AIAA SPACE Forum
17-19 September 2018, Orlando, FL
2018 AIAA SPACE and Astronautics Forum and Exposition

10.2514/6.2018-5275

The Vacuum of Space Cybersecurity

Gregory Falco, AIAA Member
Harvard University, Cambridge, MA 02138, USA

Space assets, including both ground systems and satellites are fundamental, underlying components of most critical infrastructure. Despite their importance, space systems are riddled with cybersecurity issues - both cubesats and sophisticated systems alike. There is little support infrastructure for improving space asset security such as space-specific standards or space system information sharing organizations, which exacerbates the problem. While space assets suffer similar cybersecurity issues to other industries, they are faced with a unique confluence of challenges making their cybersecurity risk mitigation considerably more complex. This paper explores the cybersecurity challenges of space systems, various attacks against space systems, and current mitigation techniques being employed by space asset organizations. Based on the analysis of these challenges and looking towards what other critical infrastructure sectors are doing to improve their cybersecurity posture, we propose a series of cybersecurity core principles. These principles should be employed by space system stakeholders including space asset organizations, policymakers and a proposed space system Information Security Analysis Center (ISAC). Should stakeholders adopt these cybersecurity principles, space assets could have a stronger cybersecurity baseline than their current state, thereby raising the barrier for attacks across the industry.

I. Acronyms

AIA	=	Aerospace Industries Association
CAVE	=	Cyber Analysis Visualization Environment
CDER	=	Cyber Defense Engineering and Research Group
CDM	=	Continuous Diagnostics and Mitigation
CISA	=	Cybersecurity Information Sharing Act
COTS	=	Commercial Off-The-Shelf
DHS	=	Department of Homeland Security
DoD	=	Department of Defense
DSN	=	Deep Space Network
FERC	=	Federal Energy Regulatory Commission
FY	=	Fiscal Year
GDPR	=	General Data Protection Regulation
GPS	=	Global Positioning System
ISAC	=	Information Security Analysis Center
IT	=	Internet Technologies
ITU	=	International Telecommunication Union
JPL	=	Jet Propulsion Laboratory
KPP	=	Key Performance Parameters
MIT	=	Massachusetts Institute of Technology
NASA	=	National Aeronautics and Space Administration
NIST	=	National Institute of Standards and Technology
OCIO	=	Office of the Chief Information Officer
PCB	=	Printed Circuit Board
TCP/IP	=	Transmission Control Protocol / Internet Protocol

II. Introduction

Critical infrastructure is defined by the US Department of Homeland Security as 16 different sectors that seem discreet; yet, there are many commonalities across them. For example, most critical infrastructure relies on space systems. We define space systems as assets that either exist in suborbital or outer space or ground control systems – including launch facilities, for these assets. Space asset organizations are organizations that build, operate, maintain or own space systems.

Some examples of critical infrastructure's reliance on space systems includes agribusiness' reliance on weather and climate satellites, the U.S. military's reliance on intelligence satellites, and various transportation industries' reliance on global positioning system (GPS) satellites. Several critical infrastructure sectors even depend on space systems for global communications. We also rely on space systems for scientific discovery, which often requires highly specialized and advanced equipment. Such equipment originally designed for scientific discovery is later used in critical infrastructure sectors upon further testing and commercialization of the intellectual property.

Despite efforts to improve the cybersecurity of critical infrastructure in the U.S., there has been comparatively little focus on cybersecurity for space systems. In 2013, the Aerospace Industries Association (AIA) published the first space system cybersecurity standard focusing on supply chain cybersecurity for space systems, but it is unclear if this has been widely adopted and there has been little guidance released since[1]. Surprisingly, MITRE, a prolific standards writer for space systems, has nothing published on this beyond a brief webpage indicating cybersecurity for space systems is important[2]. While security standards for critical infrastructure are often technically sufficient to deter many attacks, they remain a challenge to implement due to time and resource constraints[3]. Space systems, however, are more complex than critical infrastructure from a technology development, ownership and management perspective. Resultantly, space system cybersecurity has lacked guidance in the form of standards and ultimately policies that enforce these standards.

In this paper, we first explore the unique combination of cybersecurity challenges that makes space system cybersecurity especially difficult to address. Next, we explore several different attacks waged against space systems and the various techniques being used to address cybersecurity challenges. We conclude with a series of proposed cybersecurity principles that should be adopted by space asset organizations, policymakers and a proposed space system Information Security Analysis Center (ISAC).

III. A Unique Confluence of Cybersecurity Challenges

Originally, space assets, like all other technology were analog devices. These analog systems did not present the same opportunities for hacking because they lacked software with code vulnerabilities and the ability to access the system remotely. As technology moved into the digital age, space assets became digitized as well. Like most systems of the time, cybersecurity was generally not considered and certainly not prioritized. For example, when TCP/IP was created, the protocol's security was not considered. Even when space asset organizations consider the cybersecurity of their systems, it is not taken seriously. A case that illustrates this problem was the Iridium satellite constellation, which provided GPS capabilities to the Pentagon. When the constellation was created, no special cybersecurity parameters were deployed here because engineers thought the technology was too advanced for a hacker to compromise[4]. This naiveté was not unique to the Iridium constellation developers, as security was not considered a concern for decades into the early 2000s for many industries. For example, industrial control system operators and manufacturers cite the proprietary protocols in their system and insist that their protocol would be too complicated and obscure to crack – an approach called "security through obscurity"[5]. By themselves, cybersecurity issues for space systems are not distinctive to the industry. However, it is the confluence of several challenges including how space systems are a single point of failure for various industry sectors, lack cybersecurity standards and regulations, involve a complex supply chain and prolonged system lifecycle, employ commercial off-the-shelf technology, require a highly specialized workforce and battle with resource constraints, which makes space system cybersecurity a unique challenge and an attractive target for hackers.

A. Single Point of Failure for Industries

Space systems are essential to the critical infrastructure that underpin our global economy and military presence. Also, they represent a single point of failure for various industries. A stealthy cyber attacker's goal is to minimize exposure and maximize impact. One may think that a hacker attempting to cripple U.S. commerce would first try to interrupt e-commerce companies such as Amazon.com, disrupt online payments through PayPal or impede a credit card provider. However, these companies invest heavily in cybersecurity and are constantly monitoring their networks for fraudulent

and mischievous activity. Further, there are several systems that would need to be compromised simultaneously to disable US commerce activities. From the cyber attacker's perspective, a simpler route to compromising US commerce would be to target satellites or an operator of many satellites that provide connectivity to point of sale credit card systems, inventory management and even video conferencing services.

The ability to impact multiple systems by compromising a single space system makes for an attractive target. Further, there are many attack vectors for any given space system. Some attack vectors include the manufacturer of the space asset equipment, the operator or management company of the space systems, the manufacturer of test equipment used to test spacecraft components, subsystems and systems and the supply chain of hardware and software for the space system. Uniquely to space assets, they are extremely finely tuned systems relying on a diverse supply chain whose handlers have full control of various critical system components. One small flaw can be disastrous to a space mission or cause satellite failures.

B. Lack of Standards/Regulations for Space Cybersecurity

Space systems such as satellites and their controls can be sophisticated pieces of equipment considering their communication, radiation hardening, and computing requirements. Despite this, cybersecurity standards for space assets are not regulated by any governing body. This is unlike other industries such as electric systems that are regulated by the Federal Energy Regulatory Commission (FERC)[6]. In fact, regulation of satellites is generally weak. The International Telecommunication Union (ITU), a United Nations agency, regulates frequencies of satellite communications to prevent communication interference and registers the orbit of satellites, but beyond these areas there are few standards[7]. In 2007, the ITU created a "Global Cybersecurity Agenda" intended as "a framework for international cooperation in cybersecurity"; however, there does not seem to be considerable updates to this agenda since 2007, despite the changing landscape of cybersecurity[8]. At this point, there are no agencies that restrict the use of satellites and there is no overarching governing body that monitors the specific use of satellites. Even if one did exist, there are no mechanisms for enforcing any treaties/standards/governance. Because of this, it is possible that some satellites are being used as a base to launch cyber operations or for other nefarious means.

C. Complex Supply Chain and Lifecycle

While the lack of standards for such critical systems is a concern, the complexity of the supply chain required to create these systems also makes these systems attractive to hackers. Some systems will require multiple manufacturers with various specialties to develop multiple technologies and a system integrator to compile all the components to function as one. The specialized parts needed for space assets are not all created by one manufacturer. In fact, to keep costs down, NASA and other space technology developers purchase components from catalogs of approved vendors around the world[9]. Each incremental vendor provides an additional opportunity for a hacker to compromise a satellite. The approval process for these vendors does not necessarily include cybersecurity vetting standards and instead concerns physical quality control. When NASA purchases a part from a vendor, they have little control over which technician developed the printed circuit board (PCB) or what software engineer wrote the code for a given component. This lack of insight introduces considerable cybersecurity risk. In addition to vendors being vulnerable across the system supply chain, space asset organizations generally work with several research centers who may possess vulnerabilities. Collaborations across multiple partners exacerbate potential security issues.

Complex supply chains related to space assets make it challenging to discern who should be operationally and financially responsible for the cybersecurity of a system at various points of the space asset's lifecycle. The challenge of the space asset supply chain is caused by the complexity of development, management, use and ownership of space assets. Unlike most critical infrastructure sectors, space assets are not owned by the same organizations that manage the infrastructure which results in questions related to liability if they are attacked. Figure 1 depicts a graphic representing the complex landscape for cybersecurity responsibility.

As shown, company A may commission the development of a satellite with company B that then assumes the cybersecurity responsibility of the satellite. Company B then outsources components of that satellite development to companies C, D and E who own their own component of the cybersecurity responsibility of the satellite. When company B completes the development of the satellite and delivers it to the owner (company A), company F is then contracted to manage the operations of the satellite (who then assumes operational cybersecurity responsibility of the satellite). Company F then commissions company G to launch the satellite into space. Company G assumes cybersecurity responsibility during the launch process. The liability for this cybersecurity responsibility is often shifted to an insurance provider company H. Once the satellite is in orbit and operational, the management company (F) then

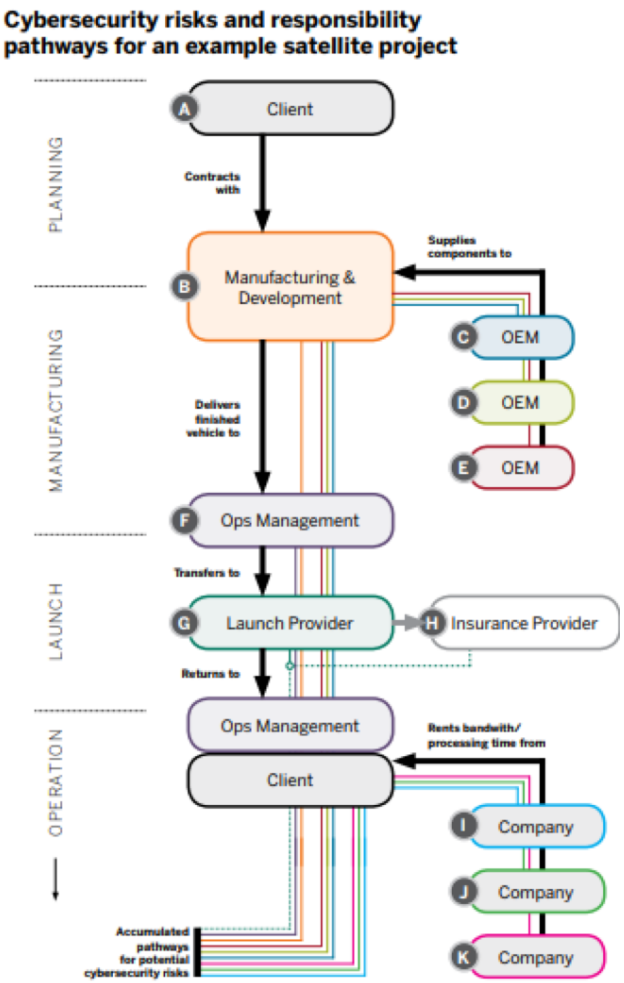

Fig. 1 Cybersecurity Responsibility Landscape.

resumes cybersecurity responsibility for the operations of the satellite. Often, the owner of the satellite (company A) will want to maximize the utility of the satellite to improve profitability and so will lease the use of bandwidth or processing on the satellite to other companies I, J, K, etc. Because of this complex ecosystem of owner, developer, operator and user cybersecurity responsibility – there are many opportunities for an adversary to gain access to the satellite. This liability lifecycle does not even cover the role of cyber insurance, which has yet to become a major player for space asset cybersecurity.

Not only are there many stakeholders involved in the space asset development lifecycle, but the lifespan of the asset itself is extensive and complicated. Space missions can last decades and because of this, security concerns can be exacerbated from legacy systems that are unpatched. Not dissimilar to industrial control systems, space assets are built to last and because they are functional in the field for such long periods and are mission critical, system downtime is not an option. This makes space assets difficult if not impossible to patch for security flaws that are discovered.

D. Widespread Use of COTS Software

For these highly complicated systems, we would assume that stringent security protocols are in place. However, not all satellites are so sophisticated. A recent trend includes low-cost satellites being launched into orbit that use commercial-off-the-shelf (COTS) technology. These "cubesats" have a fairly low barrier to entry for development from a technical standpoint and are well-within budget of any major company (or wealthy hobbyist) to launch (generally under $100K). Considering the COTS nature of the satellite, it is likely that components such as open-source operating systems riddled with security vulnerabilities are central to these satellites' function. There are considerable security concerns for

these systems because: 1) the wide distribution of COTS products means that many people have access to the devices so a hacker can extensively analyze the device for vulnerabilities 2) COTS products need to be actively maintained and upgraded for security patches which are often not applied by users and 3) anyone could have contributed to the code behind open-source technology, which means that vulnerabilities or back-doors to the software could be intentionally planted by adversaries and implanted into the codebase. In 2017, it is estimated that there are approximately 700 cubesats in orbit[10]. It is conceivable for a company to launch a cubesat to streamline operations on Earth and by doing so introduce vulnerabilities to their IT ecosystem. Government agencies are known to lease bandwidth on commercial satellites, and doing so could introduce vulnerabilities into military or other government agency IT ecosystems if the cubesat is not appropriately secured[11]. It could even be possible for a malicious organization to hack a cubesat or small satellite with propulsion and direct it to collide with other satellites. Cubesat collisions are known phenomena[12]. In one instance, the European Space Agency noticed a cubesat cut a hole in the solar panel for its Sentinel 1-A satellite[13]. This was not an intentional mishap, however one can imagine a malicious actor could do much worse.

E. Highly Specialized Workforce

The institutional design of space system organizations causes security challenges. To properly secure a system, it is important to understand how the system works and the various opportunities for a hacker to disrupt the asset. Because of this, the security experts that are experts in data management, servers and internal networks for traditional IT infrastructure likely are not the same experts that deeply understand a specialized satellite or ground control system for a deep space asset. Despite this, most space system organizations' security groups are not set up to distinguish between internal IT infrastructure and specialized space systems. This could leave space assets vulnerable because specialists that understand their function are not attending to their security. Also, because of the broad responsibilities of the security team – spanning both IT and space assets, the security experts are spread thin for time.

Part of the resourcing concern across space asset organizations is that cybersecurity is typically not a line-item in mission budgets. This makes it more difficult to justify why extra resources should be spent on cybersecurity personnel who are experts in given mission systems. Without allocated budget for cybersecurity tasks, system engineers are left to figure out security needs for their space assets. Unfortunately, they are not necessarily adequately trained to identify security flaws in their designs and are also time constrained which could result in poor attention to system security.

Another challenge at the organizational level is employee access control to sensitive information. What exacerbates this issue for space assets are the many niche skills required to develop these systems and the resulting number of resources required to complete a project. Widespread access to develop the space asset increases the need for control procedures such as access management. NASA employees have continuously been subject to phishing attacks, which, when successful, reveal sensitive information that can be used to compromise space assets to attackers[14]. The sheer volume of people that need access to such sensitive data is an ongoing risk for such organizations and begs the need for stricter operating and access standards.

F. Resource Constraints (Technical and Financial)

As data server manufacturers and operators started to care about security in the early 2000's after cyberattacks against these systems were made public and impacted their business, space assets lagged behind. Despite most industries adopting standard encryption schemes for data storage and transfer in the 90s[15], space technology designers and manufacturers seemed to resist the movement toward security[16]. We can speculate that the resistance could be a function of lower profit margins for space systems compared to commercial products or defense systems. Also, some security techniques such as encryption require more processing power to function. On many space systems, processing power and bandwidth is a precious resource and other functions are given priority. Some space systems are developed as a "labor of love" and/or "in the name of science" and the developers of the technology do not even consider why someone would want to hack their project. Because of the open-source nature of data published by NASA and other space agencies, it may have been unclear what proprietary information there even was to secure.

IV. Space System Cyberattacks

Space assets have already been compromised by nation states and criminal organizations. The most referenced attacks were mounted against government and corporate-backed space assets. These attacks demonstrate that even well-funded space projects lack the appropriate cybersecurity to defend against hackers.

A. IP Satellite Communication Attacks

Among the most interesting attacks against satellites thus far had little to do with hackers' interest in compromising the space system, but instead the technology enabled by the space system. Kaspersky Labs discovered that the Russia-based cyber-espionage group, Turla, hacked their way into a satellite internet provider to hide cyber-espionage operations against countries ranging from the US to the former Eastern Bloc[17]. By using a ground antenna, Turla could detect IP addresses from satellite internet users and then initiate a TCP/IP connection from the stolen IP address. Turla can obfuscate their nefarious operations by leveraging the stolen IP satellite address. The attack is not easily detectable because the espionage operation does not need to perceivably impact the innocent user's performance; it depends on whether the hacker and the legitimate user are using the IP address simultaneously. Because both the victim and attacker's machines would have the same IP address, the attack will be stealthy and unlikely to be flagged in intrusion detection systems.

Independent of how stealthy space-based cyberattacks can be, they can cause serious damage to an end-user's operations. Imagine hackers employ Turla's technique to target a remote electric substation. An attacker can intercept uplink or downlink packets from the victim's IP address or inject data to the user system connected to the IP address. Such a false data injection to a substation component could result in a state-estimation attack resulting in damage and downtime to the grid.

B. GPS Satellite Attacks

Another space-based cyberattack compromised GPS systems, which rely on satellites to triangulate specific positions on Earth. Introducing noise into the receiver spectrum of the GPS satellite can cause the failure of a GPS receiver on earth to provide a reading. This is a technique known as jamming. Russia has installed GPS jammers on over 250,000 cellular towers to disrupt the navigation of incoming missiles from the US[18]. While GPS jamming attacks have been used in the past and are not necessarily considered a cyberattack, GPS spoofing is a cyberattack because of the manipulation of the GPS signal. GPS spoofing is far more dangerous than jamming as it appears that the GPS is working as intended. The trust in the device is not broken for a spoof, which is difficult to detect and becomes dangerous when dealing with critical systems.

There are multiple ways to spoof a GPS satellite. One mechanisms by compromising the satellite receiver and altering the output signal from the satellite. Another opportunity to spoof the GPS satellite is via a false data injection attack where an adversary uses a GPS signal simulator (whose success will be limited because it cannot always trick the receiver) or use a software-defined spoofer. Software-defined spoofers are more reliable. They work by inserting a barely detectable fake signal behind the true signal. Gradually, the power of the fake signal is increased to the point where the receiver thinks the fake signal is actually the real signal[19]. A system that can execute a software-defined spoof attack only costs about $1,000-2,000 USD to build as demonstrated by Professor Todd Humphreys at the University of Texas, Austin[20].

Attacks using software-defined spoofing are not just theoretical or conducted in a lab. In 2017, the US Maritime Administration reported the first GPS spoofing attack against over 20 ships in the Black Sea[21]. Correspondence between one of the impacted vessels and their command center reflects that over the course of the attack, the GPS position displayed on their navigation tool sometimes showed "lost GPS fixing position"[22]. At one point during the attack, the spoofed location showed the ship was located near the Gelendzhik airport, but was in fact 25 nautical miles from the reported location. According to a non-profit organization called Resilient Navigation and Timing, which monitors GPS incidents, anecdotal spoofing reports are not uncommon in Russian waters[23]. It is widely speculated that another attack of this type was used by the Iranians to capture a US drone in December 2011[24]. In September 2011, Iranians claimed they mastered a new technique to compromise aircraft via GPS spoofing. This technique was demonstrated when they successfully captured an American RQ-170 Sentinel drone by reconfiguring the coordinates of the GPS signal to make the drone land in Iran instead of its base in Afghanistan[25]. The US military blamed the capture of the drone on a malfunction, but were unable to explain how the Iranians received the drone intact[25].

C. Government Satellite and Ground Space System Attacks

There are multiple instances of US government-run space systems being attacked by hackers. On October 7, 2007 and on July 23, 2008, an Earth observational satellite, managed by NASA and The US. Geological Survey was interfered with for "12 or more minutes"[26]. The U.S.-China Economic and Security Review Commission confirmed in 2011, several years after the attack, that the interfering party did not achieve all steps to command and control the satellite. On June 20, 2008 and October 22, 2008, Terra EOS AM-1, an earth observational satellite managed by NASA was

interfered with for 2 and 9 minutes respectively. In both cases, the hackers achieved command and control of the satellites, but did not issue commands[26]. These hacks were attributed to China and the attacks may have intended to compromise satellite imagery, stunt the transmission of imagery or exfiltrate images. Researchers believe that the hackers compromised a "commercially operated satellite ground station" using public Internet to reach the satellite[26]. Considering many space systems rely on third-party, commercially operated systems, other space systems are likely vulnerable to similar attacks.

Another example of a government space system breach was in 2011 when hackers gained full operational control over NASA's Jet Propulsion Laboratory (JPL)[27]. This was achieved by stealing over 150 NASA employee user credentials[27]. According to the Inspector General's report, "with full system access for mission-critical JPL systems the intruders could; (1) modify, copy, or delete sensitive files; (2) add, modify, or delete user accounts for mission-critical JPL systems;(3) upload hacking tools to steal user credentials and compromise other NASA systems; and (4) modify system logs to conceal their actions"[27]. It is not clear what specific damage may have been done during the time the hackers had operational control, but the scope of the potential damage from this attack is troublesome considering JPL is home to the Deep Space Network and other critical space systems.

These examples are a small sampling among many other reported cyberattacks on space assets[28]. Beyond actual cyberattacks, there are thought experiments and demonstration attacks on space assets that have been referenced in various reports[29, 30]. Given that there have been so many cybersecurity incidents involving space assets, it begs the question - what has been done to help secure these assets?

V. Current Cybersecurity Mitigation Techniques

Among the space industry community, the lack of attention to cybersecurity is acknowledged; however, the responses to the cybersecurity threats have been variable. An audit of NASA in FY 2015 revealed the need for a revamping of their cybersecurity standards and protocols. The audit cited several attacks on NASA space assets, that were not publicly disclosed, as the driver for the call for reform[31]. NASA's efforts are not necessarily representative of the broader space industry's cybersecurity awareness and efforts – however, smaller organizations working on satellites look to NASA for standards and best practices. More established private space companies such as SpaceX or Blue Origin have no public comments on their cybersecurity posture. There have been calls for more discussion from the public on how SpaceX and others plan to address cybersecurity in the future[32].

A. Access Control Management

NASA has taken several steps to improve security around space assets. With this said, there are considerable opportunities for improvement. First, NASA has begun implementing stricter access control policies across their providers and engineers. Related programs rolled out by NASA include "Spot the Phishing Email"[33]. This will help guard against some of the phishing attacks used against NASA employees in the past that steal credentials and access valuable intellectual property.

B. Specialized Security Workforce

Second, NASA has created teams across their space asset development centers that specifically work with the security of their missions systems. Previously, the Office of the Chief Information Officer (OCIO) was responsible for all cybersecurity across NASA. However, OCIO teams could not fully focus their attention on the server infrastructure security of NASA's labs, the development and operational infrastructure for NASA's mission systems, and the mission systems themselves. To address this, NASA's Jet Propulsion Laboratory (JPL) created the Cyber Defense Engineering and Research Group (CDER). CDER's goal is to specifically address mission systems (such as Mars Science Lab or the Europa Clipper), which often have unique cybersecurity requirements from traditional firewalled data servers. Developing specialized teams that have unique expertise in mission systems enables customized analysis and protection for these space assets in ways that traditional security teams that protect servers and data would not. Some of CDER's work aims to develop tools and methodologies that apply across multiple mission systems to reduce costs and security operations.

C. Employing Appropriate Security Tools

Finally, NASA has begun encrypting data while stored and during transfer. Recently, at the end of 2016, AT&T encrypted NASA's Deep Space Network (DSN), which is the foundation of communication infrastructure for NASA's

deep space missions, such as the rovers and landers on Mars, and spacecraft exploring the outer solar system[34]. Consistent with the previous section's explanations of why space assets lag behind other assets in cybersecurity, AT&T encrypted the DSN only after a report on how to hack into the Mars Rover appeared on the internet[35]. Encryption provides private communications that are only visible to others with the cryptographic key. Such encryption is a first line of defense against hackers aiming to hijack the DSN or spy on communications sent over this multi-billion-dollar, long-range communication network.

D. Fostering a Security Culture

CDER is proactively working to establish a security culture (one of healthy digital skepticism) within their group at JPL by starting a lighthearted game called "Donuts". When a CDER Group member left their computer unlocked, another CDER teammate sends an email from the unlocked computer writing "Donuts" in the subject line. If this note is sent, the compromised computer user needs to buy the team donuts. The team keeps track of the number of donuts owed by each team member thereby creating incentive for teammates to lock their machines when they step away. At first, the team was getting their fair share of donuts daily, but as security awareness grew the donuts stopped coming. This game has expanded to other teams at JPL thereby helping to establish a security culture of constant cybersecurity awareness.

E. Developing Custom Security Tools

In addition to working towards building a cybersecurity culture, CDER is also building new technology to address the ever-increasing cyber threats faced by NASA JPL mission systems. One among many projects, the team developed a tool called Cyber Analysis Visualization Environment (CAVE), which helps to model and visualize threats that can propagate throughout a mission system's network[36]. This tool can help system architects and developers better conceptualize known vulnerability information about their software that is critical to the mission.

F. Engaging with the Security Research Community

NASA JPL's Cyber Defense Engineering and Research Group is also working with the Massachusetts Institute of Technology (MIT) to conduct security tests as an educational exercise for students on mission system software[37]. By increasing engagement with the broader security research community, mission system security can be considerably improved for space assets.

Like NASA, the private space asset industry is likely currently improving its security, but as previously mentioned, it is impossible to evaluate many private sector companies who are not transparent regarding their cybersecurity efforts. Penetration testers, ethical hackers and security researchers are constantly finding holes in various satellite network systems and asking the responsible party to fix the vulnerabilities. Unfortunately, these vulnerability notifications often go ignored due to manufacturer's lack of bandwidth to address or their mistrust of the hackers. The lifecycle complexities and associated liability questions discussed earlier further complicate fixing vulnerabilities. If ignored, the ethical hackers generally follow responsible reporting procedure and expose the vulnerability to the public after a period of time after notifying the vendor. By publicly announcing the threat, the ethical hackers intend to garner large-scale attention to the problem and force the vendor to fix the issue.

Unlike GPS satellites that can be detected and penetration tested without direct access to the space asset, other private industry space asset security is inaccessible and therefore not testable by the security community. For example, SpaceX, Virgin Galactic or other private space asset developers, owners and operators do not make their technology readily available for security researchers to test. This is likely because they are concerned that their sensitive code or information will fall into competitors' hands. Another reason is because private space asset developers are concerned what the security researchers will find and that if publicly disclosed can ruin their companies. Further, there is not any required disclosure or reporting on cybersecurity testing procedures from these companies and as a result it is difficult for the security community to evaluate the cybersecurity of these space assets. Again, the theme of vulnerability disclosure liability and the risk of releasing technology for testing is substantial, which is a major barrier to transparency regarding space asset security.

Neither public nor private space asset organizations are at a complete standstill concerning their cybersecurity efforts as previously described with the NASA JPL work on building a security culture. However, there are considerable gaps to space asset security posture compared to other critical infrastructure sectors that must be addressed. The steps for improvement are not uniform for private industry and government organizations as described below.

VI. Recommended Cybersecurity Principles

Considering there are several stakeholders involved with the cybersecurity of space systems, cybersecurity principles are needed for each respective audience. Here, we offer recommendations for space system cybersecurity principles that could help address the aforementioned challenges. We divided the space system stakeholders into three audiences: space asset organizations, policymakers, and a proposed Space ISAC.

A. Space Asset Organizations

Organizations developing space assets are largely unregulated for cybersecurity. The lack of specific space asset cybersecurity requirements necessitates a considerable degree of self-policing. Without mandatory standards, space asset organizations can improve their security either individually or collectively.

1. Employ existing cybersecurity standards and develop new standards for space systems where needed.

There is no lack of cybersecurity standards and best practices available for developers to follow when attempting to design and develop secure systems. Many of these standards like the National Institute of Standards and Technology (NIST) Cybersecurity Framework is well-documented and widely adopted in some form[38]. Another such framework is the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) Program for identifying, prioritizing and mitigating cybersecurity risks of government networks and systems[39]. Most space systems' security can benefit from using these standards. In some cases, these standards may not apply for the specific technologies used in space systems. For these systems, space asset organizations should create new space asset-specific standards and best practices so that security can be applied consistently across organizations. Vendors of space asset organizations should also be held to these standards. This should involve explicit testing and demonstrations that vendors of space asset organizations must conform to when building and selling components to a space asset organization.

2. Establish cybersecurity capabilities for missions systems and internal network/server systems.

Similarly to what was done at NASA JPL, it is important to establish separate cybersecurity specialists for mission systems and internal networks/server systems. The distinction between the two systems are operational technology versus information technology – each have very different operating and security requirements and need to be addressed accordingly. A security expert who knows how to manage firewall settings for servers is not necessarily the best security expert to deal with small microprocessors or operational technology mission systems. Security expertise should be specialized so that the right cybersecurity strategies are being employed for the particular function and threats of the system. To be able to allocate specific cybersecurity resources to mission systems, cybersecurity should be listed as a line-item in mission budgets.

3. Build a security culture.

Establishing a security culture encouraging everyone in an organization to care about cybersecurity rather than relying entirely on a designated cybersecurity team is important. This could begin as simply as starting the "Donuts" game. Rewarding good cybersecurity behavior or using the traditional "name and shame" approach to punishing bad cybersecurity practices could help to encourage the security culture.

4. Assess cyber risk and choose mitigation techniques for a mission considering the risk posture and risk assessment.

Space asset organizations should conduct cyber risk assessments for each mission using a cyber risk framework such as NIST's or CDM. Such an assessment involves critical asset identifications, vulnerability assessment and threat landscape evaluation. Risks should then be ranked and those with the highest priority, at the least, should be mitigated. One mitigation technique could be using encryption to secure space asset data. Modern encryption schemes provide a cost-effective and rather simple security measure without much computational overhead. Some space asset organizations disregard encrypting satellite communications due to the public, open-source nature of the data flowing across these systems (in the case of some scientific satellite data). However, encrypting the data is still important to maintain the integrity of the data so that it can ultimately be useful for consumption. While encryption could be the right mitigation technique for some projects, others may prioritize different risks requiring mitigation techniques like installing "threat intelligence" tools.

5. Cooperate with security researchers.

Space asset organizations can collectively work with ethical hackers and university researchers to conduct penetration tests of systems. This would provide a low-cost resource to space asset organizations seeking to improve their cybersecurity posture. A relationship with ethical hackers and university researchers can facilitate not only the discovery of vulnerabilities for critical space systems, but also the remediation of these security holes. Many organizations establish bug bounty programs for security researchers to identify vulnerabilities in systems, but these often have limited success. One reason is because bug bounty programs do not allow any privileged system access. This limits the researchers' abilities to find deeper bugs and security vulnerabilities that are not at the surface layer of the exposed system. Another challenge with the traditional approach to bug bounty is that after the bugs are identified, there are too many for the security team of the organization to patch or remediate in a timely fashion, thereby exposing the organization to additional risk during this period. Partnering with security researchers to not only discover vulnerabilities but also fix security issues can potentially improve security outcomes. There are barriers to establishing a transparent and substantial relationship with security researchers as described. For example, providing privileged access to security researchers could expose the space asset organization to liabilities. For example, the researchers could unintentionally disclose private data or vulnerabilities to the public. This could cause a public relations disaster and provide an invitation to "black-hat" hackers to exploit the space asset organization's vulnerabilities.

These are some actions that space asset organizations can take without national policy or legal guidance. However, some of these cybersecurity improvements can be enabled through policy shifts concerning space assets.

B. Policymakers

To date, congress has provided little guidance in terms of enabling cybersecurity across sectors. One of the few examples includes the Cybersecurity Information Sharing Act (CISA) which was signed into law in late 2015 by President Obama. CISA is meant to help facilitate information sharing between the government and the private sector by limiting the liability of the private sector for certain attack disclosure[40]. Congress should develop more laws that could be specifically relevant to space assets. Recommendations concerning these laws are below.

1. Be proactive, not reactive.

Do not wait to pass a law on space cybersecurity until there is a WannaCry (major ransomware attack that compromised healthcare systems around the world) or Mirai (major IoT attack that took down a major DNS provider on the East Coast resulting in downtime for websites such as Facebook, Twitter and Reddit) equivalent for Space. It seems that there is only action when a disaster strikes. A space cyberattack can have serious consequences as detailed previously and we cannot wait until something happens to pass legislation protecting these critical systems.

2. Clarify critical infrastructure security requirements to include underlying systems.

Currently, policy concerning critical infrastructure security does not require third-party, enabling infrastructure to also comply with the same requirements. Space systems should be held to the same standards of the critical infrastructure that they support.

3. Assign responsibility and liability for cyber.

Cybersecurity responsibility and associated liability for a breach should be clarified and assigned for space asset organizations. An important component of cybersecurity legislation currently under review concerns the liability of technology developers, owners and operators. In January 2017, the FTC sued D-Link for the vulnerability in their routers leading to the widespread Mirai botnet attack in October 2016[41]. This was the first time a manufacturer was sued for the cybersecurity of their devices. Legal guidance concerning where liability falls will encourage the responsible party to take necessary measures to secure their systems. The lack of clarity around liability today for the space asset ecosystem results in poor accountability and inaction to secure these important systems.

4. Make space asset organizations accountable for cybersecurity.

All government contracts with space asset organizations should require the contractor to comply with key performance parameters (KPPs) pertaining to cybersecurity. Today, cybersecurity KPPs are a subcomponent of system survivability KPPs. Cybersecurity KPPs should be firmly enforced for all government contracts.

5. Expand 32 CFR 236 to include space asset organizations.

Currently, the defense industrial base is required to report all cyber incidents that have impacted or could impact national security under the Department of Defense-Defense Industrial Base Cybersecurity Activities Regulation[42]. Considering the critical posture of space systems and the U.S. reliance on these assets for both national security and critical infrastructure, space asset organizations should be included under this ruling. This would improve cybersecurity transparency between the government and space asset organizations.

6. Establish a Space System Information Sharing and Analysis Center (ISAC).

Government agencies such as the Department of Homeland Security (DHS) could play a crucial role as a convener for public and private sector entities that work with space systems. The DHS could become an important facilitator for this sector's efforts to improve cybersecurity by creating a Space System Information Sharing and Analysis Center. The DHS should require participation of government agencies that work with space systems ranging from the Department of Defense (DoD) to NASA to participate in the Space System ISAC. This would provide an incentive for private sector space asset organizations to also join. If 32 CFR 236 were expanded to include space asset organizations, the Space System ISAC could be made compulsory through this requirement.

C. Space ISAC

Sharing threat information across space system agencies and space asset organizations would be a logical step to improve the security posture of the sector. Some agencies or private organizations may be much further ahead in securing systems than others and sharing insights will help all ISAC members involved. Recommendations for what a Space System ISAC should do follow.

1. Establish information sharing requirements.

The Space System ISAC should require member entities to disclose vulnerability and attack information to each other within a predefined period. This would be in the spirit of UK's General Data Protection Regulation (GDPR) that requires an organization to disclose when personally identifiable information is breached within 72 hours of discovery[43].

2. Document and maintain space system cybersecurity principles and standards.

Member organizations should share internal or contractor standards for cybersecurity in a manner that does not release sensitive information. A master list of best practices should be shared across the Space System ISAC and curated. Member organizations can comment on the merits of the best practices and cater existing cybersecurity standards to be highly relevant to the idiosyncrasies of space systems.

3. Cooperate with ISACs for other critical infrastructure sectors that rely on space systems.

Because space systems do underpin other sectors, certain threat information for space systems should be shared with the relevant sectors that might be affected if an attack occurs. The Space System ISAC should work with the oil/gas, electricity and emergency services ISAC to communicate threats that are relevant to these critical infrastructure and services. The potentially affected critical infrastructure organizations could then work with the space asset organizations to remediate the vulnerability where appropriate.

VII. Conclusion

Space assets are underlying systems on which most critical infrastructure in the US relies. Researchers, policymakers and engineers are increasingly concerned with the cybersecurity of critical infrastructure, but fail to include the space assets that enable these systems. Cybersecurity challenges will only become more substantial as technology continues to evolve and attackers will always find the weakest link to penetrate a target system. Today, space assets are the weakest link. Space asset organizations must not wait for policymakers to take action on this issue as there are several actions that could be taken to secure their systems without policy guidance. With this said, it is the responsibility of policymakers to include space assets when addressing which technologies require cyberdefense to enable our country's continued digital manifest destiny. It is time to fill the vacuum of space asset cybersecurity.

VIII. Acknowledgements

The author would like to thank the Jet Propulsion Laboratory's Cyber Defense Engineering and Research Group for an inside look into mission system security at NASA. He would also like to thank Michel Ingham at NASA's JPL for the guidance and detailed review of this paper, Arun Viswanathan for the insights to historical cyber incidents at NASA and Michael Sulmeyer for the encouragement and review of the work. This paper could not have been written without the support of the Belfer Family and Harvard University who sponsored this research.

References

[1] Aerospace Industries Association of America Inc. Cyber Security Baseline: NAS9924. Aerospace Industries Association of America Inc., 2013. https://www.aia-aerospace.org/news/aia-announces-first-cyber-security-standard/

[2] MITRE. Securing Civil Space. The MITRE Corporation. https://www.mitre.org/capabilities/cybersecurity/securing-civil-space

[3] Trends in Security Framework Adoption: A Survey of IT and Security Professionals. Dimensional Research. 2016. https://static.tenable.com/marketing/tenable-csf-report.pdf

[4] David Wigglesworth. Iridium Security. WikiLeaks. 2007. https://wikileaks.org/wiki/Iridium_Security

[5] Knowles, William, et al. A survey of cyber security management in industrial control systems. International journal of critical infrastructure protection 9 (2015): 52-80. https://www.sciencedirect.com/science/article/pii/S1874548215000207

[6] Federal Energy Regulatory Commission. What FERC Does. 2018. https://www.ferc.gov/about/ferc-does.asp

[7] International Telecommunications Union. ITU Radio Regulatory Framework For Space Services. 2016. https://www.itu.int/en/ITU-R/space/snl/Documents/ITU-Space_reg.pdf

[8] Schjølberg, Stein. ITU Global Cybersecurity Agenda High-Level Experts Group. International Telecommunications Union. 2007. https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

[9] Michael Sampson. NASA Parts Selection List. NASA Electronic Parts and Packaging Program. 2016. https://nepp.nasa.gov/npsl/

[10] Leonard David. Sweating the Small Stuff: CubeSats Swarm Earth Orbit. Scientific American. 2017. https://www.scientificamerican.com/article/sweating-the-small-stuff-cubesats-swarm-earth-orbit/

[11] Ryan Schradin. Government Space Leaders Look To Commercial Satellites for More Resilient Communications. The Government Satellite Report. 2016. https://ses-gs.com/govsat/defense-intelligence/government-space-leaders-look-to-commercial-satellites-for-more-resilient-communications/

[12] Lewis, Hugh G., et al. An assessment of CubeSat collision risk. 2014. https://eprints.soton.ac.uk/369583/1/IAC-1%252CA6%252C4%252C1%252Cx26805.pdf

[13] Tereza Pultarova. Could Cubesats Trigger a Space Junk Apocalypse?. Space.com. 2017. https://www.space.com/36506-cubesats-space-junk-apocalypse.html

[14] John Sprague. Collaboration that Pays NASA Back. NASA IT Talk. 2012. https://www.nasa.gov/pdf/666064main_ITTalk_JUL2012_final.pdf

[15] Jinwoo Hwang. The Secure Sockets Layer and Transport Layer Security. IBM Developer Works. 2012 https://www.ibm.com/developerworks/library/ws-ssl-security/index.html

[16] Paul Martin. NASA Cybersecurity: An Examination of the Agency's Information Security. Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology. 2012 https://oig.nasa.gov/docs/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf

[17] Tanase, Stefan. Satellite Turla: APT command and control in the sky. Kaspersky. 2015. https://media.kaspersky.com/pdf/SatTurla_Solution_Paper.pdf

[18] Andrew Dalton. Russia Hopes to Block Cruise Missile Attacks with Cell Towers. Engadget. 2016. https://www.engadget.com/2016/10/17/russia-jamming-cruise-missile-attacks-with-cell-towers/

[19] Humphreys, Todd E., et al. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. Radionavigation Laboratory Conference Proceedings. 2008. https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf

[20] Colin Lecher. Texas Students Hijack a U.S. Government Drone in Midair. Popular Science. 2012. https://www.popsci.com/technology/article/2012-06/researchers-hack-government-drone-1000-parts

[21] Maritime Administration. 2017-005A-GPS Interference-Black Sea. US Department of Transportation. 2017. https://www.marad.dot.gov/msci/alert/2017/2017-005a-gps-interference-black-sea/

[22] Dana Goward. Mass GPS Spoofing Attack in Black Sea? The Maritime Executive. 2017 https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

[23] Lisa Vaas. Suspected Mass-Spoofing Of Ships' GPS In The Black Sea. Naked Security, 2017. https://nakedsecurity.sophos.com/2017/09/26/suspected-mass-spoofing-of-ships-gps-in-the-black-sea/

[24] Lisa Vaas. Drone Hijacked By Hackers From Texas College With $1,000 Spoofer. Naked Security. 2012 https://nakedsecurity.sophos.com/2012/07/02/drone-hackedwith-1000-spoofer/

[25] Scott Peterson. Exclusive: Iran Hijacked US Drone, Says Iranian Engineer. The Christian Science Monitor. 2011 https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer

[26] U.S.-China Economic and Security Review Commission. 2011 Report to Congress. U.S. Government Printing Office. 2011. https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

[27] Martin, Paul. NASA Cybersecurity: An Examination of the Agency's Information Security. Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology. 2012. https://oig.nasa.gov/docs/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf

[28] D.J. Byrne, David Morgan, Kymie Tan, Bryan Johnson, Chris Dorros. Cyber Defense of Space-based Assets: Verifying and Validating Defensive Designs and Implementations. Procedia Computer Science. Volume 28. 2014 11 https://www.sciencedirect.com/science/article/pii/S1877050914001276

[29] Hutchins, Ryan. Cyber Defense of Space Assets. 2016. http://www.cs.tufts.edu/comp/116/archive/fall2016/rhutchins.pdf

[30] Santamarta, Ruben. A wake-up call for SATCOM security. IOActive. 2014. https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

[31] Paul Martin. NASA's Management of the Deep Space Network. NASA Office of Audits. 2015. https://oig.nasa.gov/NASA2015ManagementChallenges.pdf

[32] Zulfikar Abbany. SpaceX's Starlink satellite internet: It's time for tough talk on cyber security in space. Deutsche Welle. 2018. https://www.dw.com/en/spacexs-starlink-satellite-internet-its-time-for-tough-talk-on-cyber-security-in-space/a-42678704

[33] Office of the CIO. IT Talk. National Aeronautics and Space Administration (NASA). 2012. https://www.nasa.gov/pdf/666064main_ITTalk_JUL2012_final.pdf

[34] Sharon Gaudin. 2016. NASA installs VPN to protect Deep Space Network. 2016. https://www.computerworld.com/article/3150973/space-technology/nasa-installs-vpn-to-protect-deep-space-network.html

[35] Sebastian Anthony. Could you hack into Mars rover Curiosity? ExtremeTech.com. 2012. https://www.extremetech.com/extreme/134334-could-you-hack-into-mars-rover-curiosity

[36] Pecharich, J.L., Viswanathan, A., Stathatos, S., Wright, B. and Tan, K. Mission-centric cyber security assessment of critical systems. AIAA SPACE 2016. https://arc.aiaa.org/doi/abs/10.2514/6.2016-5603

[37] Falco, G., Sigholm, J., and Viswanathan, A. Enhancing Cybersecurity Education through High-Fidelity Live Exercises (HiFLiX). Hawaii International Conference on System Sciences. 2019.

[38] Cieslak, N. NIST cybersecurity framework adoption on the rise. Tenable Network Security. 2016. https://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise

[39] US Department of Homeland Security. Continuous Diagnostics and Mitigation. Department of Homeland Security. 2018. https://www.us-cert.gov/cdm/home

[40] Brad Karp. Federal Guidance on the Cybersecurity Information Sharing Act of 2015. Harvard Law School Forum on Corporate Governance and Financial Regulation. 2016. https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

[41] Ari Lazarus. FTC sues D-Link over router and camera security flaws. Federal Trade Commission. 2017. https://www.consumer.ftc.gov/blog/2017/01/ftc-sues-d-link-over-router-and-camera-security-flaws

[42] Defense Department. Department of Defense (DoD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities. Federal Register. 2015. https://www.gpo.gov/fdsys/granule/CFR-2013-title32-vol2/CFR-2013-title32-vol2-part236

[43] European Union. General Data Protection Regulation. 2018. https://www.eugdpr.org/