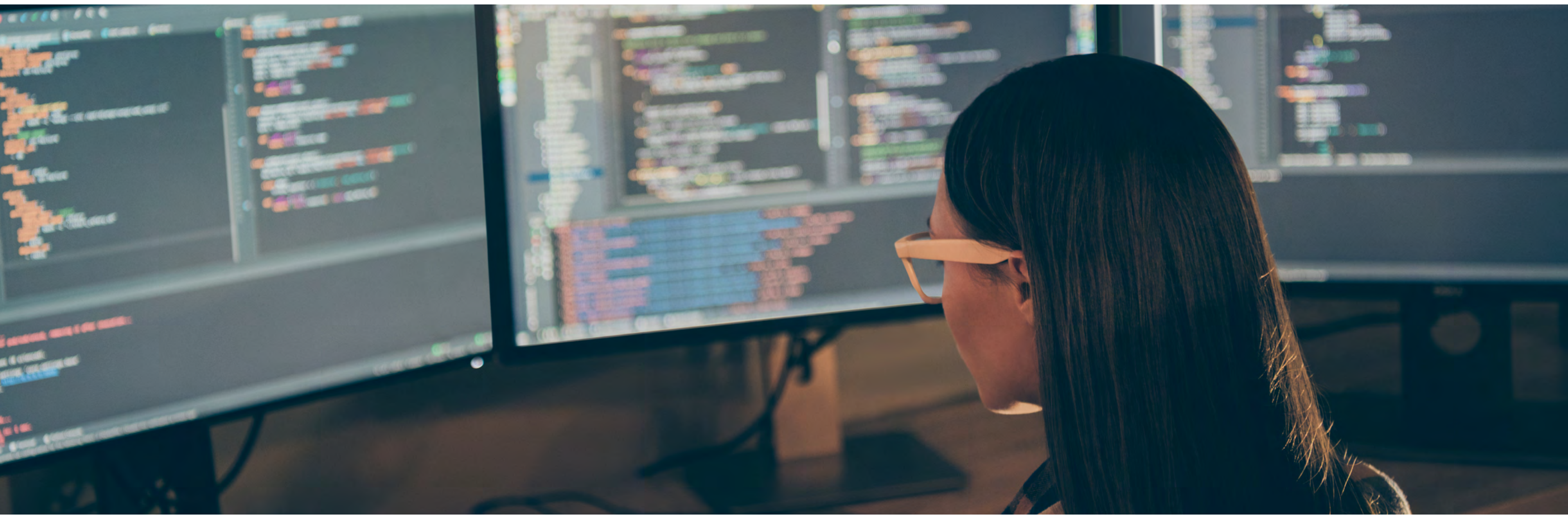
It is critical that spacecraft developers implement a supply chain risk management program. They must ensure that each of their vendors handles hardware and software appropriately and with an agreed-upon chain of custody. Critical units and subsystems should be identified and handled with different rigor and requirements than noncritical units and subsystems. Parts should be sourced from reputable vendors and checked for signs of counterfeiting [7].

All software on the spacecraft should be thoroughly vetted and properly handled through configuration management and secure software development processes. This can include the use of secure coding standards or principles that aid in the reduction of non-intended weaknesses. Software often leverages third-party code, which may introduce vulnerabilities into the system. The prime integrator must take responsibility for all security weaknesses introduced via the use of third-party code. At a minimum that means obtaining the code via trusted means and updating to new versions that fix security weaknesses, and ideally includes scanning and testing third-party software for security weaknesses [7].

IV.5 On-board logging

Logging is the process of collecting and storing data over a period of time in order to analyse events / actions of the system. For example, parameters at the input to the command receivers may be of use for anomaly investigations. The technique enables the tracking of all interactions through which data, files, or software is stored, accessed, or modified. As such any indications of an intrusion attempt or other cyberattack will be recorded for further investigation.

Both the spacecraft and ground should independently perform command logging and anomaly detection of command sequences for cross validation. Commands received may be stored and sent to the ground through telemetry and automatically checked to verify consistency between commands sent and commands received [7].



V. Industry Efforts to Address Satellite Cybersecurity

Despite industry efforts to improve cybersecurity in many areas of critical infrastructure, there has been little focus on cybersecurity for space systems. Space systems are more complex than other forms of critical infrastructure from a technology development, ownership and management perspective as has been previously noted (see Figure 3). This has historically led to a lack of guidance in the form of international standards that govern space system security, and ultimately, policies that enforce these standards [6]. It is only recently that certain cybersecurity policies, such as the NIST Cybersecurity Framework, have started to be considered in the frame of the commercial satellite industry [25].

Among the space industry community the lack of attention to cybersecurity is acknowledged; however the responses to cybersecurity threats have been variable. An audit of NASA in 2015 revealed the need for a revamping of their cybersecurity standards and protocols, citing several attacks that were not publically disclosed. NASA's efforts are not necessarily representative of the broader space industry's cybersecurity awareness and efforts, however smaller organisations working on satellites look to NASA for standards and best practices. More established private space companies such as SpaceX or Blue Origin have no public comments on their cybersecurity posture [6].

Neither public nor private space asset organisations are at a complete standstill concerning their cybersecurity efforts; however there remain considerable gaps in the space asset security posture compared with other critical infrastructure sectors, and these must be addressed.

V.1 Existing standards and regulation

The International Telecommunication Union (ITU), a United Nations agency, regulates frequencies of satellite communications to prevent communication interference and registers the orbits of satellites; but beyond these areas there are currently few standards. In 2007 the ITU created a "global cybersecurity agenda" intended as "a framework for international cooperation in cybersecurity"; however it seems there have not been considerable updates to this agenda since 2007 despite the changing landscape of cybersecurity. At this point, there are no agencies that restrict the use of satellites and there is no overarching governing body that monitors the specific use of satellites. Even if one did exist, there are currently no mechanisms for enforcing any treaties / standards / governance [16]. Research by Chatham House has described these deficiencies on a global scale in relation to the North Atlantic Treaty Organisation (NATO) and the need for a NATO Space Policy [22].

General IT-based cybersecurity standards or frameworks however are widely available, and most space system security could benefit from adopting these. One of the best examples is the NIST CSF (Cybersecurity Framework). A draft paper recently published by NIST in June 2021, "Introduction to Cybersecurity for Commercial Satellite Operations", is intended to introduce the CSF to commercial space businesses [25]. This includes describing a specific method for applying the CSF to commercial satellite operations; creating an example CSF set of desired security outcomes based on missions and anticipated threats; and describing an abstracted set of cybersecurity outcomes, requirements, and suggested cybersecurity controls. Another example is the CNSS (Committee on National Security Systems) Instruction 1253F (see Figure 4).

While efforts are being made to mould these frameworks for space systems, uniformity is lacking, and updated standards and guidelines for spacecraft are likely warranted [7]. There are pockets of initiatives across the space community that are addressing cybersecurity for space systems, however most work in this area to-date has focused on the ground segment with little research or guidance on securing the space segment (i.e. spacecraft).

Figure 4 outlines some of the known initiatives and standards that have been published relating to cybersecurity within the space domain. These range from high-level compliance controls to low-level communication protocol standards but are not overarching engineering principles for a spacecraft.

Organization	Title of Standard	Applicability/ Scope	Link to Standard	Description of Standard
CNSS	CNSSI 1200 National Information Assurance Instruction for Space Systems Used to Support National Security Missions	Ground and spacecraft for National Security System (NSS) only	https://www.cnss.gov/CNSS/issuances/Instructions.cfm	This standard elaborates on how to appropriately integrate information assurance (IA) into the planning, development, design, launch, sustained operation, and deactivation of those space systems used to collect, generate, process, store, display, or transmit national security information, as well as any supporting or related national security systems.
CNSS	CNSSI 1253F Attachment 2 Space Platform Overlay	Unmanned spacecraft for NSS only	https://www.cnss.gov/CNSS/issuances/Instructions.cfm	This overlay applies to the space platform portion of all space systems that must comply with CNSS Policy No. 12. The controls specified in this overlay are intended to apply to the space platform after it is launched and undergoing pre-operational testing and during operation. This overlay attempts to mold NIST 800-53 for the space segment.
Consultative Committee for Space Data Systems (CCSDS)	352.0-B Cryptographic Algorithms	Civilian space communications	https://public.ccsds.org/Pubs/352x0b2.pdf	This standard provides several alternative authentication/integrity algorithms that may be chosen for use by individual missions depending on their specific mission environments. It does not specify how, when, or where these algorithms should be implemented or used. Those specifics are left to the individual mission planners based on the mission security requirements and the results of the mission risk analysis.
Consultative Committee for Space Data Systems	355.0-B Space Data Link Security (SDLS) Protocol	Civilian space communications	https://public.ccsds.org/Pubs/355x0b1.pdf	This protocol provides a security header and trailer along with associated procedures that may be used with the CCSDS Telemetry, Telecommand, and Advanced Orbiting Systems Space Data Link Protocols to provide a structured method for applying data authentication and/or data confidentiality at the data link layer.
Consultative Committee for Space Data Systems	356.0-B Network Layer Security	Civilian space communications	https://public.ccsds.org/Pubs/356xb1.pdf	This standard provides the basis for network layer security for space missions utilizing the Internet protocol (IP) and complying with IP over CCSDS space links.
Consultative Committee for Space Data Systems	357.0-B Authentication Credentials	Civilian space communications	https://public.ccsds.org/Pubs/357x0b1.pdf	In the CCSDS space environment, credentials are needed to allow communicating entities to authenticate each other to determine potential authorization and access control actions. CCSDS recommends two types of credentials in this standard: X.509 certificates and protected simple authentication.
Aerospace Industries Association	NAS9933 Critical Security Controls for Effective Capability in Cyber Defense	Department of Defense (DOD) Aerospace contractors enterprise/ground infrastructure	http://www.aia-aerospace.org/wp-content/uploads/2018/12/AIA-Cybersecurity-standard-onepager.pdf	The goal of this standard is to align the fragmented and conflicting requirements that the DOD contracting process imposes on industry. Rather than different DOD organizations using different tools to assess a company's security across different contracts, this standard is designed to apply common and universal elements of cybersecurity across each enterprise.

Figure 4 – Known cybersecurity initiatives and standards within the space domain [7].

V.2 Public space asset organisations

NASA has taken several steps to improve security around space assets as follows:

- First, NASA has begun implementing stricter access control policies across their providers and engineers in order to help guard against the phishing attacks that have been used in the past to steal credentials and access intellectual property.
- Secondly, NASA has created teams across their space asset development centres that specifically work with the security of their missions systems. NASA's Jet Propulsion Laboratory (JPL) has created the Cyber Defense Engineering and Research Group (CDER) whose goal is specifically to address mission systems (e.g. the Mars Science Lab) which often have unique cybersecurity requirements. Some of CDER's work aims to develop tools and methodologies that apply across multiple mission systems to reduce costs and security operations.
- Finally, NASA has begun encrypting data while it is stored and during transfer. At the end of 2016 AT&T encrypted NASA's Deep Space Network (DSN), which is the foundation of communication infrastructure for interplanetary spacecraft missions. Somewhat ironically however this encryption was only performed after a report on how to hack into the Mars rover Curiosity appeared on the internet [6] [16].

NASA JPL's CDER Group is also working with university researchers at the Massachusetts Institute of Technology (MIT) to conduct penetration tests on mission system software. Increasing engagement with the broader security research community will considerably improve mission system security for space assets.

V.3 Private space asset organisations

Like NASA the private space asset industry is currently improving its security, but as previously mentioned, it is impossible to evaluate many private sector companies who are not transparent regarding their cybersecurity efforts. SpaceX, Virgin Galactic or other space asset developers, owners and operators do not make their technology readily available for security researchers to test. This is probably because they are concerned that their sensitive code or information will fall into competitors' hands.

Despite this, penetration testers, ethical hackers and security researchers are constantly finding holes in various satellite network systems and asking the responsible party to fix the vulnerabilities. Unfortunately these vulnerability notifications often go ignored due to manufacturers' lack of bandwidth to address the issues or mistrust of the hackers. The lifecycle complexities and associated liability questions discussed earlier (Figure 3) further complicate fixing vulnerabilities. If ignored, the ethical hackers generally follow responsible reporting procedures and expose the vulnerability to the public following a period of time after notifying the vendor. By publicly announcing the threat, the ethical hackers intend to garner large-scale attention to the problem and force the vendor to fix the issue. This was the case with the Iridium satellite owners who asserted their systems were extremely difficult to hack [23]. Only after ethical hackers announced their vulnerabilities and embarrassed the company did Iridium take steps to improve the security of their communication network [6].

VI. Present Insurance Standpoint

As of 2021, none of the established insurers provide coverage against cyberattacks in their policies. Prior to 2018 the majority of space insurance policies did not exclude hacking explicitly (although there were often exclusions that applied under certain conditions), and as a result there was often ambiguity over the extent to which cyberattacks may or may not be covered, both on the part of the insured and the insurers.

Since 2018 however the market has become more aware of cyber risks and policies have hardened with all now explicitly excluding cyberattacks. Many brokers now include a 'cyber coverage clarification clause' removing any possibility of a claim being made as a result of cyberattack. In cases where such a clause is not included by default, insurers will insist that one is included and it is now a Lloyd's requirement that all policies include some reference to cyber. Despite this, 'cyber incidents' whereby there is accidental interaction or natural failures associated with computer systems or data may still be covered.

VI.1 Cyberattack policy challenges

In the present market, brokers are looking for the first insurer to step forward and offer cyberattack coverage. However there are a variety of reasons why this has not yet happened including that these risks would not presently be covered under the insurers reinsurance. There is also uncertainty over whether coverage should be provided by space underwriters or alternatively cyber underwriters who have more experience of cyberattack risks (albeit not in the space domain). Additionally it is widely acknowledged that most insurers do not know what to charge for explicit satellite cyber coverage, given a lack of understanding of the risk involved and no precedent on which to base policies. On this last point it has been noted by one industry expert that: "The challenge is that insurers have to contend with a new and potentially catastrophic class of risk, with limited historical loss data on the nature and severity of the threat. To some extent therefore it is a jump into an unknown world where criminal, business and political/ strategic interests could be at play." [9]

"The challenge is that insurers have to contend with a new and potentially catastrophic class of risk, with limited historical loss data on the nature and severity of the threat. To some extent therefore it is a jump into an unknown world where criminal, business and political/ strategic interests could be at play." [9]

As was discussed at the start of this study, multiple points of vulnerability exist across the overall space system including space, user, link, and ground segments (Figure 1). Since the cyber risk is always a risk to the network, a specific cyber market for satellite operators may be needed because it is not only a risk to the spacecraft but rather a risk to the space-based service that the entire system provides. This is much wider than the legacy approach of risk to the reliability and success of each individual satellite [24].

Despite the challenges posed in developing dedicated cyber insurance policies for satellites, the experience gained in cyber insurance policies that have been developed for other large critical infrastructure (e.g. the energy sector) could be utilised as a starting point. Some cyber risks will be common across sectors, therefore similar insurance coverage could be proposed with modification for space specific threats and the associated wording to fit the operators' needs.

VI.2 Demand for cyberattack coverage

From the perspective of satellite operators it seems there is currently little demand for cyberattack coverage, with few if any specific requests to subscribe to dedicated cyber insurance policies. The reasons for this are not fully established, however the most probable reasons are that most operators still view the established in-orbit and launch risks (i.e. hardware reliability) as being of higher priority than the cyber risk, and secondly that they trust in the ability of their built-in defence mechanisms and cyber risk management to protect them against attack. Due to the heavy reliance of all satellites on IT, operators are generally expected to make sure they are adequately and proactively protecting against cyberattacks, regardless of whether they carry cyber insurance.

Demand for in-orbit insurance varies by operator, with some only seeking coverage for launch plus 1 year while others are more risk averse and look to cover all eventualities over the life of their satellites. While some may take the pragmatic approach and show interest in the pre-emptive development of dedicated cyberattack policies it is possible that the majority will only show greater enthusiasm once more significant losses attributable to cyberattacks materialise.

Conclusion

The aim of this study has been to provide an overview of the current state of knowledge surrounding satellite cyberattacks. Satellites are crucial for everyday life in our society and their importance is only set to grow in future. At the same time they represent a single point of failure within a tree of critical infrastructure, making them attractive targets to a range of different groups including state and non-state actors. The current lack of effective cybersecurity standards makes satellites easier to attack than if such standards were in place and systematically followed.

Satellites are crucial for everyday life in our society and their importance is only set to grow in future.

Satellites are vulnerable to attack from multiple avenues due to the highly connected nature of the overall space system, with the typical four major segments (space, ground, user, and link) each having their own vulnerabilities. As such it is not sufficient to consider only the satellite, rather the whole space system must be considered. The supply chain represents an additional vulnerability since the development of space systems is highly complex, requiring the involvement of many organisations.

In section I the potential consequences of a cyberattack were described. These include disruption of the service being provided by the satellite; whether it be communications, navigation, or some other service. Loss of satellite control represents one of the most severe potential consequences and the ability to commit such an attack has already been demonstrated. Many nation states around the world have developed capabilities to perform espionage on their adversaries via space systems.

Common modes of attacking a space system via cyber means were discussed in section II. The main points of access typically exploited include ground stations and the extended terrestrial infrastructure; the satellites themselves; and the supply, development, and operational chain. These forms of attack can result in unauthorised access to satellite control systems, the monitoring and modification of transmitted information, or the compromise of hardware and software design during satellite development.

In section III several case studies were presented of well publicised cyberattacks on satellites, specifically ROSAT, Landsat 7, and Terra EOS AM-1. Despite these examples, actual evidence in the public domain of cyberattacks against space systems is limited. Many other examples may go unreported because of the sensitive nature of such attacks and the unwillingness of operators to disclose the vulnerabilities (and/or defence mechanisms) of their systems.

Defence mechanisms are essential if a space system is to resist cyberattack. Section IV outlined several mechanisms that can be implemented specifically on the space segment (i.e. the satellite itself); including encryption and authentication, cyber resilience testing, supply chain risk management, and on-board logging. While each of these mechanisms can be effective in isolation, a thorough defence strategy should rely on multiple layers of security to protect the space assets.

In section V the current state of industry efforts to address satellite cyber security were described. Historically there has been little focus on cybersecurity for space systems, resulting in the present lack of guidance in the form of international standards, and policies to enforce these standards. More general IT-based cybersecurity standards exist and efforts are being made to apply these to space systems, for example the recently published “Introduction to Cybersecurity for Commercial Satellite Operations” by NIST. Public organisations such as NASA are taking steps to improve cybersecurity around space assets, however private organisations are not transparent about the actions being taken and so it is hard to evaluate the progress being made.

Finally in section VI a brief review of the present insurance standpoint regarding satellite cyberattacks has been given. As of 2021, none of the established insurers provide coverage against cyberattacks in their policies. Several challenges inhibit the development of cyberattack coverage, not least of which is that multiple points of vulnerability exist across the overall space system. Despite the publicity surrounding cyberattacks in the modern age there is currently little demand from operators for cyberattack coverage, with the majority still viewing the established in-orbit and launch risks (i.e. hardware reliability) as being of higher priority.

In conclusion, while it is clear from this study that the risks to satellites from cyberattack are real and of growing concern, it is also evident that the space sector has so far taken a non-regulated approach towards addressing the threat. The current lack of international standards and policies towards satellite cybersecurity principles is an area of weakness that needs to be addressed. The information available suggests that consideration is being given to cybersecurity by national institutes and both public and private space asset organisations, however in the case of the latter it is very difficult to judge the extent to which satellite cybersecurity measures are being implemented. While there are many ways in which a cyberattack can be made, there are a range of defence mechanisms that can be implemented at the design and development stage. Any modern satellite should ideally incorporate a selection of such defences, thereby providing it with multiple layers of security control.

The insurance industry currently does not provide policies that cover cyberattack alongside the established hardware reliability risks associated with launch and in-orbit operations. Challenges facing the development of such policies include the unique complexity of the overall space system and therefore the difficulty in attributing liability in the case of a claim. Despite this many brokers and insurers alike have shown an interest in furthering their understanding of the cyber threat. In one example of this an insurer recently provided financial support for research into satellite-to-satellite cyberattacks [13]. A specific cyber market for satellites may need to be developed rather than incorporating cyber coverage in existing policies. While the challenges could be overcome with a determined and collective effort, there also needs to be demand from operators for cyberattack coverage. At the present time this demand is not apparent, however if the threat from cyberattacks grows in future as is expected then more operators may start to show an interest in obtaining coverage.

It is worth noting again the very limited number of satellite cyberattacks that have been published in the public domain. A comprehensive space data publisher has only three examples of cyberattacks against satellites within its database (the three case studies given in part 3 of this study). This risks giving the impression that cyberattacks are exceptionally rare and of minimal concern. On the contrary, it is known that cyberattacks against satellites are not uncommon and that the potential consequences of an attack can be severe. It is therefore imperative that if policies covering cyberattacks are to be developed then a much deeper library of historical loss data is required.

Despite the challenges in developing satellite cyberattack policies, we foresee a growing need. We understand, however, to develop satellite cyberattack policies will require reaching out to the industry, investment in further research, market study and the acquisition of historical loss data.

References

[1] Rajeswari Pillai Rajagopalan, UNIDIR, "Electronic and Cyber Warfare in Outer Space," 2019. [Online]. Available: https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf.

[2] Defense Intelligence Agency, "Challenges to Security in Space," 2019. [Online]. Available: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[3] Center for Strategic & International Studies, "Space Threat Assessment 2019," 2019. [Online]. Available: https://aerospace.csis.org/wp-content/uploads/2019/04/SpaceThreatAssessment2019-compressed.pdf.

[4] Airbus, "Protecting everyday life – How Airbus protects satellite systems against attacks," [Online]. Available: https://airbus-cyber-security.com/news/protecting-everyday-life-how-airbus-protects-satellites-against-attacks/.

[5] Secure World Foundation, "Global Counterspace Capabilities: An Open Source Assessment," 2018. [Online]. Available: https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf.

[6] Belfer Center, Harvard Kennedy School, "Job One for Space Force: Space Asset Cybersecurity," 2018. [Online]. Available: https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf.

[7] The Aerospace Corporation, "Defending Spacecraft in the Cyber Domain," 2019. [Online]. Available: https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf.

[8] A. Gini, "Cyber Crime from Cyber Space to Outer Space," Space Safety Magazine, 14 02 2014. [Online]. Available: http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/cyber-crime-cyber-space-outer-space/. [Accessed 5 March 2021].

[9] Chatham House, The Royal Institute of International Affairs, "Space, the Final Frontier for Cybersecurity?," 2016. [Online]. Available: https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

[10] TIME magazine, "Did Hackers Hijack a British Military Satellite?," 01 03 1999. [Online]. Available: http://content.time.com/time/magazine/article/0,9171,20673,00.html. [Accessed 22 February 2021].

[11] WIRED, "Russian Spy Gang Hijacks Satellite Links to Steal Data," 09 09 2015. [Online]. Available: https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/. [Accessed 22 February 2021].

[12] Via Satellite, "The Growing Risk of a Major Satellite Cyber Attack," [Online]. Available: http://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/. [Accessed 23 February 2021].

[13] G. Falco, "When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience," American Institute of Aeronautics and Astronautics, 2020.

[14] Attila Security, "Cyber Concerns For The Satellite Sector," [Online]. Available: https://www.attilasec.com/blog/satellite-cybersecurity. [Accessed 23 February 2021].

References

[15] The Consultative Committee for Space Data Systems (CCSDS), “Security Threats Against Space Missions,” 2015. [Online]. Available: https://public.ccsds.org/Pubs/350x1g2.pdf.

[16] G. Falco, “Cybersecurity Principles for Space Systems,” Journal of Aerospace Information Systems, 2018.

[17] GCN, “Hackers could shut down satellites -- or turn them into weapons,” 12 02 2020. [Online]. Available: https://gcn.com/articles/2020/02/12/hackers-satellites.aspx. [Accessed 24 February 2021].

[18] Via Satellite, “NASA Computers Hacked By Intruders,” 01 12 2008. [Online]. Available: https://www.satellitetoday.com/government-military/2008/12/01/nasa-computers-hacked-by-intruders/. [Accessed 24 February 2021].

[19] CSO, “What is quantum cryptography? It’s no silver bullet, but could improve security,” 12 03 2019. [Online]. Available: https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.html. [Accessed 25 February 2021].

[20] Forbes, “ManTech ‘Space Range’ Simulates Cyberattacks On Satellites & Ground Stations To Bolster Defenses,” 12 06 2020. [Online]. Available: https://www.forbes.com/sites/lorenthompson/2020/06/12/mantech-space-range-simulates-cyberattacks-on-satellites--ground-stations-to-bolster-defenses/?sh=12af469140f7. [Accessed 25 February 2021].

[21] ESA, “ESA practices cybersecurity,” 07 11 2019. [Online]. Available: https://www.esa.int/Safety_Security/ESA_practices_cybersecurity. [Accessed 4 March 2021].

[22] Chatham House, The Royal Institute of International Affairs, “Cybersecurity of NATO’s Space-based Strategic Assets,” 2019. [Online]. Available: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf.

[23] VICE media group, “It’s Surprisingly Simple to Hack a Satellite,” 21 08 2015. [Online]. Available: https://www.vice.com/en/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite. [Accessed 26 February 2021].

[24] World Space Risk Forum, “Newsletter Issue 3,” February 2016. [Online]. Available: https://www.worldspaceriskforum.com/contents/blog_post/document/newsletters-3.pdf.

[25] National Institute of Standards and Technology, “Introduction to Cybersecurity for Commercial Satellite Operations” June 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8270-draft.pdf. [Accessed 2 July 2021].

HDI Global Specialty SE
10 Fenchurch Street,
London, EC3M 3BE
United Kingdom

Tel. +44 20 7015 4000
hdi-specialty.com