Commercial Space System Security Guidelines

Edited by Harrison Caudill & Chris Wake, Orbital Security Alliance

rev-1.0.1 – February 1, 2020

For some time, the question of "What should we be doing to protect our space assets?" has been posed and discussed. While there is not yet a widely-accepted answer, some partial answers are known such as the use of multifactor authentication for critical systems, encrypted communications links with proper key management, and throwing salt over your left shoulder before performing in-orbit software upgrades. Other approaches (such as use of quantum communications and formal methods verification of core systems) require further research and development before widespread adoption.

Additionally, the appropriate magnitude of execution is often unclear. For example, "use of multifactor authentication" can be equally satisfied by sending a text message to a cell phone or by utilizing a hardware token that is unlocked with biometrics and kept in a safe in a secure building. Both solutions are, technically, "use of multifactor authentication" but are decidedly *not* equal. Utilizing a risk-based approach to assess appropriate magnitudes depends upon an appropriate shared understanding of those risks, and appropriate countermeasures.

In an effort to advance the conversation within industry, the question was restated as "What are *some* of the things that we should be doing to protect our space assets?" and was posed to various organizations. This paper contains a collection of such partial answers. As described in the previous paper, *Big Risks in Small Satellites*[54], the presented solutions are also amenable to implementation as services so as to permit rapid and widespread industry adoption at low cost.

info@orbitalsecurity.space

Contents

1 Introduction

Harrison Caudill *Orbital Security Alliance*

1.1 Scope

Space assets and infrastructure should be protected in proportion to the threats against them and the threat to the nation should they be compromised. Four categories of assets may be broadly recognized:

1. Assets which are directly utilized by the DoD.
2. Assets deemed critical for national functions.
3. Assets which, if compromised, could represent a physical threat to orbital systems.
4. Assets which may be of benefit to an adversary if compromised.[1]

Each category represents a different type of threat, resulting in slightly different security requirements:

1. Assets utilized by the DoD must protect confidentiality of data in addition to operational integrity.
2. Critical systems must be protected not only from being commandeered, but also from interference to ensure continued availability.
3. If a spacecraft has the hardware necessary to perform precision orbital maneuvers, then the ability to neutralize that hardware is necessary.
4. If a spacecraft contains a payload which would be of benefit to an adversary, then the spacecraft must retain the ability to neutralize that payload.

As category 1 infrastructure is already covered by CNSS Policy 12, this paper will primarily address categories 2, 3, and 4.

1.2 Reference Architecture

It is understood that this reference architecture may not be representative of any specific space mission. It is intended to provide a basic vocabulary for use in later sections.

1.2.1 Critical Components

- **On Board Computer (OBC):** Like most devices under control, satellites will utilize at least one computer capable of controlling other on-board systems.
- **Telemetry, Tracking, & Control (TT&C)** Typically a low-speed omni-directional radio link, a TT&C link provides the three essential services for which it is named.
- **Service Link:** Radio link intended and licensed for transmitting payload data.

[1] This category includes any payload which would be weaponized against us, such as any agile transmitter which could be made to interfere with legitimate communications.

- **Thrusters:** Most thruster systems utilize chemical propellants which provide high thrust for short durations.
- **Attitude Control Systems:** To utilize sensors, high-gain antennas, and thruster systems, satellites must be able to orient the satellite.
- **Mission Operations Management System (MOMS):** Software running on a combination of the spacecraft and various ground systems will coordinate execution of missions (such as imaging a target area).
- **Payload:** All other spacecraft systems exist for the benefit of the payload, it provides the services for which the spacecraft was designed.

1.2.2 Flow of Information

Mission execution is typically fully automated, but can also be a consequence of direct human involvement. For example, a system designed to consistently gather weather data may operate autonomously and continuously, while a software update may be the result of an operator rolling out new software.

- (Optionally) Operator defines a mission within the MOMS to be executed by a specific spacecraft.
- The TT&C communications link is utilized to transmit the mission to the spacecraft.
- The OBC instructs the payload and executes the mission.
- Any resulting data are collected by the OBC.
- Resulting data are transmitted back to the ground-side server systems utilizing the service link.

1.2.3 Commoditized Services

By commoditizing and securing services which provide communications services (both TT&C and Service) as well as MOMS, many of the security risks associated with spacecraft may be neutralized.

1. **Utilized by DoD:** Secure infrastructure service providers could be a significant part of a Policy-12 compliance strategy.
2. **Critical Assets:** Operational integrity of critical assets may be ensured.
3. **Physical Threats:** Secure communications/operations guarantee the ability to neutralize thruster systems.
4. **Adversarial Advantage:** Payloads which may be desired by a foreign adversary may be disabled securely, denying that advantage.

Several obvious blind spots exist in this architecture. For example, a payload which is compromised from manufacturing presents an attack vector to the entire spacecraft and could result in a critical asset being denied when needed. This architecture is intended to follow the 80/20 rule, providing 80% of the benefit at 20% of the cost.

2 Status of Cybersecurity in the Industry

Dr. Gregory Falco *Orbital Security Alliance*

Currently, there is no single authority that provides regulatory oversight for space security. Generally speaking, space security oversight falls into two categories: national security systems, and commercial remote-sensing systems. While national security systems have a relatively well-developed process for validating their security, the commerical side is woefully underdeveloped, to the point where commercial organizations are openly calling for guidance.[1] The process available to national security actors is ill-equipped to handle the growing number of actors in space leaving an effective vacuum of cybersecurity.

2.1 Commercial-Only Space Systems

NIST is no stranger to high-impact cybersecurity standards. NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* is the gold standard for federal systems, whereas NIST SP 800-37 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* has become a common reference across the security industry. Space systems are no stranger to these standards.

The US Code of Federal Regulations (CFR), title 15 §960 also establishes some minimum requirements for cybersecurity of federal space activity including a mandatory review.[2] Chapter 4, parts 3 and 4 of the appendix outlines requirements for the ground segment of remote sensing space systems which includes plans for the protection of any data links and plans for the integrity of operations. However, there are no explicit measures or controls recommended, leaving this open to interpretation of the designer. Some industry participants have also been known to actively hide pertinent detail from these filings to avoid leaking proprietary information.[2] Even if good-faith compliance was not an issue, these requirements only apply to the ground segment for remote sensing space missions. If the mission is not remote sensing (such as a communications satellite) it does not apply; nor does it apply to the space segment.

Finally, while not explicitly a standard, policy or regulation, insurers require minimum cybersecurity requirements for certain space asset coverage. Launch insurance which covers space asset launch procedures may require certain software security provisions for compliance with the insurance policy. This varies by insurer and policy, however could be a means for enforcing cybersecurity in space assets.

2.2 National Security Missions

In December 2018, a bill was introduced and quickly signed into law by the U.S. House of Representatives called H.R.7327[3] *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act*. This law made provisions for requiring supply chain security for any federal acquisitions process. The Act provided little guidance on how this should be deployed, therefore NIST and the Department of Defense (DoD) have embarked to outline the means for vendor security to be released in 2020.[55] Because the federal government is a large buyer of space assets, the space industry is subject to H.R. 7327 and must ultimately comply with the upcoming guidance from NIST.

Commercial space systems utilized for national security purposes must be in compliance with Committee on National Security Systems (CNSS) Policy 12 (*Cybersecurity Policy for Space Systems used to Support*

[2]Confidential source.

National Security Missions).[4] However, that policy is designed to support the needs of the Intelligence Community (IC) in concert with the heritage space community. With the growing availability of parts, services, and launches to small startups and hobbyists, this process is not well-suited to the needs of the market:

- **Scalability:** One of the more enforceable and effective portions of Committee on National Security Systems Policy (CNSSP) 12 is the mandatory review by the National Security Agency (NSA). It seems unlikely that the NSA would have the time/availability to perform in-depth reviews of every hobbyist wishing to include a thruster, nor is there a mechanism for the general public to do so.
- **Privacy:** CNSSP 12 also requires use of cryptographic systems approved by the NSA. With a history of credible allegations of introducing "back-doors"[5] into such crypto-systems, it seems unlikely that privacy-sensitive commercial organizations would hesitate to utilize such an approved cryptographic stack.
- **Availability:** Much of the guidance of CNSSP 12 is not even available. Several of the attachments to Committee on National Security Systems Instruction (CNSSI) 1253, for example, are classified as For Official Use Only (FOUO).
- **Scope:** National security assets don't just require the Integrity of the Telemetry, Tracking, & Control (TT&C) links, or on-board systems, they also require high Availability so that they might be utilized in times of conflict, and also Confidentiality of the resulting data. Protecting national security interests usually only requires Integrity of the TT&C systems and a few on-board components for commercial systems.

While commercial adoption of CNSSP 12 may be widespread, with the DoD leveraging commercial assets for the bulk of their telecommunications needs, it is not well suited to the burgeoning commercial smallsat market. It is largely designed around the paradigm of a large heritage space company working closely with the intelligence community. As such, much the content and resulting processes and norms are of little utility to the upcoming majority of the industry.

In this early stage of the small satellite and commercial space industry, there is a unique opportunity to establish precedent for future generations of technology. The most critical legacy that early pioneers in the commercial space sector can leave is establishing a baseline of security for these assets. Considering cybersecurity is not a new discipline, it is critical to draw from effective cybersecurity practices in other sectors that are still relevant to the unique requirements of space assets. While space assets have a wide array of functionality and limitations, managing the cyber risk of these systems is essential to the health of both the asset as well as the ecosystem of space systems. Future efforts are needed for regulatory bodies to adopt compulsory measures regarding commercial space asset cybersecurity. Without such requirements, it will take decades for the industry to evolve.

Part I: Immediately Deployable Solutions

As discussed earlier, many approaches and partial solutions are currently known and can be implemented immediately. Those partial solutions are discussed here.

3 Operational Integrity of TT&C

Karl Mattson *LA Cyber Lab*

Telemetry, Tracking, & Control (TT&C) systems are indispensable services aboard every satellite and space vehicle, providing the vital telecommunication link between a satellite and ground station. They provide the uplink for command, downlink for monitoring the various health parameters through telemetry, and tracking information for the satellite for monitoring its position in orbit. TT&C system integrity must be assured continuously, as it is foundational to the satellite's overall protection from compromise or misuse.

We find a useful and relevant comparison of the TT&C systems to the global banking system's Society for Worldwide Interbank Financial Telecommunication (SWIFT) network. Across the SWIFT network each day, global financial institutions perform over 24 million transactions amongst 10,000 member organizations.[6, p63]

The daily value of money transacted over the SWIFT network is over $5 trillion per day ($1.25 quadrillion dollars annually), making it vital to economic health around the world. While SWIFT member institutions have been victimized by cyber fraud, such as the Bank of Bangladesh attack in 2016, the overall integrity of the SWIFT network itself is remarkably successful by any measure. It also continues to improve with a robust SWIFT Customer Security Program, outlined further below.

The SWIFT financial network is notable in the diversity of banks and bank technologies which operate securely on the underlying SWIFT network. The SWIFT security model provides an excellent example of how diverse and decentralized assets can still operate with high assurance and effective security controls. There is broad diversity in types of satellite and space assets which can be interconnected, a factor which is not prohibitive in achieving high assurance and integrity of TT&C systems, should a relevant security model be adopted by nodes or participants on the network.

A key success factor in the security of the SWIFT network is the Customer Security Program (CSP). Mandatory security controls outlined by the CSP establish the minimum security standards for SWIFT participants, as well as the self-reporting requirements which provide transparency to other relevant parties within the SWIFT network.

SWIFT CUSTOMER SECURITY CONTROLS FRAMEWORK v2019

OBJECTIVES	PRINCIPLES	CONTROLS
Secure your environment	▪ Restrict internet access ▪ Protect critical systems from general IT environment ▪ Reduce attack surface and vulnerabilities ▪ Physically secure the environment	29 total security controls ▪ 19 mandatory ▪ 10 advisory controls CSCF v2019 ▪ Promotes 3 advisory controls to mandatory controls ▪ Introduces 2 new advisory controls
Know and limit access	▪ Prevent compromise of credentials ▪ Manage identities and segregate privileges	
Detect and respond	▪ Detect anomalous activity to systems or transaction records ▪ Plan for incident response and information sharing	

[7]

Figure 1: SWIFT Cyber Security Framework (CSP)

3.1 TT&C Integrity Model

Borrowing heavily from the SWIFT CSP security model, the TT&C Integrity Model is articulated around three mutually reinforcing areas. Operators first need to protect and secure their local environment (Self), then about prevent and detect the compromise of peers (Peers), and then continuously share information and prepare for future cyber threats (Community).

3.1.1 Protect and Secure Local Environment (Self)

In this phase, we introduce the need for a TT&C Security Controls framework focused on the security of local TT&C systems - a series of common sense, but mandatory, set of controls required by satellite operators to achieve a base level of assurance for TT&C systems.

Society for Worldwide Interbank Financial Telecommunication's (SWIFT's) security controls framework consists of 29 security controls, including both mandatory and advisory controls. The mandatory security controls establish a security baseline for the entire community and must be implemented by all users on their local SWIFT infrastructure. Over time, mandatory controls can and should evolve due to the evolving threat landscape and technology advancements.

We find that only minor adjustments or language clarifications of the SWIFT CSP controls would be necessary to apply as an effective TT&C systems security control framework. The controls and control language are largely agnostic to industry or vertical, and have been proven to be effective approach in practice.

Another important success factor in the SWIFT CSP framework is that it is an "applied" framework, allowing members to consider controls applicable for their particular architecture, with guidance as to what architectural factors (internally hosted, third party hosted, etc.) drive control assessment assertions.

3.1.2 Prevent and Detect Compromise of Peers (Peer)

Satellites and space vehicles are interconnected, and therefore reliant on the integrity of other network nodes and participants. Even with strong security measures in place, sophisticated attackers can identify weaknesses to use as an entry point for subsequent lateral network movement. It is vital to manage security risk in interactions and relationships with other network participants in two ways:

If you are breached: Routine reports of assurance to a central authority which provide confirmation of ongoing integrity. In the SWIFT network, the emphasis is on daily reconciliation of account balances to serve as confirmation that integrity has been maintained prior to close out for the day. For TT&C systems, assurance reporting would be a net new design requirement.

If your peer is breached: Receive and review peer assurance reports to identity a) potential exposure to a compromised peer and b) forensic or historical information that may be relevant to the peer event.

3.1.3 Share Information and Prepare (Community)

Cyberattacks against TT&C systems can be replicated quickly. Sharing information is vital to ensure that information and indicators of compromise (IOCs) are shared accurately and quickly to peers in order for cyber defenses to be updated in response. [3].

Despite the assurance level of TT&C systems, it is inevitable that some subset of systems will be compromised at some point in time. As such, preparing through incident response planning and exercises is important to reduce the duration and impact of a compromise. SWIFT, for example, hosts a variety of member/participant exercise events which provide network participants a venue for training, practice and education. An important role fulfilled by an Information Sharing and Analysis Center (ISAC) type model is to serve as a host/coordinator for exercise events and the knowledge sharing amongst peers.

The SWIFT CSP also has two practical elements which promote adoption and guide its diverse member base towards uniform compliance with the standard – a major hurdle given the diversity in volume and technology across its global banking members. First, each CSP security control is supported by recommended implementation guidance and a description of the specific SWIFT IT components to which the control applies. This provides members the specificity in implementing controls which minimizes ambiguity or interpretation. Second, the SWIFT guidelines also prompt the user to select the type of technology architecture used by the member bank – internally hosted, externally hosted, Software-as-a-Service (SaaS) or hybrid. Based on the member's SWIFT technology footprint, only the security controls applicable to that footprint are deemed relevant. This tailored application of the framework is a design highlight which we anticipate modeling for space vehicle and satellite technical patterns. The standard is set uniformly at a high level, and the formal guidance to achieve or tailor appropriately is specific and relevant.

Key Recommendations	
Recommendation	**Level**
Adapt and adopt the mandatory security controls recommended by the SWIFT CSP to protect the operational integrity of the TT&C system.	–

[3] Intelligence and information sharing is covered in more detail in section 7

External References	
Reference	**Organization**
SWIFT Customer Security Program[8]	SWIFT

4 Guidelines for Physical Layer Security

Mark Lombardi, James Low, & Phil Trainor *Keysight Technologies*

When modelling the security risk for satellite networks, it's crucial to pragmatically assess all possible venues of exploitation. These avenues can exist prior to deployment within the supply chain of vendors, during assembly, or post launch via radio frequency attacks. Action items must be assigned to remedy risk factors for our model. Overly focusing on one aspect, such as radio frequency attacks, while ignoring physical security during assembly, or not properly vetting a supply chain, leaves an open window for security risk.

The primary risk to satellite networks is an enemy combatant, or malicious organization, taking control of the satellite network and using the resource for themselves in two specific manners:

- Mislead and/or withhold crucial information or relayed messages from the original owners
- Using the productive resources of the satellite for their purposes

Secondary risks include loss of connectivity of the satellite network due to intentional failure and sporadic failure of crucial functionality.

Risk, including security risk, cannot be eliminated until it is quantified through pragmatic modelling. This section will define specific areas of risk as well as steps for mitigation.

4.1 Risk Modeling, "Probability of Physical Intercept"

In order to better characterize the risk at the physical layer, it is useful to extend the concept of "probability of intercept." This concept can help categorize the various threats to the physical layer.

Probability of "Physical Intercept" is useful in discussion of physical accessibility to a particular component in the satellite network. In prioritizing threats, it is clear that once a satellite is in space it is effectively air-gapped and difficult to physically alter. With ever increasing access to space, this may become an issue, but for this document, will be considered low risk. The more important physical risk to the satellite is when it is on earth, and it can be physically altered. Typically, securing the supply chain is discussed as an example of insuring counterfeit parts or code do not enter into the design. While this is discussed in §8, the intent of this section is to highlight the importance of traceable processes to mitigate the overall risk when the satellite is physically accessible. This puts a high importance on using mission based design, with integrated design flow that allows for resilient tracking of every aspect of the satellite's development. Every component, every line of code, every verification test should be centrally managed and interconnected in a digital design flow. The intention of this approach is to provide visibility and checks to a digital model that runs in parallel throughout the design. This becomes a critical tool for detecting deviation, whether a resistor, or line of code between the intended design and the one ultimately in space.

While the satellite will eventually be air-gapped, the ground segment by definition will not. There are two

points of concern for the ground, the control segment and user segment. Access to hardware that can impact the user segment and experience can have negative impacts on a business model, but access to the satellite command and control has dire consequences. The ground stations of the past typically were few and effectively air-gapped with secure parameters, fences, and locked rooms. This may still be viable protection for Telemetry, Tracking, & Control (TT&C) moving forward, but constellations are driving the access points up, increasing the risk of physical access to critical infrastructure.

4.2 Risk Modeling, "Probability of Electrical Intercept"

Once the probability of physical intercept has been reduced, the issues that bridge an air-gap need to be addressed. This concept can be thought about as mitigating the probability of electrical intercept.

In order to electrically interface to an air-gapped system, typically their needs to be line-of-site. At low frequencies there can be exceptions to this, and it is important to point out that the line-of-site could be from land or space. The most basic example would be a Geostationary Orbit (GSO) satellite with a single large coverage antenna. Effectively the satellite is always accessible anywhere in the one-third of the planet illuminated by the hypothetical wideband transmit/receive antenna. While this type of system could theoretically be sent an interfering signal from almost anywhere, there are highly effective geolocation systems for quick identification and location of the problematic signal. If the GSO satellite is utilizing spot beams or an electronically steerable array, then the locations of most likely intercept are in the "illumination" spots of the antenna. This can include unintentional locations where sidelobes of higher gain might exist. It should also be mentioned that with enough power, even a low gain portion of the receive antenna might be vulnerable.

For Non-Geostationary Orbit (NGSO) satellite systems, their constant motion with respect to the ground provides protection from a persistent electrical intercept. Only when the satellite is over a particular area of concern and the receive antenna illumination covers the origin of the interference is there a potential for intercept. It is worth mentioning that with the increased access to space, there could be instances of intercept from satellites flying lower orbits.

There are a number of orbital modeling tools that can be used to examine the basic relationships between the space platform and points of concern on the ground, in space and time. Most can implement simple sensors to illuminate the approximate antenna coverage. Knowledge of potential issues is the first line of defense.

Once a physically viable method of intercept is established, there are a number of topics to be covered around particular radio designs that are more or less susceptible to electrical interference. In the past the air-gap to a satellite was considered sufficient protection. The satellite network could be designed purely around simplicity and power efficiency of the satellite. The ground station locations were typically chosen for clear line-of-site and typically did not have to be designed to tolerate interference. The designs could utilize simple, efficient modulation types focused on ease of generation and reception. With growing concern for electrical interference, modulations and methods more commonly found in terrestrial applications are now becoming more prevalent. They include frequency agility and wideband modulation methods, which effectively lower the probability of intercept, by either not staying at one frequency, or by spreading the data across large frequency bands with Orthogonal Frequency Division Multiplexing (OFDM) modulations. The growing use of software defined radios (SDR) and phased array antennas, allow for much greater flexibility and adaptability to mitigate the probability for interference and intercept.

As the communication payload or TT&C design is being formulated, software simulation tools that model the RF system should be considered. Trade studies can illustrate potential susceptibilities of a particular modulation type or most likely interference. Once the hardware has been selected, hardware-in-the-loop test should be utilized to analyze the robustness of critical receive paths. Even while testing is being executed in the lab, attention should be paid to recreating the actual dynamic signal conditions that the system will experience from space. Cross checking results using multiple sources of "truth", can provide an additional layer of confidence that the parts and design being built are the same and therefore less likely to have been altered. This approach can be carried all the way into operations. By using high fidelity downlink monitoring along with knowledge of the system operational norms, deviations from normal physical operational parameters can be identified.

Once the signal path has successfully transitioned through the RF path or layer 1, it is time to consider the upper layers of the transport system.

4.3 Need for Hardening IP Packet Transport Systems in Satellite Networks

Failure to appropriately manage the security risk of critical satellite networking infrastructure through hardening can lead to failures in the integrity of those systems where adversaries can compromise individual operations and, possibly, national security. Risk can be defined as the confidence level of the integrity of satellite function with respect to secure, uninterrupted telemetry. Satellite telemetry is facilitated by IP Packet Transport Systems which are comprised of networked infrastructure. All network infrastructure, including the satellites themselves, are subject to risk of compromise. As a precursor to hardening, the risk must be modeled. Once risk is completely understood through modeling, a clear methodology of hardening can be defined and implemented. Hardening IP Packet Transport systems can be defined as the methodical reduction of the defined risk.[4]

4.4 Risk Modelling and Hardening

When evaluating the risk within a satellite system, even if the system is completely air-gapped, the attack surface is always the starting point for evaluating risk. The attack surface can be defined as all available venues in which to communicate with either the endpoint satellite or any aspect of the IP Transport System. Unnecessary communication scenarios increase the risk of compromise and must be eliminated during the process of hardening. Once the entire system has been boiled down to the most efficient configuration, hardening of the existing networked services can take place. Hardening of critical networked services can be defined as the process of ensuring that unauthorized or unintended commands cannot compromise the fidelity of the system. This practice will be discussed further in this document.

Many of the security protections in place today are inherently designed to protect sensitive data. A brief analysis of security tools in the industry demonstrates that the primary objective is to mitigate the threat of compromise to protected information. But what if the objective of an attack is not just access to information, but to compromise the underlying asset and jeopardize mission success?

This question, when asked, is one that shifts the strategy from focusing only on cybercriminals to including state actor threats. The mission objective of a state actor may not only be compromise and collection of sensitive information, but also to disrupt, deny or destroy an asset. When this is included in analysis of total threat, it significantly increases the surface area that must be addressed. It goes beyond using appliances

[4] A method of hardening the surrounding network is discussed in §3.

and software to protect assets. It forces re-assessment on not just protecting the data and data systems, but also maintaining operational uptime of the network components as well.

There is no single off the shelf tool for ensuring a network device is hardened against potential threat. Rather there are some best practice guidelines that should be followed to maximize the capability to withstand an attack. The best practices for ensuring that a network device can withstand a targeted persistent threat can be categorized into three areas: 1) Engineering a robust network device; 2) providing a secure network; and 3) adherence to security policy.

4.5 Engineering a Robust Device

Network devices are an example of a complex integration of hardware and software. This complex integration is further pressed by the necessity for these devices to interoperate with other devices in order to operate effectively. Failure of integration or interoperability is managed with error handlers in the code to recognize the fault and either report or restart the process, depending on criticality.

It takes only moderate skill for a hacker to exploit error handlers in network devices, gain access and persist permanently in network systems and hardware. Forcing a process to restart on a security device, especially if it is related to applied policy, might allow an attacker to bypass security policy. Even an inline network device, forced to execute an unplanned reboot, can provide timely disruption to operations and intelligence at a critical juncture in the mission. In addition to a reboot, malformed packets can be part of a well planned, targeted attack to compromise a device and enable direct code injection for nefarious purposes.

Injecting a malformed packet to a router may cause a denial of service by hanging process or causing the router to reboot. Most of these types of exploits can be mitigated with careful implementation of protocol standards, system design and thorough testing, not only by the vendor, but by the implementer as well. The following are a few recommendations for validating system robustness addressed to individual responsibility:

Malformed Packet: The equipment manufacturer tests the device to ensure that protocol stacks do not process malformed packets. This includes the individual packet or any packet that is out of communications sequence within an industry defined standard. Protocol fuzzing is one effective method to validate packet handling. Fuzzing presents a valid header with invalid data to determine how a device responds.

Memory Leak: The equipment manufacturer tests the device to ensure that the memory is managed effectively. Processes that impact forwarding are especially susceptible to leaks. An exploit by an attacker can overload memory utilization and force a device reboot.

Interoperation: The implementer tests device operation with a focus on protocol interoperability in delivery of an end to end system. This testing is critical to fill in the gap from the vendor. The vendor will have resource limitations to the number of unique permutations it can test against. A breakdown in protocol sequence that is caused by an interoperation issue may inject an unhandled packet and cause a denial of service.

4.6 Providing a Secure Network

Device exploits can in effect be mitigated by a comprehensive network security policy. A network security policy must be able to do the following to protect the underlying network devices:

DoS, DDoS mitigation: This is recognition of data structure and traffic patterns that indicate a potential DoS, DDoS attack. Not all attacks will be brute force and easily recognizable through automated detection. The security team will also require periodic training on recognizing potential threats.

Network Segmentation, Whitelisting: Network segmentation is a design policy that breaks up the network into subnets based on necessary interaction between devices on that subnet. Effective use of this practice will limit direct network access from standard user systems to mission critical transport devices. This significantly reduces the threat surface of the network device. It is also recommended to use a "whitelist" policy for access to these physical devices. A whitelist ensures that only IPs from known trusted devices are allowed to connect to that physical device.

Protection of the physical asset: A physical security policy that considers threat and mitigation to threat is needed not only for network assets under direct control, but also considered for assets that are leased or not under direct control of a party that can immediately guarantee the safety of the physical asset.

If physical protection is not possible due to asset location, consider how to minimize disruption to mitigate a critical failure. Some strategies to consider are limiting sensitive data transmission over infrastructure that is not under direct supervision or to have alternate sites as terrestrial backup paths for segments that are less physically secure.

4.7 Adherence to Security Policy

It is recommended that any device included in the communications path is certified and accredited as defined in NIST special publication 800-37. Because network devices operate transparently, they can be easily missed when assessing overall security posture.

Key Recommendations	
Recommendation	**Level**
Be cognizant of the probability of electrical intercept when operating antenna systems.	e.g. Don't do software upgrades from insecure ground stations.
Trust but verify. Only believe what can be proven, and understand that this principle applies equally to networking switches as it does to wireless networking chips.	e.g. Assume inaccuracy in every data sheet, and only believe what you can prove in the lab.
In secure ground stations, employ sophisticated monitoring systems looking for signal anomalies beyond just quality of service.	e.g. Monitor for transmissions that occur before a contact begins, and after it ends.
Utilize a signal spreading technique to guard against impersonation, and possibly also confer jamming resistance.	e.g. DSSS with a chip rate of $\geq$8
Utilize strong encryption on all communications.	e.g. AES 256
While beyond the scope of this section to properly define, it is crucial to ensure strong Network Access Controls are employed to guard the sensitive Radio Frequency systems.	–

External References	
Reference	**Organization**
Zero Trust Architecture: Draft NIST SP 800-207[9]	NIST
Risk Management Framework[65]	NIST
Spectrum Spreading[10]	Telesat
Application Note 1313 - Testing and Troubleshooting Digital RF Communications Transmitter Designs[11]	Keysight Technologies
The Evolution of Security in 5G[12]	5G Americas

5 Intelligence: Local Monitoring

Arun Viswanathan *Jet Propulsion Laboratory*

It is crucial to ensure that local monitoring is occurring and being fed into the overall threat intelligence picture. The Jet Propulsion Laboratory (JPL) plans to publish a set of lessons learned and best practices on this topic in the future. The OSA would like to refer readers to the impending publication by Dr. Arun Viswanathan and members of the Cyber Defense Engineering and Research Team at JPL.

6 Intelligence: The IoT Crisis

Garry Drummond *802Secure*

For all the benefits that Internet of Things (IoT) brings, the sheer volume of billions of intelligent IoT endpoints is proving to be a cybersecurity nightmare - there is now an expanding attack surface with each IoT device becoming an entry point for attacks.

Much has been written about the Internet of Things (IoT) and how they are poised to transform the way in which our physical and digital worlds interact. The “things” in IoT is a broad concept and are sometimes referred to as smart devices, connected machines or intelligent endpoints. In general, these “things” are physical objects (or systems of objects) that have to compute capabilities that permit two-way communications over the Internet.

Devices and networks that were once air-gapped are now connected and therefore now a target for compromise i.e. Thermostats[13], Heating, Ventilation, and Cooling (HVAC) Systems, Smart TVs, Surveillance Cameras and Drones to name a few. All these systems have proven to be vulnerable to attack and data breaches have been reported across multiple verticals including Hospitality/Gaming, Critical Infrastructure, and Financial Services.

There are 3 main Exfiltration Methods employed by IoT devices that make networks so vulnerable to attack: Targeted, Opportunistic, and Espionage.

Targeted Zero Configuration Devices – or devices that are obscured from normal network operations – can operate autonomously outside the scope of the enterprise network. These devices do not require DHCP to be on the network, or require DNS in order to be able to do name translation because they self configure and they don’t need to communicate to the enterprise network. This creates obscurity because they can

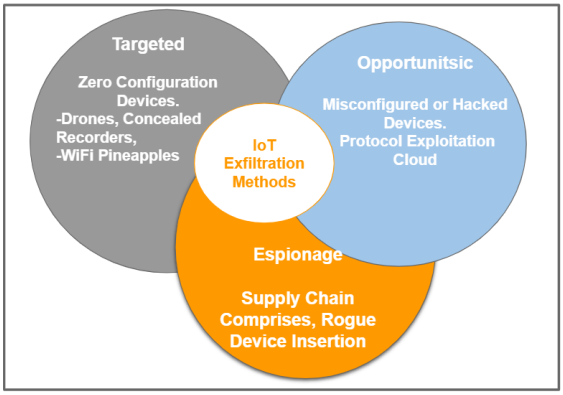

Figure 2: Overalapping exfiltration methods

communicate between one another through self-discovery. These are real threats that we didn't have to think of before. Data could, for example, be collected autonomously by self-organizing devices then those data could be delivered to a passing drone.

Opportunistic - IoT protocols being used often lack basic authentication, integrity or privacy. An inspection of the protocols and data structures employed by many existing systems makes it all too easy to exfiltrate data. These devices will typically lack basic Challenge and Response authentication to avoid utilizing the more expensive components necessary to do so, allowing them to keep their price-points between $25 and $50.

Espionage - Devices being provided coming from a reliable supply chain source may contain hidden surveillance capabilities.[5] The ability to embed this extra processing capability for data exfiltration on the chip/motherboard often goes unnoticed. The lack of security tools for IoT vulnerability assessment have made the task challenging. Most devices communicate over UDP and they will not even respond to pen-testing probes.

6.1 Critical Infrastructure and OT Systems

While the cyberattacks on IT systems are troublesome and costly, the damage is generally confined to the organization and its customers and partners. There is another type of cyberattack that already exists. These attacks are targeted at the critical infrastructure and the Operational Technology (OT) used by industries, economies, and society. Critical Infrastructure serves society's essential functions and needs. Disruptions to these systems from cyberattacks can have catastrophic consequences.

OT refers to computing systems that are used to manage industrial operations such as electrical power generation, water utilities, smart grid, chemical processing, factory production, mining operations, oil and gas extraction, pharmaceuticals, and transportation systems. OT systems typically include mission-critical applications with high-availability requirements and are designed to operate for years or even many decades.[14]

Part of the challenge lies in the fact that OT systems were not built with cybersecurity in mind but instead with

[5]See §8 for more information on securing the supply chain, and §7 for more information on maintaining appropriate situational awareness of those vendors.

reliability, safety and continuity as the top priorities. Most OT systems typically ran on closed platforms using proprietary protocols and were isolated (or air-gapped) from the Internet. But they were still not immune to cyberattacks from hackers and adversaries.

6.2 5G Wireless Networks - the IoT Connective Tissue

5G is the fifth generation of mobile networks that promises to usher in new applications for consumers, businesses and society - ranging from self-driving cars, telemedicine, connected factories, Machine-to-Machine (M2M), Vehicle-to-Everything (V2X), smart utilities and smart cities. 5G will address many of the limitations of current 4G technologies by lowering network latency, providing throughputs of up to 20 Gbps, and allowing billions of machine-to-machine connections for massively connected Internet of Things (IoT).[15]

6.3 5G Cybersecurity Challenges

The race to 5G is on and will be the predominant network of choice for IoT and OT deployments going forward. While 5G promises many innovative and unprecedented features, it also brings along a series of new security threats. For example, given the distributed nature of the network, hackers could run cellular man-in-middle surveillance attacks and gain command and control over devices and networks causing crippling attacks. Deployment of these rogue nodes and small cells has been labeled as “Stingrays”, a common and growing problem. Furthermore, 5G is faster and more secure than 4G but research shows it also has vulnerabilities that could put users, networks, and devices at risk. Privacy attacks on the 4G and 5G cellular paging protocols using side channel information is on the increase.[6]

“In today’s 4G world, a huge botnet formed by hacking into user devices in the home could be used to mount large-scale Distributed Denial of Service (DDoS) attacks on websites. In tomorrow’s 5G world, that same botnet could be used to take out an entire network of self-driving cars in a single city, leading to mayhem on the roads.”[15][7]

6.4 5G and National Security

Given the potential benefits of 5G networks, there is universal interest from governments, service providers and equipment manufacturers to support the rollout of this new wireless technology. Governments have made spectrum available, and equipment vendors are scrambling to build wireless related equipment for 5G networks.

The growth of Huawei, in particular, has not gone unnoticed, and with 5G imminent, the US government has taken steps to ban the use of Huawei equipment in US telecommunications networks. The US government has also been trying to coerce many Western governments to take similar steps.

Concerns about Chinese telecom equipment vendors were first raised in 2012 when the U.S. House Intelligence Committee published an “Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.” The committee was concerned by the close ties of these two companies to the Chinese government - allowing their equipment to be installed in U.S.

[6] More information on these exploits can be found here - https://www.documentcloud.org/documents/5749002-4G-5G-paper-at-NDSS-2019.html

[7] Keysight Technologies discusses some of the security controls from the 5G community which may be applied to space systems in §4.

networks would give the Chinese government the ability to conduct espionage and start online attacks on critical infrastructure.[56]

6.5 Actionable Defense - A New Approach is Required

Propelled by the need to consolidate management and create efficiencies, organizations are converging Information Technology (IT) and OT networks, thereby increasing the risk and complexity of these previously isolated OT networks. This convergence is referred to as Cyber-Physical Security.

Combined with the introduction of IoT enabled devices with wireless capabilities, this evolution creates new risks to buildings, infrastructure, and delivery of modernized services across healthcare, hospitality, critical infrastructure, manufacturing, and numerous other industries.

With 80% of IoT devices now being wirelessly connected, wireless is now the new network and new attack surface. The IoT ecosystem introduces a plethora of new operating systems, new protocols, and new frequencies that traditional IT and Information Security teams are unfamiliar with – creating a huge security blind-spot. In addition, most Information Security Teams don't have the security assessment tools in place to be able to detect, assess and prevent risk. This culmination of lack of visibility and lack of security is creating a 'perfect storm' for massive exploitation. For example; IoT devices like Wireless Thermostats, Wireless Thumb Drives, Voice Assistance devices like Amazon's Echo, Surveillance Cameras, Drones, Smart TVs, Wireless Printers, Wireless Medical Devices, Spy Cameras, Rogue Cell Towers all can lead to rogue communications and back-door access to data exfiltration.[8]

Combined with the introduction of IoT enabled devices with wireless capabilities, this evolution creates new risks to buildings, infrastructure, and delivery of modernized services across healthcare, hospitality critical infrastructure, manufacturing, and numerous other industries.

As we dig a little deeper into the applied aspects of IoT and OT networks. First and foremost, we are moving away from a wired-world to a wireless-world. Most organizations still have a wired centric view of IoT, hence creating another blind-spot. Companies have a difficult time trying to answer even the basic questions - "Is there an IoT network within my environment?", and "How do I know if anyone is trying to target my Network through IoT?" So a new approach is required.

In order to solve this security blind-spot, you first have to approach the problem from the correct perspective; i.e. if IoT and OT networks are predominantly wireless, therefore it makes sense to have comprehensive visibility of the broader RF spectrum.

6.6 Key Requirements & Recommendations

- IoT Fidelity – Wireless Deep Packet Inspection (WDPI) is required and necessary to determine the actual device. For example, distinguishing between a Surveillance Camera vs Spy Camera.
- Coverage – Broad Spectrum RF coverage of the most commercially viable frequencies in use.
- Adaptability – Software Defined Radio that can perform multi-protocol, multi-frequency demodulation in real-time. Fingerprinting of IoT devices as they pop-up within the environment with the ability to classify and categorize devices and networks.

[8] JPL discusses the issue of local situational awareness and monitoring as well. See §5 for more information.

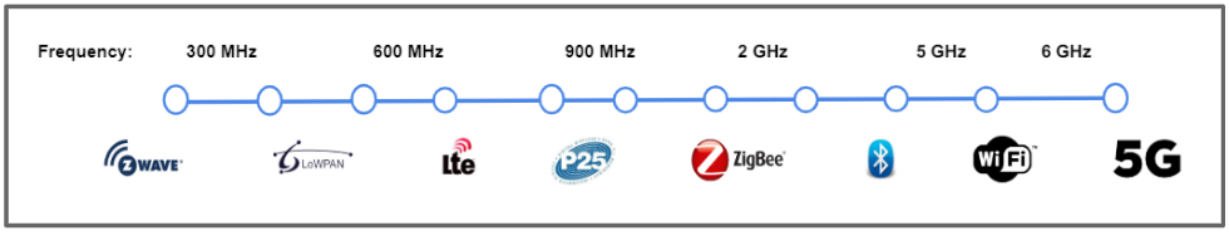

Figure 3: Common frequencies now in use for IoT enablement.

- IoT Interrogation – passive interrogation of IoT devices to validate security controls.
- Policy Enforcement – the ability to measure 'what should' be against 'what is'. For example, if you have standardized on *Sigfox* as an IoT protocol wouldn't it be to have notification to any new protocols that pop-up within the environment. This is your 1st Line of Defense.
- Proactive Vulnerability Assessments – a system that is dynamically in-tune with your ever-changing environment. The ability to access risk and fix unacceptable vulnerability exposures states - prior to loss or incident occurring. This is your 2nd Line of Defense.
- WiFI and 5G Intrusion Detection – deploy a solution capable of understanding both WiFi 6 and 5G network channels.
- Remediation – Air Isolation (Termination) capabilities or API integration to Network Address Control (NAC) systems to block misconfigured or nefarious IoT activities.
- Mitigation – the ability to integrate with Incident Response Technologies such as Security Incident and Event Management (SIEM) in order to find non-compliant devices, including rogue cell towers.
- Response – the ability to quickly respond to nefarious wireless communications via automated Air Isolation / Termination or through the use of API to wired-side NAC solutions to send block commands.

Key Recommendations	
Recommendation	**Level**
Discovery – Deploy a wireless IoT monitoring system capable of discovering wireless systems over a wide band, passively interrogating to determine device type, and validating the device's configuration against a security policy.	–
Detection – Proactively identify and address unacceptable vulnerability conditions and exposure states prior to loss or incident occurring.	Continually
Response – Integrate wireless monitoring system with general monitoring and response systems (such as SIEM and/or software-defined networking systems).	Able to isolate devices from core network at minimum.

External References	
Reference	**Organization**
The Emerging Cybersecurity IoT Crisis	802Secure

7 Intelligence: Threat Intelligence Platforms

Chris Adams *ThreatConnect Inc.*

The global space industry is experiencing significant growth through the introduction of innovative and lower cost space systems, products, and services. Aggressive competition in satellite and launch services is lowering the bar to entry, and initiatives such as large constellation network models promise to disrupt communication & networking markets. All told, the cyberattack surface of space assets is growing proportionally and asset owners must think differently about how to protect them from well-funded, nation-state adversaries attracted to the potential to disrupt or inflict pain on US or allies.

Potential losses due to cyberattacks can range from the exfiltration of scientific or military data to purposeful destruction of expensive space mission hardware, or loss of life. The responsibility of CISOs in charge of managing cyber-based risks can seem daunting due to the nature of those risks, especially when dealing with Advanced Persistent Threat (APT) groups with a formidable track record of compromising well-established institutions and organizations. This paper will attempt to briefly characterize the problem set and offer recommendations on how threat intelligence and analysis can help to reduce the risk of exploitation. Before discussing threat intelligence and analysis, let's get a sense for the big picture with respect to risk.

7.1 Step One

First, ask: For a mission to succeed, what operations are most vital? What systems do those operations depend upon? What assets comprise those systems?

As security professionals in the space industry, our number one objective is to reduce the risk of mission failure by reducing the risk of asset exploitation. Certainly, from an adversary's perspective, compromising a mission begins with targeting specific assets upon which mission operations depend. It is fair to state that the risk of mission failure is a function of risk across all operations-dependent assets.

At the end of the day we'd like to say we've protected every asset to the maximum extent possible and reduce the risk of exploit to zero, however that's neither plausible nor economically feasible any more than saying we expect 100% availability of systems. Therefore, we need to determine those operations most vital to mission success in order to allocate investment appropriately. This is referred to in industry as Crown Jewels Analysis (CJA) - a process for identifying cyber assets that are critical to the accomplishment of a space organization's mission.[16] For example, a rocket launch company may consider a rocket and supporting systems their crown jewels for a particular mission. Security teams must work with the mission engineers to identify and enumerate all assets comprising mission and mission support systems.

While the Information Technology (IT) function of asset management would seem to be a fundamental step in any organization, it's been cited that some space organizations have not done well at this. For example, NASA has been criticized for not having a good understanding of their assets.[17] For obvious reasons, it's

difficult to protect something you don't know you have.[9] That's like not knowing there is a trap door on the roof of the building you are trying to protect.

The CJA model promotes a hierarchical dependency between mission objectives, operational tasks, information assets and cyber assets. Operational tasks enable the mission to succeed and the exercise is to identify the impact caused to the mission should a particular operational task fail. Subsequently, those operational tasks depend upon information assets that depend upon cyber assets. When a model is constructed, one can begin to predict the impact to a mission should a particular cyber asset be exploited.

Additionally, once you've identified the heaviest weighted cyber and information assets in terms of impact, you will have a more instinctive sense of what must be protected. Many large businesses in the finance, energy, retail, and other sectors subscribe to threat intelligence providers to learn about the strategic intent of APT groups and to know the indicators of compromise those groups typically use. Security teams can confidently prioritize their work when they learn a specific threat group notorious for exploiting vulnerabilities of an asset your operations depend upon, is present in your network. Some suggestions on how this is achieved are mentioned later in the paper.

7.2 Step Two

Next, map your attack surface. Know what systems are most vulnerable, ask how they might be attacked.

Now that you know which assets are most critical to mission success, identify what makes those assets vulnerable to attacks. Cyber assets are comprised of a variety of system hardware, software, controls, and communication interfaces. Recent commoditization of space systems is driving broader adoption of open source and Commercial Off-The-Shelf (COTS) technologies; the same technologies that adversaries typically create exploits for due to that very reason – prolific adoption. Linux is currently used to control launch vehicles, satellites, and possibly manned-craft in the future.[18] On-board computers control the spacecraft platform and payloads with mission-specific software that communicate with other systems. Scanning all systems can help identify when a known vulnerability is present by leveraging public vulnerability databases.

Industrial Control Systems (ICS) and Operational Technology (OT) devices reside in a world disconnected from standard networks and this reduces the risk of them exploited. Still, the OT and IT world continue to merge, for the sake of necessity, convenience, and cost. For example, NASA's cryogenic fuel loading systems are designed to reduce the number of people required to control crucial, complex systems.[19] While this is positive from a systems optimization perspective, reducing the number of people implies greater automation, more systems, more networks - a larger attack surface. More so, protecting OT devices falls outside of the typical experience bracket of most security engineers that were trained in the traditional security-intensive sectors such as finance.

Attempting to predict how assets can be exploited requires the expertise of the engineers familiar with OT devices, not just a review by a security engineer. That's because there may be more access methods to a system or device than may be commonly known. For example, there may be a primary control system interface that is well documented so security teams protect it, then later it is determined that Basic Input/Output System (BIOS) updates occur via alternative method that is unprotected.[10] Working together,

[9] This issue is further illustrated in §6.

[10] Ensuring appropriate security measures throughout the supply chain can assist with this issue. See §8 for more information.

security teams and operations engineers will do a better job in protecting assets.

7.3 Threat Intelligence can Help

Threat Intelligence (TI) can help protect assets and reduce the risk of mission failure.

Despite massive investments in standard security devices (firewalls, endpoint protection, etc.) over the years, organizations continue to be hacked. That doesn't mean these devices no longer serve a purpose, but it's fair to say that security architectures must evolve as adversary tactics and techniques change over time.

Consider that firewalls were created to block inbound access to assets or networks on specific ports and protocols. Adversaries understand the firewall is there and circumvent it. For example, they may use social engineering techniques (phishing email, USB, etc) to deliver malicious code that runs inside the network and establishes a reverse connection to their workstation. The adversary then issues commands as if they were local to the network.

Now while the firewall is not preventing access, it is logging the connection to the adversary's external IP address. If someone told you about that specific IP address (a shared threat indicator), you could run a check against all connections in your firewall logs and have an alert sent when a match occurred. More so, if the file hash of the malware was also known and shared, you could compare that indicator against all file hashes across network systems, throwing an alert if there is a match. Obviously, when the matched indicator is associated to a well-known APT group, you are now able to prioritise your response.

These indicator matching scenarios using threat intelligence are becoming a vital part in an evolving cyber defense. Building this architecture to scale, typically involves ingesting intelligence feeds (from public and private sources) into a Threat Intelligence Platform (TIP) that integrates with Security Incident and Event Management (SIEM) products. And while most SIEMs are designed to work within IT environments, there are newer vendors with a focus on OT controls and protocols conducive to space asset organizations with critical OT infrastructure that need protection.

Centers like Space Information Sharing and Analysis Center (ISAC)[20] hold promise in that space asset organizations can benefit by learning new threat information from partners and act quickly to defend themselves. Both public and private organizations that provide threat intelligence typically do so using STIX/TAXII, therefore TIPs should easily ingest those threat indicators and integrate with defense infrastructure for matching paradigms or blocking.

7.4 Threat Analysis: A Critical Capability

In the threat intelligence world, context is king. While someone may tell you that an IP address is dangerous, analysts will typically want the big picture to help them make a decision regarding what to do about it. If you find a bullet in a wall at a crime scene, you'll want to investigate what type of gun fires that bullet. Next, you'd probably look up local individuals that have registered that type of gun, so on and so forth. Analyzing cyber threats requires similar analytical thought processes.

Suppose an analyst is suspicious of an IP address. The next step could be to perform a reverse DNS lookup which would indicate which host or domain resolves to that IP. The next step could be to run a reverse WHOIS lookup and discover the name and location of the person who registered it. Analysts can leverage threat analysis platforms to support this type of analysis and adopt methodologies, such as the Diamond

Model for Intrusion Analysis or Kill Chain, to find associations and relationships in data that helps determine context.

The better threat intelligence platforms will also make it simple to characterize the data found in your own threat hunting with MITRE ATT&CK Framework (ATT&CK) - a knowledge base of the most common adversary tactics and techniques based on real-world experience in the field. There is an ATT&CK matrix for enterprise IT and a just-released matrix for industrial control systems, which will help address threats to the OT environment common in space organization environments.[21] Adding these dimensions to threat analysis is what empowers turning threat data into intelligence that analysts can act on.

Analysis models can provide the insight needed to determine if suspicious activity within an environment is cause for alarm and immediate action, or something that can be ignored. For example, if it is determined that indicators discovered in the network belong to a particular threat group, perhaps an APT known for exploiting vulnerabilities in systems that support the mission, it is clear what that day's priorities will be. Embracing threat intelligence and analytical tools, and integrating those into your network defense, are some of the key methods employed today to defend against advanced threats.

Key Recommendations	
Recommendation	**Level**
Perform a Crown Jewels Analysis of all operational systems and keep that analysis up-to-date.	–
Enumerate assets, infrastructure, and networks identified during the Crown Jewels Analysis and employ appropriate monitoring and controls.	–
Deploy a Threat Intelligence Platform compatible with existing infrastructure.	–

External References	
Reference	**Organization**
Systems Engineering Guide[16]	MITRE
ATT&CK for Industrial Control Systems[21]	MITRE
ATT&CK for Enterprise[22]	MITRE
STIX/TAXII Documentation[23]	MITRE
Diamond Model for Intrusion Analysis[24]	Department of Defense (DoD)

8 Supply Chain Management

Steve Lee *AIAA*

In 2010, the world learned of a targeted computer virus, developed by one nation state to address a growing strategic threat from another – STUXNET. The United States and its allies were able to significantly delay the development of nuclear weapons in Iran by causing physical damage to the centrifuges Iran was using for refinement of nuclear material.[25] Many years later, the entire cellular industry is turned upside down by the declaration that one of the major players, Huawei, poses a national security risk.[26] In both cases, the vulnerabilities were made possible by way of the supply chain. Space systems manufacturers and operators

rely on external suppliers for many critical components and services , especially those related to digital systems and associated services. Experience across a variety of industrial sectors bears out this risk. In an effort to counter pervasive and effective supply chain threats, the Department of Defense has integrated supply chain security into its new Cybersecurity Maturity Model Certification (CMMC) program.

The commercial nuclear industry, with its grounding in advanced science, demands for precision and safety in the face of demanding and forbidding environments, and its business case based on high-risk yet high-yield, high-availability performance, parallels the space industry in many of its cybersecurity needs. Indeed, space manufacturers and operators can leverage other industries' cybersecurity experiences adapting to emerging requirements to economically and efficiently improve cyber security posture. It is recommended to start with two standards from the nuclear industry. Specifically the Nuclear Energy Institute publication 08-09 *Cyber Security Plan for Nuclear Power Reactors* §11.2, and Nuclear Regulatory Commission Regulatory Guide 5.71 *Cyber Security Programs for Nuclear Facilities*.

Generally speaking, these recommendations revolve around the concepts of validating a trusted vendor, maintaining custody and control of all products as they transition from the vendor to the facility for installation and use, and integration of cybersecurity testing principles into product acceptance and testing processes. This guidance applies to the acquisition of Critical Digital Assets (CDAs), components of CDAs, and services related to CDAs and components of CDAs following an operator's space operations Cyber Security Plan.

In order to use vendor-testing programs to meet malware detection requirements, the space system operator must demonstrate that custody and control of the devices have been maintained from the vendor through the time period that the CDA or software has been installed in the space system. Operator receipt processes shall ensure that devices or software were procured and expected to arrive and were received with normal vendor shipping packaging, such as shrink-wrap, tamper seal or other recognizable packaging and marking in place. Control of the CDA or software package shall be maintained and placed into segregated areas with access controls in place, that at a minimum meet the requirements, if located outside of the operator's controlled secure area to ensure that only authorized individuals have physical access to the materials while being stored prior to installation. For software, integrity of the software shall be maintained by verifying integrity of the software before use.

These standards, however, were last updated in 2010, and were not designed for the commecial space industry. It is further recommended that several adaptations and amendments be made, such as inclusion of Threat Intelligence (TI) and addressing internet-based software distribution channels. Vendor validation requirements should also be improved to be more in line with NISPOM recommendations.[27]

Supply chain cybersecurity is recognized as a significant challenge across a variety of industrial sectors. The unique cybersecurity characteristics and criticality of space systems heighten the urgency of addressing the supply chain challenge. Nonetheless, effective practices from other industrial sectors – augmented by measures tailored to new developments and specific space operations practices and needs – can form the basis for effective space sector supply chain cybersecurity.

Key Recommendations	
Recommendation	**Level**
Comply with §11.2 of the Nuclear Energy Institute publication 08-09, *Cyber Security Plan for Nuclear Power Reactors* and/or Nuclear Regulatory Commission Regulatory Guide 5.71.	–
Use Cybersecurity Maturity Model Certification (CMMC) ratings to facilitate vendor selection and risk management.	Minimum of Level 3
Follow NISPOM subguidance (Sections 8-209. 8-212, 8-215, 8-301, and 8-306) for vendor-related cybersecurity procedures.	–

External References	
Reference	**Organization**
Cyber Security Plan for Nuclear Power Reactors[28]	NRC
Regulatory Guide 5.71[29]	NRC

9 On Board Computer Security and Containerization

Dean Hawes & Frank Pound *KubOS & AstroSec*

The US' reliance on satellites for everything from critical defensive technologies, to vital networking connectivity, and even essential remote sensing capabilities means a breach can have devastating impacts. Results from successful attacks can result in denial of service, spoofed or delayed data, and even failures within the nation's infrastructure. Any of these types of failures can leave the nation vulnerable and create chaos – planned and unplanned. Great emphasis and effort have been placed on protecting our terrestrial systems, yet the processing systems running our satellites haven't kept up, making them a prime entry point and facilitator for an attack. This makes any enterprise system relying on assets in space a significant vulnerability – and it could get much worse if not addressed immediately. The intent of this section is to look at what types of vulnerabilities exist in a typical satellite and to make general recommendations on how to better protect our systems in space.

9.1 Challenges in Securing Embedded Systems In Satellites

Implementing cybersecurity mitigations developed for terrestrial Information Technology (IT) systems would provide a significant increase in resilience against cybersecurity attacks that threaten a space system. Unfortunately, satellites and space systems present unique challenges to implementing these protections against system vulnerabilities. To begin with, the Size, Weight, And Power (SWAP) of space systems often creates limitations in processing throughput and memory.[30] Mitigations that may be highly effective in terrestrial systems that come with a high level of processing or memory overhead become much less attractive on space systems because of these physical processing limitations.

Additionally, at the enterprise level, embedded systems in spacecraft interact with existing systems (an enterprise architecture or fleet of space systems) that are connected only intermittently (during ground station passes for example), resulting in limited opportunities to install or upgrade cybersecurity measures,

restricting the amount of time available to install updates that protect against new attacks, or address recently identified vulnerabilities.

These challenges and others like it can make it difficult to protect our space systems. Implementing an effective means to reduce intrusions into space systems is only half the battle. We then must consider what actions need to be taken when a system vulnerability has already been exploited and the satellite has been penetrated. We cannot assume a perfect defense is attainable and thus must prepare for the inevitable intrusion. A method of detection, isolation, and recovery must be implemented to mitigate these threats as quickly as possible and return the space asset back to service. All of this protection must be balanced against the resources available on the spacecraft, which may result in a decrease in mitigating capabilities at the cost of an increase in the risk that must be taken.[31]

9.2 Relevant Emerging Cyberspace Threats

Cyber risks have grown significantly around software and hardware exploits, information breaches from third-party vendors, information theft, and the altering of mission data. To further complicate the cyber threat landscape, the threat actors increasingly consist of coordinated efforts between nation-state cyber attack groups, criminal cyberattack groups, and individual hacktivists, resulting in more sophisticated cyberattacks on today's critical systems. These threats go beyond theft and security breaches. It has now been observed that non Department of Defense (DoD) assets serve as a laboratory for bad actors to develop and mature attacks for DoD assets, and the trend will most likely not stop there.

These threats can penetrate space systems in the form of tainted components from the supply chain, intrusion through Telemetry, Tracking, & Control (TT&C), interactions between satellites and ground stations, interactions between space vehicles on Intersatellite Links (ISLs), and an increasing number of other methods. These penetrations may manifest themselves in the form of unplanned changes to spacecraft configurations, Advanced Persistent Threats (APTs) that linger until triggered, or in more immediate catastrophic events.

Threats can also penetrate cloud based ground systems. We should note that the recent discovery of APT10 named "CloudHopper" indicates that over 14 large companies who provide cloud based software and hosting services have been actively penetrated since 2016. What's notable is that even with detection of these intrusions the defenders are not confident in declaring the intrusion as over.[32] This is notable because it gives us pause in thinking the cloud is a safe bastion of cyber security and reliability; one must also include risk analysis of cloud configurations and software services in their overall risk calculus for spacecraft operations. This is even more important today with the rapid deployment of cloud based ground stations as a service.

9.3 System Elements to Be Addressed

9.3.1 Operating System

The Operating System (OS) can be described as the life of a computer system. It's the primary software component that is loaded into the system which allows the system to become operational and controllable. Since it manages all the programs and applications on the computer, it has a critical role in the overall security of the system. Since threats may occur deliberately or due to human error, malicious programs or persons, or existing system vulnerability mitigations must be deployed to protect the OS. These mitigations include:

- Use of proper user management (user authentication based on credentials and privileges)
- Performing regular OS patch updates
- Installing updated antivirus engines and software
- Making backups of critical files and software images

9.3.2 Flight Software

Standard intrusion mitigations in place today such as encryption on spacecraft to ground segment communications and robust access control are good practices to prevent intrusions. But when considering the more advanced threats that are rapidly evolving today it makes sense to assume the spacecraft will ultimately be penetrated in some unpredictable manner. To combat this, spacecraft developers may implement a robust Intrusion Detection System (IDS).[57] The implemented IDS may take different forms from one space system architecture to the next, but should include continuous monitoring of telemetry, command sequences, command receiver status, processor throughput profiles, shared bus traffic, and flight software configuration and operating states.[11]

Each spacecraft and its associated software architecture, while different in form and function will have several identifiable parameters that have a significant likelihood of indicating a cyberattack against a spacecraft. Monitoring these parameters on the ground is a good start but carries the risk of not detecting the breach before the asset is compromised. Developing autonomous telemetry monitors onboard may provide a more immediate response to an attack once it is detected, and possibly initiate threat isolation and system recovery actions more rapidly. In either scenario the IDS approach must be flexible enough to be quickly updated to combat new threats as they evolve.

A more advanced approach would involve evaluating multiple parameters for correctness when combined together. For example when a spacecraft is given a command to adjust its position one would expect a flurry of bus traffic from various sensors indicating this was taking place. Battery current draw, thruster activity, solar pointing/sun sensor readings etc would all potentially change. These changes can be expected to all be within certain levels relative to each other. An individual reading taken alone may be acceptable but not when taken in total with the whole activity. This may indicate a suspicious action being taken by an adversary. Building such an "expert" system will require an adaptable rule set which can be adjusted as the spacecraft ages and as threats evolve. Beyond expert systems one could foresee the use of a lightweight neural network which looks for outliers in acceptable readings using clustering algorithms.

[11] See §5.

Software Supply Chain Another potential path for intrusion into a spacecraft or space system onboard computers is the supply chain. It is critical that spacecraft developers implement a supply chain risk management program to ensure that each of their vendors handles hardware and software appropriately and with an agreed-upon chain of custody. Space vehicle developers must define approaches to ensure that vendors are trusted suppliers. Critical parts and software should be sourced from these trusted vendors and checked for signs of counterfeiting or malicious content. Well managed configuration management is a critical element and must be implemented for all software and firmware residing in any system on a spacecraft.[12]

9.3.3 Software Development Cycle

The software development environment of today is inherently creative and collaborative and can span across geographically diverse teams. Available technology makes sharing and collaborating easier than ever, but it also makes containment and distribution control significantly harder, creating new security concerns. In today's environment, software developers and their development environment can be considered threat sources.

It's difficult to recommend a specific development model to be used as a standard for the space industry, but here are a few actions that may help to improve security in the software development environment.

- Agile Development - Maintain an agile test regime that is responsive to in-depth testing requirements. This keeps untested code changes from deleting or corrupting production data, and it keeps developers from having access to test and production systems. This also supports rapid development and incorporation of new security patches and features.
- Secure Endpoints - When developing applications, consider encrypting endpoints. Also, prohibit external storage media from connecting to the development environment.
- Keep Code in the Environment - In addition to creating secure endpoints, do your best to keep code within a secure environment. This may be more of a challenge when using open source libraries.
- Protect the Code Repository - As a central point from which your code is stored and managed, it's crucial that the repository is appropriately secured. Loss or compromise of access credentials, or breach of the underlying service may allow attackers to modify your codebase without your knowledge.
- Audit Often - Regular code audits with high coverage (close to, or at 100%) can detect malicious functions or vulnerabilities earlier in the development cycle and prevent them from entering into the production release.
- Design Security for the Target Application - Robust cybersecurity is ideal, but for systems that have limited resources and are less critical, fully encrypting everything may add overhead without adding value and be a waste of system resources.
- Plan for Security Flaws - All code is susceptible to bugs and security vulnerabilities - this is a fact of life. Accept that your code will have exploitable shortcomings and establish a process for capturing and managing them from identification through to the release of a fix.

[12] See §8 for more information on how to secure the supply chain.

- Introduction of Adversarial Testing - Existing security checklists and software security guidelines do not necessarily address the full spectrum of possible attack vectors a malicious entity may take against the system. It is critical that new systems be exposed, during early testing and continuously throughout, to adversarial thinking and penetration testing as part of the regular software development process.

- Rethinking Requirements - Instead of simply dictating what the system "should" do, also ask the question "What should the system NOT do". This is important for security and supports a more deterministic system overall.

In the end its up to the organization developing the system and applications to determine the right level of security based on the target application, the environment the application is developed in, and the environment the system will perform in.

9.3.4 Containers and Hypervisors

For Linux operating systems containers and hypervisors are used to isolate an application and its dependencies from the primary applications into a self-contained unit that can run anywhere. The key difference is that while the hypervisor abstracts an entire processing device, containers just abstract the OS kernel. Both have their advantages and disadvantages, but when used effectively for the given application and architecture they can create a high-level "standard" and framework for security mitigations.

Containers Containers, in short, contain applications in a way that keeps them isolated from the host system that they run on. Containers allow a developer to package up an application with all of the parts it needs, such as libraries and other dependencies, and ship it all out as one package. And they are designed to make it easier to provide a consistent experience as developers and system administrators move code from development environments into production in a fast and replicable way. Containers provide execution isolation, tools for organizing software components, flexible software deployment options, facilitate better control over coupling, and enable changes to be made to individual software components without ripple effects into other software components.

A key benefit of containers to space systems is the ability to group applications that have similar risk profiles into a single container, isolating the risks to the applications in that container and protecting the balance of the system. Similarly, containers can be grouped to create the same isolation on a larger scale. To be effective, the software architecture that will host the containers must be designed with containerization in mind.

Another benefit to the use of containers is the ability to establish a configurable "sandbox" for the application to run in. When the application is initiated in the container, the Docker function which initiates the container and application application configures the boundaries of the container establishing the resources that are allocated to the application while it's running. The Docker function verifies the resources are available before the application is allowed to initiate; if they are not available the application will not be allowed to run.

The National Institute of Standards has published NIST Special Publication 800-190, *Application Container Security Guide*, which provides recommendations for the implementation and use of containers.

Hypervisors The Hypervisor is a collection of software modules that provides virtualization of hardware resources such as CPU/GPU, Memory, Network, and Storage, and thus enables multiple computing stacks

with heterogeneous OSs and multiple applications hosted within them. Secure configuration of the hypervisor, together with its physical host, is collectively called the hypervisor platform and is needed to provide a safe platform for the execution of mission-critical applications.

The National Institute of Standards has published NIST Special Publication 800-125A, *Security Recommendations for Hypervisor Deployment on Servers*, which provides recommendations for the implementation and use of hypervisors along with security recommendations for the various hypervisor configurations. There are 5 hypervisor baseline functions outlined in that publication; Virtual Machine (VM) Process Isolation (HY-BF1), Devices Emulation & Access Control (HY-BF2), Execution of Privileged Operations for Guest VMs (HY-BF3), VM Lifecycle Management (HY-BF4), and Management of Hypervisor (HY-BF5). Each of these baseline functions has unique vulnerabilities and is susceptible to unique threats. Since there are multiple ways by which an architecture of a hypervisor can be classified, the approach recommended by NIST is to review the five baseline functions that a hypervisor performs, the tasks involved in each baseline function, the potential threats to secure execution of the task, and to express the countermeasures that provide assurance against exploitation of these threats in the form of security recommendations.

Notable attacks in the past include the famous “Blue Pill” attack where a covert hypervisor was used to virtualize a running operating system and then gain full control of it.[33] Other attacks involve crafting specific CPU instructions which trigger flaws in the hypervisor translation software to gain control of the underlying virtual systems. These types of attacks can give a bad actor full control of the virtualized operating systems. During software development of systems which will use containers and hypervisor components these types of adversarial attacks can be used to test and simulate what an attacker may attempt and thus help make the system more secure and continuously educate the software teams about these types of threats.

Configuration changes, module version changes, and patches affect the content of the hypervisor platform components such as Basic Input/Output System (BIOS), hypervisor kernel, and back-end device drivers running in the kernel. To ensure that each of these components that are part of the hypervisor stack can be trusted, it is necessary to check their integrity through a hardware-rooted attestation scheme that provides assurance of boot integrity. Checking integrity is done by cryptographically authenticating the hypervisor components that are launched. This authentication verifies that only authorized code runs on the system. Specifically, in the context of the hypervisor, the assurance of integrity protects against tampering and low-level targeted attacks such as root kits. It is also important to consider cryptographic signatures for higher layer application software to provide an in depth layered defense of the entire software stack.

Integrated Modular Avionics (IMA) standards can be adapted and applied to spacecraft flight safety. A derivative IMA for Space (IMA-SP) has been proposed by the European Space Agency (ESA).[34] IMA-SP is proposed to help improve the reliability and security of space systems. IMA is an integrated architecture which has definitions for fault containment/partitioning, separations of concerns and multi-level operations within various criticality levels. Memory protection strategies and other partitioning schemes are available to implement with the help of software and hardware components.

IMA-SP will likely make use of existing ARINC standards like:

- ARINC 429 Networking
- ARINC 650 and ARINC 651 provide general purpose hardware and software standards used in an IMA architecture

- ARINC 653 for the software avionics partitioning constraints to the underlying Real-time Operating System (RTOS), and the associated API

9.4 Security Implementations and Policies

9.4.1 Information Flow

This security policy states that information should not be allowed to flow between partitioned applications unless explicitly permitted by the system security policy. This security policy prevents unauthorized access to devices and other system resources by employing an efficient capability based object model that supports both confinement and revocation of these capabilities when the system security policy deems it necessary.

9.4.2 Data Isolation

Data within partitioned applications cannot be read or modified by other applications.

9.4.3 Damage Limitation

If a bug or attack damages a partitioned application, this damage cannot spread to other applications.

9.4.4 Tamper Proof Security Policies and Enforcement Mechanisms

Applications must not be able to tamper with the security policy or its enforcement mechanisms. Using the preceding file system example, the access control policy for a file is encoded in the file's metadata or in a special policy file maintained by the file system.

9.4.5 Evaluability

Implementing mitigations against cybersecurity threats may not be effective if the protections installed cannot be measured, or are not evaluable. It's not clear how effective the system will protect itself against threats if the mitigations can not be quantified. Use of the Common Criteria Evaluated Assurance Level (EAL) is one way to accomplish this.

An EAL is a category ranking assigned to an IT product or system after a Common Criteria security evaluation. A product or system must meet specific assurance requirements to achieve a particular EAL. Evaluation requirements involve design documentation, analysis and functional or penetration testing.

It is important during software development to ensure software components are always in testable state as early in the software development process as possible. This allows adversarial testing to proceed and provide the needed feedback early in the process.

Not all of these recommendations may make sense for all spacecraft processing systems. But if the developer that can take a good look at the types of threats that may exist in the environment they intend to operate in, they can choose and tailor the recommendations that make sense for their particular system and its intended operation. The software development cycle is a good example. Good practices must be measured against the threat environment and interleaved with the policies of the organization doing the development. This is further complicated with the tightly constrained budgets that exist today and the available resources on the

spacecraft OBC. The development organization must take a holistic look at all of these factors in order to determine the best practices to implement.

Key Recommendations	
Recommendation	**Level**
Ensure process partitioning and isolation on the On-Board Computer (OBC).	e.g. Docker containers with appropriate configuration.
Ensure data is partitioned between processes on the OBC.	e.g. Docker containers with appropriate configuration.
Leverage methods employed by the Cyber Independent Testing Lab to help guide the decision to perform a software upgrade.	Further research required.
Perform attestation at each stage of startup and ensure overall trusted boot regime.	–
Design in a flexible wipe and redeploy strategy from known good scheme.	–
Implement a strong adversarial testing process as part of the SDL. Think like the adversary.	Best Effort
Ensure software implementation includes unit tests and integration tests. This includes an emulation/simulation environment which will allow for high levels of instrumentation and introspection.	e.g. NASA GSC-16720-1 and/or american fuzzy lop

External References	
Reference	**Organization**
Secure Architecture Design[35]	CISA, Department of Homeland Security
Architecting Cybersecurity Into Embedded Systems & Signals[36]	Armed Forces Communications & Electronics Association (AFCEA)
General-Purpose Controls Simulation[37]	NASA
american fuzzy lop[38]	Michał Zalewski
Cyber Independent Test Lab[39]	

Part II: Future Directions

The future will present many new and varied challenges for which there are promising approaches and considerations to be made today. Quantum computers, for example, will eventually break existing encryption methodologies (hence the NIST *Post Quantum Cryptography Standardization Process*), but since that day has not yet come, industry-wide action is not yet warranted.

In other cases, the fundamental technology has already been developed, but require further product development before deployment. Two such approaches are discussed below.

10 Quantum Key Distribution

David Mitlyng *Speqtral Quantum Technologies*

Previous sections have outlined the current state of cybersecurity in the space industry, highlighting the lack of standards and awareness, as well as a fundamental lack of secure communication systems. As we look to the future we need stronger encryption distribution protocols to overcome increasingly sophisticated eavesdroppers and hackers. Quantum Key Distribution (QKD), also known as quantum encryption and quantum cryptography, offers a secure solution for distributing the encryption keys that are used to encrypt terrestrial and satellite data. Quantum communications offers the unique ability to detect the presence of eavesdroppers (traditionally known as Eve) using the quantum properties of photons. This is more secure than traditional RF or optical communications, where eavesdropping and spoofing can occur without the knowledge of the two parties trying to communicate (in cryptographic parlance, Alice and Bob).

There are two main types of QKD: Prepare and Measure, also known as BB84 (named after a 1984 paper by Charles Bennett and Gilles Brassard)[40]; and Entanglement, also known as E91 (named after a 1991 paper by Artur Ekert)[41] and BBM92 (named after a 1992 paper by Charles Bennett, Gilles Brassard, and David Mermin).[42]

In the Prepare and Measure protocol the sender (Alice) prepares the state of individual photons, which the receiver (Bob) then measures. This is secure because any attempt by the adversary, Eve, to measure the quantum state of the photon sent from Alice to Bob inevitably changes it. This change shows up as an error that will be detected by Alice and Bob. Depending on the error rate, it will either be privacy amplified away, or if there is too much disturbance, the key will be rejected as insecure. Ultimately, if the protocol is successful, Alice and Bob end up with a shared secret key with guaranteed security. In practice, the implementation of BB84 is complicated by the technical difficulty of creating true single photons. Because of this most BB84 implementations rely on highly attenuated laser pulses and need modifications to the protocol to be secure in the strict sense. This modified form is known as weak coherent pulse QKD.

The Entanglement protocol uses the quantum property of entanglement as the basis for its secure connection. Two photons that are entangled cannot be entangled with any other quantum system, so the information about their state cannot leak to third parties. Only Alice and Bob can know their state – Eve is left out in the cold. Entanglement QKD works like Prepare and Measure QKD but with some important differences:

In principle, the source of entangled particles can be in a non-secure location, and could even be controlled by Eve.

There is no need to actively choose which states get sent from Alice to Bob. The inherent randomness of quantum mechanics provides the choice.

The BB84 protocol consists of the following steps:

1. Alice and Bob each have a secure location and are connected to each other via a quantum channel and a classical public channel. A possible eavesdropper, Eve, has full access to both channels, but not to the inside of Alice and Bob's laboratories.

2. Alice prepares individual photons in one of four possible polarization states based on a random choice, and sends them to Bob over the quantum channel. Alice keeps track of all her choices for each photon (two bits of information, one bit for the choice of basis and one bit for the choice of state within the basis).

3. Bob makes a random choice of measurement basis for each photon received from Alice. He keeps track of both his choice of basis (one bit) and his measurement result (one bit).

4. Alice shares over the public channel one of her two bits of information, her basis choice. Bob compares Alice's choice of basis with his own choice. If they are the same, he marks the photon as "good" and confirms that status with Alice. All other results are discarded. Both Alice and Bob have effective shared one out of two of the bits in their possession over the public channel. The remaining bits are the raw sifted key.

5. Error checking: Alice and Bob reveal over the public channel some of their "secret" results. In the absence of errors, Alice and Bob now have a string of bits that are identical and known only to them, thus secure. In practice, there are always some errors in the raw key. This does not mean the raw key must be completely rejected. Alice and Bob estimate the error rate in their correlated bit strings by sharing a fraction over the public channel. Once the quantum bit error rate is known, there is a secure procedure (privacy amplification) to extract a completely secure key out of a longer, partially secure key.

In practice, Entanglement protocol is similar to what was described for BB84, including the need for Alice and Bob to have a quantum and a classical channel connecting them and a secure lab to perform their measurements. The key differences in the steps:

1. Photon pairs are created in a maximally entangled state, one photon is sent to Alice and another one to Bob.

2. Alice and Bob perform independent measurements that, when the results are combined, measure the degree of entanglement. By quantifying that entanglement, it is possible to strictly bound the knowledge that any external party can have about the states that were measured by Alice and Bob.

Based on these protocols QKD systems were built and tested over the decades, leading up to recent space-based QKD demonstrations. Most well-known is the Chinese Micius satellite mission, which launched in 2017 and demonstrated three ground-breaking QKD experiments.[43] A compact entangled photon source

was also demonstrated on a cubesat, most recently on the SpooQy-1 satellite launched in 2019.[44]

Space-based QKD systems can be used to securely distribute symmetric encryption keys between a satellite (Alice) and a ground station (Bob), which has the following applications:

- Encrypting sensitive data collected by Earth Observation satellites as the step before a data downlink
- Encrypting the commands on satellites that are susceptible to hijacking
- Encrypting data links on communication satellites

QKD can be used to securely distribute encryption keys between two different ground stations (Alice and Bob). If the two ground sites are close, QKD over fiber optics can be used. Currently, fiber-based QKD works only through short distances (less than 100 km) due to the attenuation of the glass in fiber optics and the impossibility of using amplifiers to boost the signal, as is commonly done in typical optical communications. Since quantum repeaters are not practicably viable yet, every 100km (or fewer) a secure node installation would need to be added, adding the expense of round-the-clock guards and security.

Space-based QKD is the best choice for distributing encryption keys to two distant ground sites. This is ideally achieved from a satellite with entanglement that has a view of both ground stations at the same time, known as double-downlink QKD. When the conditions are right, the satellite simply delivers one pair of entangled photons to each ground station, thereby giving them both the same set of encryption keys. But the distance and complexity required for this system requires some future development. In the meantime, there is a method for delivering symmetric keys to two distant ground stations using one LEO satellite that passes over the ground stations at separate times, known as Trusted Node QKD. Keys are distributed between the satellite and ground station. However, the satellite keeps the knowledge of the keys delivered to Alice and Bob, which it uses to help Bob deduce Alice's key. This protocol requires that the satellite knows both keys, which means the satellite is trusted to be secure by both Alice and Bob; it is a trusted node.

The mathematical problems that currently underpin all major encryption methods will not last forever – they're unlikely even to last much longer as quantum computation moves out of the laboratory and into the hands of attackers. QKD is a critical part of the next phase of confidentiality and it has already been demonstrated on smallsats and ground systems alike.

Key Recommendations	
Recommendation	**Level**
Employ QKD for Telemetry, Tracking, & Control (TT&C) systems.	Ideally 100% duty-cycle (One-Time Pad (OTP) equivalent).
Employ QKD for less sensitive service links.	1% duty-cycle

External References	
Reference	**Organization**
Quantum Cryptography Demystified: How It Works in Plain Language[45]	ExtremeTech
Explainer: What is Quantum Communication?[46]	MIT Technology Review
Satellite-Based QKD[47]	Optics & Photonics News

11 Formal Methods for Cyber Resilience

Eddy Westbrook & David Archer *Galois, Inc.*

Errors or "bugs" in software can cost money, time, and sometimes even lives. Notable examples include the Ariane 5 rocket[48], the Japanese Hitomi satellite[49], the Boeing 737 Max[50], and the Therac 25[51]. Space systems in particular rely on a wide variety of software systems where errors can cause mission failure, including software for everything from temperature monitoring to thruster and attitude control to payload software. Software errors related to security, also known as vulnerabilities, can additionally provide vectors for cyberattackers to not only compromise the mission of a space system but to subvert its operation to their own ends. Software vulnerabilities pose a real and imminent threat to space systems because of the vast resources that a number of nations around the world are devoting towards developing cyberattack capabilities and the high value of space systems as targets. As space systems evolve to rely on more and more complex software, the possibility for software bugs including vulnerabilities will only grow.

How can software errors be prevented? Traditional approaches, including testing and code reviews, are of limited effectiveness and do not scale with the complexity of software. For example, the well-known Heartbleed vulnerability, which affected around two thirds of all web servers on the internet when it was discovered, went unnoticed for two years, despite rigorous testing and reviews of the code containing it. [52] A key problem with testing is that it must be exhaustive over all possible states and execution paths of the code being tested. Otherwise there is no guarantee that an error is not lurking in some corner case that has not been tested. However, the size of the test suite required grows exponentially, or worse, with the size and complexity of the code being tested, making it prohibitive as software grows. It is also difficult to test for security and vulnerabilities, since these properties often cannot be directly observed during testing. The key issue with code reviews is that human beings often make mistakes and can fail to see subtle errors in complex software.

One emerging approach that does not suffer from these drawbacks is formal methods. The formal methods approach works by analyzing a piece of software and reducing it down to mathematical formulas that must hold in order for the software to be free from errors. It then applies tools like satisfiability solvers and theorem-provers that can check and mathematically prove these mathematical formulas. The power of formal methods is that these formula-checking tools exhaustively cover all possible inputs of a mathematical formula and show that it holds under all possible conditions. This translates into exhaustive coverage of all possible states and execution paths of the software being analyzed. Formal methods thus provide a strong, mathematically rigorous proof that software is free from errors including security vulnerabilities. That is, formal methods help make software *cyber resilient* against both failures and cyberattack.

A class of formal methods that is particularly useful for analyzing software for security and for interactions with physical components, both of which are relevant to space systems, is functional correctness verification. Functional Correctness Verification (FCV) starts from a specification or model written as a mathematical function that describes how the software being analyzed should behave. It then involves two steps: 1) verification that the software does indeed behave according to the specification; and 2) model validation that the specification has some desired properties. These steps are performed by checking and proving mathematical formulas as described above. For example, FCV of a control system involves writing a model of the control system, verifying that the software correctly implements that model, and validating that the model does not lead to a failure.

FCV can be especially effective at eliminating vulnerabilities by applying it to software that implements communication protocols. This is because the communication software of a system is by design outward-facing and interacts with the outside world, and is thus the primary entrypoint for a cyberattack. FCV of communication software involves writing a specification of the communication protocol(s) it implements and verifying that the software correctly implements this protocol. The verification step already prevents common vulnerabilities like buffer overflows that cause a piece of software to diverge wildly from its specification. The validation step can then be used to check for security-related properties like all external communication being encrypted or only certain information can flow out to the network.

FCV comes with its own caveats that merit discussion here. First of all, just as with testing, the assurance you get from FCV is only as good as the set of properties you specify to the validation step. Second, FCV is only as good as the reference model you create. That model must be a full, executable specification of the target system in order to give solid results. Both of these caveats mean that FCV requires skill sets distinct from typical validation engineering, making FCV somewhat difficult to integrate into an engineering team.

Third, the complexity of modules that are viable for the second step – equivalence proof – is still limited. That limit may equate to several thousand lines of implementation code, give or take. This caveat means that FCV cannot be applied to entire complex systems en masse. Instead, designs that will employ FCV for assurance should be decomposable into small critical modules, each of which is verifiable separately. The bottom line here is that FCV is not a magic bullet. It requires thoughtful system design, some special skills, and significant effort. However, both the high degree of assurance and the leverage of FCV make it a worthwhile endeavor.

So where to start? FCV can't simply be "swapped in" to replace testing, and doesn't (yet) scale to handle the full complexity of large, monolithic designs. In our experience, there are two sorts of critical modules that make good starting points: interface modules and critical core functions. For interface module FCV offers assurance that the system will correctly evaluate and accept or reject inputs, and will correctly confine failures so as not to communicate them to other modules. FCV for critical modules offers assurance that in isolation the concise critical functionality of a system sustains important properties for correct operation. Over time FCV can be added for more modules in a system once the critical communication and core modules are formally assured.

Recent work has shown that FCV approaches are easily integrated into DevOps environments. Work by Galois, sponsored by Amazon, resulted in FCV applied to significant portions of the Amazon s2n secure networking communications library, along with full integration of all FCV proofs into their DevOps environment. [53] As a result, each time new code is checked into the s2n repository, all relevant FCV proofs are re-run, giving assurance that all relevant properties continue to persist in the new code. This integration is also complementary to automated test-driven validation: the same DevOps platform can run functional correctness verification of critical modules while running more traditional test suites on other parts of a design. The success of FCV tooling deployed into production DevOps environments is paving the way for the industrialization of FCV at scale.

How can design teams deploy FCV for high assurance? As with adoption of any new technology, it requires will and investment to deploy FCV. Ad hoc attempts, especially those adopted mid-stream in a design, are likely to fail. However, a structured and intentional approach works - and has been proven in developments of an increasing number of production, long-term products.

Key Recommendations	
Recommendation	**Level**
Specify systems with requirements and properties in mind.	–
Design systems with strong boundaries, starting by isolating critical functions whose expected behavior can be described concisely, and where interfaces to other modules can be succinctly described in terms of correctness.	–
Identify which portions of the system should be formally modeled, and which properties of those models should be proven, according to the system specification.	–
Develop formal models and formal specifications of those properties, and then discharge the relevant proofs.	–
Use automated tools to formally verify the production implementation against those formal models.	–
Develop a DevOps mechanism that includes formal-methods capability and CI implementation of formal-methods proofs, just as is done with testing, so that every design change is fully checked and verified against all of the formal models used.	–

External References	
Reference	**Organization**
Continuous Formal Verification of Amazon s2n[53]	Springer Open

12 Conclusion

Harrison Caudill *Orbital Security Alliance*

Effective cyber/physical security for the US' space infrastructure is absolutely essential. Credible threat assessments have shown a strong incentive for foreign military powers to attack civilian space infrastructure, so appropriate security measures must be effective against nation-state actors.

Currently, commercial space system security is enforced by a combination of 15 CFR §960 and business/insurance requirements. 15 CFR §960 offers no guidance, no standard, and results in little security on the scale required. Systems carrying national security secrets, on the other hand, do have significant security measures, as dictated by CNSS Policy 12. However, the most consequential portion of that requirement is the mandatory NSA security review and NSA-approved cryptographic systems. Mandatory NSA security review will not scale to the commercial world, and NSA-backdoored encryption systems would likely prove unpalatable to many organizations.

Many of the security challenges exerienced within the commercial space community can also be found in other industries – and with far more developed standards and guidance, and with more experienced practitioners. Banking standards, where literally trillions of dollars per day are transacted over secure systems can help secure the Telemetry, Tracking, & Control (TT&C) radio links. The Nuclear Power Industry knows how to ensure integrity and reliability of the components it sources and can offer that wisdom and experience

to the space industry. Cloud computing environments have seen so much abuse from cyberattack that they have been forced to adopt highly-evolved defenses that can also be leveraged both on the spacecraft and on the ground systems. While existing capabilities may be brough in immediately, the security community will continue to push the boundaries in this never-ending cat-and-mouse game with quantum cryptography and mathematically proven software.

All of the security measures discussed herein, may be implemented by secure infrastructure service providers, as described in the previous paper *Big Risks in Small Satellites*.[54] Developing these guidelines into a fully-formed standard backed by the force of law, and carried out by secure service providers will bring much, if not all, of the security that the market so desperately needs.

There is currently a golden opportunity that will not last forever. It is not just economically feasibile to adopt good security, it is actually favorable. Moving away from the industry-practice of vertical integration with largely insecure homegrown systems to secure and professional service providers can simultaneously bring the desired measure of security, and decrease the overall monetary, time, and risk costs associated with operating a space company.

References

[1] S. Erwin. (2020, 01) Space executive says the industry needs help to understand cyber threats. [Online]. Available: https://spacenews.com/space-executive-says-the-industry-needs-help-to-understand-cyber-threats/

[2] 15 cfr part 960 - licensing of private remote sensing systems. [Online]. Available: https://www.law.cornell.edu/cfr/text/15/part-960

[3] 115th Congress, "Strengthening and enhancing cyber-capabilities by utilizing risk exposure technology act," US House of Representatives, Tech. Rep., 12 2018. [Online]. Available: https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf

[4] "Cybersecurity policy for space systems used to support national security missions," Committee on National Security Systems, Tech. Rep., 02 2018. [Online]. Available: http://www.cnss.gov/CNSS/openDoc.cfm?euEW42BfdInBtl6dBI9aTg==

[5] K. Zetter. (2013, 09) How a crypto 'backdoor' pitted the tech world against the nsa. [Online]. Available: https://www.wired.com/2013/09/nsa-backdoor/

[6] "Feasibility of a cross-border electronic funds transfer reporting system under the bank secrecy act," U.S. Department of the Treasury, Tech. Rep., 10 2006. [Online]. Available: https://www.fincen.gov/sites/default/files/shared/CBFTFS_Complete.pdf

[7] V. Tero. (2019, 05) Are you ready for swift's customer security controls framework v2019? [Online]. Available: https://www.illumio.com/blog/are-you-ready-for-swift-customer-security-controls-framework-v2019

[8] Swift customer security controls framework. [Online]. Available: https://www.swift.com/myswift/customer-security-programme-csp/security-controls

[9] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Draft nist special publication 800-207, zero trust architecture," NIST, Tech. Rep., 09 2019. [Online]. Available: https://csrc.nist.gov/News/2019/zero-trust-architecture-draft-sp-800-207

[10] "Briefing on spread spectrum technology," Telesat, Tech. Rep., 11 2010. [Online]. Available: https://www.telesat.com/sites/default/files/telesat/files/whitepapers/Spread-Spectrum.pdf

[11] "Testing and troubleshooting digital rf communications transmitter designs," Agilent Technologies, Tech. Rep., 01 2002.

[12] "The evolution of security in 5g," 5G Americas, Tech. Rep., 10 2018. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper-07-26-19-FINAL.pdf

[13] K. Beck. (2018, 04) Hackers exploit casino's smart thermometer to steal database info. [Online]. Available: https://mashable.com/2018/04/15/casino-smart-thermometer-hacked/

[14] G. Williamson. (2015) Ot, ics, scada - what's the difference? [Online]. Available: https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

[15] C. Team. (2015) 5g and the future of cybersecurity. [Online]. Available: https://www.cpomagazine.com/cyber-security/5g-and-the-future-of-cybersecurity/

[16] “Systems engineering guide,” MITRE, Tech. Rep., 2014. [Online]. Available: https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf

[17] “Cybersecurity management and oversight at the jet propulsion laboratory,” NASA, Tech. Rep. IG-19-022, 06 2019. [Online]. Available: https://oig.nasa.gov/docs/IG-19-022.pdf

[18] H. Leppinen, “Current use of linux in spacecraft flight software,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 10, pp. 4–13, October 2017.

[19] (2014, 09) Automated system to help make propellant loading more efficient. [Online]. Available: https://www.nasa.gov/content/automated-system-to-help-make-propellant-loading-more-efficient

[20] (2020) Welcome to space isac. [Online]. Available: https://s-isac.org/

[21] (2020, 01) Att&ck for industrial control systems. [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page

[22] (2019, 10) Att&ck enterprise matrix. [Online]. Available: https://attack.mitre.org/matrices/enterprise/

[23] (2019, 08) Cyber threat intelligence technical committee. [Online]. Available: https://oasis-open.github.io/cti-documentation/

[24] S. Caltagirone, A. Pendergast, and C. Betz, “The diamond model of intrusion analysis,” Department of Defense, Tech. Rep., 05. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

[25] K. Zetter. (2014, 11) An unprecedented look at stuxnet, the world’s first digital weapon. [Online]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[26] K. K. H. B. T. Minárik, “Huawei, 5g and china as a security threat,” NATO Cooperative Cyber Defence Center of Excellence, Tech. Rep., 03 2019. [Online]. Available: https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2018-03-28-FINAL.pdf

[27] “National industrial security program operating manual,” Department of Defense, Tech. Rep., 05 2016. [Online]. Available: http://acqnotes.com/wp-content/uploads/2014/09/DoD-522022M-National-Industrial-Security-Program-Operating-Manual-NISPOM-18-May-2016.pdf

[28] “Nei 08-09: Cyber security plan for nuclear power reactors rev 6,” Nuclear Energy Institute, Tech. Rep., 04 2010. [Online]. Available: https://www.nrc.gov/docs/ML1011/ML101180437.pdf

[29] “Regulatory guide 5.71: Cyber security programs for nuclear facilities,” U.S. Nuclear Regulatory Commission, Tech. Rep., 01 2010. [Online]. Available: https://www.nrc.gov/docs/ML0903/ML090340159.pdf

[30] F. Pound, “Space cybersecurity: Why we mustn’t forget the basics,” *ROOM, The Space Journal of Asgardia*, 09 2019. [Online]. Available: https://room.eu.com/article/space-cybersecurity-why-we-mustnt-forget-the-basics

[31] D. Sheets, “Architecting cybersecurity into embedded systems,” *The Cyber Edge*, 01 2019. [Online]. Available: https://www.afcea.org/content/architecting-cybersecurity-embedded-systems

[32] R. Barry and D. Volz, “Ghosts in the clouds: Inside china’s major corporate hack,” *The Wall Street Journal*, Dec 2019. [Online]. Available: https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061

[33] J. Rutkowska. (2006, 06) Introducing blue pill. [Online]. Available: http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html

[34] J. Windsor, “Integrated modular avionics for spacecraft - user requirements, architecture and role definition,” in *2011 IEEE/AIAA 30th Digital Avionics Systems Conference*, Oct 2011, pp. 1–17.

[35] Secure architecture design. [Online]. Available: https://www.us-cert.gov/ics/Secure-Architecture-Design

[36] D. Sheets. (2019, 01) Architecting cybersecurity into embedded systems & signals. [Online]. Available: https://www.afcea.org/content/architecting-cybersecurity-embedded-systems

[37] 42: A comprehensive general-purpose simulation of attitude and trajectory dynamics and control of multiple spacecraft composed of multiple rigid or flexible bodies. [Online]. Available: https://software.nasa.gov/software/GSC-16720-1

[38] M. Zalewski. american fuzzy lop (2.52b). [Online]. Available: http://lcamtuf.coredump.cx/afl/

[39] The cyber independent testing lab. [Online]. Available: https://cyber-itl.org/

[40] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *1984 International Conference on Computers, Systems & Signal Processing*, vol. 1, 12 1984, pp. 175–179. [Online]. Available: https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

[41] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.67.661

[42] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without bell’s theorem,” *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.68.557

[43] G. Popkin. (2017, 06) China’s quantum satellite achieves ’spooky action’ at record distance. [Online]. Available: https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance

[44] (2017, 11) Spooqy-1: Singapore’s experimental quantum cubesat and its kibo launch. [Online]. Available: https://www.spacetechasia.com/spooqy-1-singapores-experimental-quantum-cubesat-and-its-jaxa-launch/

[45] D. Cardinal. (2019, 03) Quantum cryptography demystified: How it works in plain language. [Online]. Available: https://www.extremetech.com/extreme/287094-quantum-cryptography

[46] M. Giles. (2019, 02) Explainer: What is quantum communication? [Online]. Available: https://www.technologyreview.com/s/612964/what-is-quantum-communications/

[47] I. Khan, B. Heim, A. Neuzner, and C. Marquardt, “Satellite-based qkd,” *Optics & Photonics News*, 2 2018. [Online]. Available: Anoptionalnote

[48] J. Lions. (1996) Ariane 5: Flight 501 failure. [Online]. Available: http://sunnyday.mit.edu/nasa-class/Ariane5-report.html

[49] A. Witze. (2016, 04) Software error doomed japanese hitomi spacecraft. [Online]. Available: https://www.nature.com/news/software-error-doomed-japanese-hitomi-spacecraft-1.19835

[50] A. Levin. (2019, 07) Latest 737 max fault that alarmed test pilots rooted in software. [Online]. Available: https://www.bloomberg.com/news/articles/2019-07-27/latest-737-max-fault-that-alarmed-test-pilots-rooted-in-software

[51] A. Fabio. (2015, 10) Killed by a machine: The therac-25. [Online]. Available: https://hackaday.com/2015/10/26/killed-by-a-machine-the-therac-25/

[52] The heartbleed bug. [Online]. Available: http://heartbleed.com

[53] A. Chudnov, N. Collins, B. Cook, J. Dodds, B. Huffman, C. MacCarthaigh, S. Magill, E. Mertens, E. Mullen, S. Tasiran, A. Tomb, and E. Westbrook, “Continuous formal verification of amazon s2n,” in *30th International Conference on Computer Aided Verification (CAV)*, 2018.

Recommended Reading

[54] H. Caudill, "Big risks in small satellites," Orbital Security Alliance, Tech. Rep., 04 2019. [Online]. Available: https://osa-public.s3.amazonaws.com/papers/big_risks_in_small_sats-v1.0.pdf

[55] "Cybersecurity maturity model certification - draft," Department of Defense, Tech. Rep., 12 2019. [Online]. Available: https://www.acq.osd.mil/cmmc/docs/CMMC_Version0.7_UpdatedCompiledDeliverable_20191209.pdf

[56] D. R. Coats, "Worldwide threat assessment of the us intelligence community," Office of the Director of National Intelligence, Tech. Rep., 01 2019. [Online]. Available: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[57] B. Bailey, R. J. Speelman, P. A. Doshi, N. C. Cohen, and W. A. Wheeler, "Defending space in the cyber domain," The Aerospace Corporation, Tech. Rep., 11 2019. [Online]. Available: https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf

[58] G. Falco, "Job one for space force: Space asset cybersecurity," Harvard Kennedy School, Tech. Rep., 07 2018. [Online]. Available: https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf

[59] "Challenges to security in space," Defense Intelligence Agency, Tech. Rep., 02 2019. [Online]. Available: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

[60] "Global counterspace capabilities: An open source assessment," Secure World Foundation, Tech. Rep., 04 2019. [Online]. Available: https://swfound.org/media/206118/swf_global_counterspace_april2018.pdf

[61] R. Santamarta, "A wake-up call for satcom security," IOActive, Tech. Rep., 2014. [Online]. Available: https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

[62] B. Unal, "Cybersecurity of nato's space-based strategic assets," Chatham House, Tech. Rep., 07 2019. [Online]. Available: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf

[63] D. Livingstone and P. Lewis, "Space, the final frontier for cybersecurity?" Chatham House, Tech. Rep., 09 2016. [Online]. Available: https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf

[64] T. Harrison, K. Johnson, and T. G. Roberts, "Space threat assessment 2019," Center for Strategic & International Studies, Tech. Rep., 04 2019. [Online]. Available: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf

[65] "Risk management framework for information systems and organizations," NIST, Tech. Rep., 12 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf