Cyber Defense of Space Assets

Ryan Hutchins

Contents

Abstract

Our modern way of life depends greatly on space assets. These assets are mostly either unprotected or have minimal protection against cyber attack. For example, many military constellations rely on encrypted transmissions from the ground-control segment to the spacecraft, but have no further defenses, such as least permissions, intrusion detection, and mitigation, should an attacker manage to circumvent the encryption. The most prominent potential ingress for a cyber attack against such a system is the ground-control station. A hacker that compromised the station could take complete control of a spacecraft by sending messages prior to encryption. The attacker could also leave behind an advanced persistent threat, to make strategic use of compromised satellites at later times. The threat of this attack vector is reified by the numerous successful cyber attacks directed against NASA. This report details several issues in the cyber defense of space assets: (1) it reviews and classifies several known vulnerabilities in civilian and military space systems; (2) it provides details of several successful cyber attacks against space assets using these vectors, including the recent, successful hack of the Iridium Satellite constellation by hackers at the Chaos Communication Camp in Zehdenick, Germany; (3) it discusses current efforts to remediate space system vulnerabilities; and (4) it concludes with recommendations for a more secure future in space.

Introduction

"There is no greater danger than underestimating your opponent."

-Lao Tzu, Tao Te Ching*, Ch. 69*

The computer technology industry has grown at an explosive pace for the last half-century. This business climate has engendered numerous horse races between businesses competing to be the first-to-market with user-facing products and features. Although it is very attractive to be the first to market from a business perspective, the push for an ever-expanding set of software features has made the security of software and of cyber-physical systems an afterthought. The result of failing to design systems with security in mind is a proliferation of highly-vulnerable devices that are currently using the World Wide Web to wreak havoc on the systems connected to it. [1] [2] [3]

Vulnerabilities abound even in highly sensitive systems, such as civilian and military satellite constellations that are used for communications, navigation, time synchronization for distributed systems (think "power grid"), weather forecasting, and deterrence weapon systems. Many valuable space assets were placed in orbit with the assumption that their space-based nature would afford sufficient protection from would-be hackers. This assumption may have been valid at the time, but it has not kept pace with the technology revolution. We have underestimated the distributed ingenuity of humanity, and in so doing, we have underestimated our opponents. An individual hacker can now intercept, e.g., Iridium satellite traffic, with a homemade, software-defined radio assembled for less than one-hundred dollars and using instructions that are freely-available on YouTube. Moreover, many satellites were orbited prior to cyber-security considerations being taken seriously to the extent that we take for granted today. Given the ubiquitous reliance of modern technology on space-based assets, the potential exists for attackers to spark a global catastrophe should they compromise the confidentiality, integrity, or availability of satellite systems. This potential is especially strong in situations where highly sophisticated, globally distributed systems have come to depend on a technology, such as GPS navigation, for which there is no backup system.

In this article, we will discuss the importance of space assets and how they fit into a larger civilian and military security perspective. We will describe some of the known vulnerabilities of satellite systems, as well as the potential consequences of malicious hackers exploiting them. Finally, we will discuss current efforts, plans, and recommendations for remediating space-asset vulnerabilities.

A Brief Introduction to Space Systems

Space systems, such as the Air Force Satellite Control Network (AFSCN), and NASA's Deep Space and Near Earth Networks (DSN & NEN) comprise two types of asset: a space segment and a ground segment. The space segment generally consists of satellites in earth orbit. When there are multiple satellites working together for a common purpose, such as with the Tracking Data Relay Satellites (TDRS), they are collectively referred to as a constellation. The ground segment is a set of geographically distributed stations with powerful satellite communications (SATCOM) equipment that can send command and control telemetry to satellites and receive telemetry data from the satellite's systems and instruments.

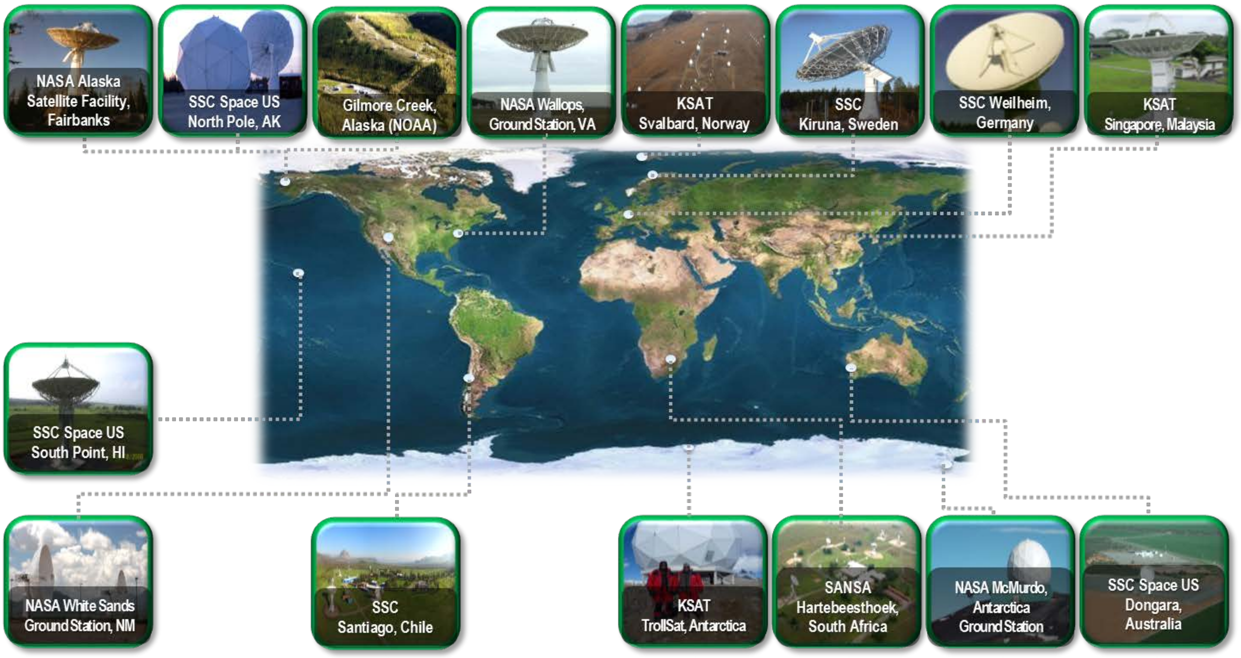

NASA Alaska Satellite Facility, Fairbanks
SSC Space US North Pole, AK
Gilmore Creek, Alaska (NOAA)
NASA Wallops, Ground Station, VA
KSAT Svalbard, Norway
SSC Kiruna, Sweden
SSC Weilheim, Germany
KSAT Singapore, Malaysia
SSC Space US South Point, HI
NASA White Sands Ground Station, NM
SSC Santiago, Chile
KSAT TrollSat, Antarctica
SANSA Hartebeesthoek, South Africa
NASA McMurdo, Antarctica Ground Station
SSC Space US Dongara, Australia

Figure 1: NASA's Near-Earth Network Ground Stations. Image courtesy of NASA

In the case of military constellations. There are often mobile SATCOM units in the ground segment of the network that allow forward-deployed units to navigate and maintain situational awareness of their surroundings. Vulnerabilities in mobile and stationary ground segment components are the primary attack vectors through which an attacker can compromise the confidentiality, integrity, or availability of a satellite. Because satellites must accept communications including command and control information from the ground segment, compromising the ground segment may enable an attacker to take control of a satellite completely. This threat is particularly potent if there is a single bus for all types of telemetry received by the satellite. The single-bus design was a serious concern in automobile hacks because communications from the satellite radio went to the same messaging bus as automatic steering commands, enabling an attacker to use the radio to send steering commands to the vehicle [4]. This same weakness could be exploited on a satellite. (See the section entitled: The Vulnerabilities).

To the Community

Why Cyber Defense of Space Assets?

Cyber defense of space assets is considered a top priority by the United States military [4] [5] [6]. Space assets have, perhaps even to a greater extent than ordinary, consumer electronics, been left bereft of security measures against cyber attack. The reason for this lack of security is described in [7]:

> *"Security in space systems is often based upon strong boundary protection in the ground segment with encryption to protect communications with the spacecraft. Onboard a satellite, there is an assumption that communications with the ground and among components on the spacecraft bus can be trusted due to encryption and assurances in the supply chain. This means spacecraft are designed with few if any cyber defenses. If an adversary were able to gain access to the ground segment or insert malware into a spacecraft component, there are often few or no protections to prevent them from directly*

> *controlling the space segment."* – Cohen, Ewart, Wheeler, and Betser, *Spacecraft Embedded Cyber Defense – Prototype and Experimentation*

The consequent lack of security measures built into space assets makes this a very ripe area for the identification of problems. Moreover, given the remoteness and lack of physical access to space assets, the domain represents unique challenges. One such challenge is the need to perform satellite firmware updates that may require more than a single fly-by. These updates can only be performed when the satellites are visible to ground stations. A firmware update that must be delivered to multiple satellites may be beamed to a single satellite across multiple passes over a ground station, and then transmitted by that satellite to other satellites requiring the same update. Despite the challenges in dealing with satellite remoteness, the software problems afflicting satellites are precisely the same as those afflicting ordinary software. These problems can be particularly pronounced in the space segment because security was not incorporated into a design of satellites' computing systems. Additionally, many of these aging systems contain legacy code from a time before security was taken as seriously as it is today.

The final reason for selecting space assets as a topic is that space assets are vital assets. They are the means by which many fundamental systems on which our way of life depends function, and their compromise could spell disaster for the world. Space assets are the basis for the asymmetric warfare deterrence strategies that help to keep the US, Russian, European, and Chinese spheres of influence relatively peaceful and prosperous. They are the means by which civilians communicate vital information, by which the power grid is kept synchronized, and by which stock-market transactions are timed. These transactions facilitate global trade and provide materials for, e.g., disaster relief and reconstruction projects. Moreover, global navigation services, such as GLONASS and GPS that are used for trans-oceanic shipping and in daily civilian travel depend on these vulnerable assets.

The Importance of the Topic

Given that there are few distributed technological system that does not rely on satellites for some vital piece of its functionality, the importance of space assets and retaining the confidentiality, integrity, and availability of the information that they carry cannot be overstated. For example, satellites provide the microsecond-level timing required for stock market transactions. Should the availability of such timing become unavailable, the economy could be crippled, leading to shortages of food, water, medicine, and commodities. The importance of space assets is continuously increasing with time, and the Chatham House estimates [8]:

"The space market in both the upstream (the building of rockets and vehicles) and the downstream (goods and services enabled by space technology – i.e. the 'applications' market) is estimated to be worth £125 billion per annum today, and some £400 billion by 2030."

Satellite data provides aerial coverage to, for example, view an area struck by natural disasters. Satellites enable live reporting of the event, and provide the information for intelligent and organized coordination of international relief efforts. This communication conveys regional crises, such as shortages in life-sustaining supplies, whose presence or absence could mean the difference between regional stability and destabilization.

Moreover, US national security and, indeed, the peace and prosperity of the free (and even the unfree) world relies on the functionality of asymmetric weapon systems as a deterrent, and this may be threatened by a single rogue actor. In their 2011 International Strategy for Cyberspace, the Office of the President of the United States stated [8]

> *"Military strategic and tactical missile systems rely on satellites and the space infrastructure for navigation and targeting, command and control, operational monitoring and other functions. However, insufficient attention has been paid to the increasing vulnerability of space-based assets, ground stations, and associated command and control systems. Cyberattacks on satellites would undermine the integrity of strategic weapons systems, destabilize the deterrence relationships and obfuscate the originator of the attack without creating the debris problem that a physical attack would cause. Because cyber technologies are within the grasp of most states (no matter how small or impoverished) and non-state actors, they level the strategic field and create hitherto unparalleled opportunities for small belligerent governments or terrorist groups to instigate high impact attacks. As stated in the 2011 US International Strategy for Cyberspace, international approaches and cooperation are needed in order to address and mitigate the full range of cyber threats to military systems."*

An Erosion of Faith

One major consequence of exploited cyber security vulnerabilities is the erosion of faith in the technological systems that comprise the modern world. As the above example whose result could be regional food, water, and medicine shortages implies, there is no level of Maslow's *Hierarchy of Needs* that cannot now be threatened by a cyber attack. Indeed, Todd Humphreys recently demonstrated the capability to spoof GPS signals to a degree that allowed him to crash a military drone and steer a civilian yacht miles off course [9]. This demonstrates a capability, which was impossible for a nation-state adversary ten years years ago, that can now be executed by an individual with sufficient technical know-how and a few hundred dollars.

The GPS system provides both the aforementioned timing for stock market trades, as well as military and civilian navigation. Given the relatively low technological barrier to spoofing existing GPS systems, it is quite conceivable that GPS spoofing could soon be used regularly to lure drivers into unsafe areas or lure ships in international waters into pirate ambushes. A few high-profile incidents of this nature would be enough to erode the population's faith in GPS completely. The result could be mass hysteria.

The same holds true for the satellites that relay our communications. Many communications are made with a reasonable expectation of privacy, and should that be breached by, for example, individuals capable of intercepting satellite traffic to expose personal or state secrets, the resulting damage to the faith in our systems could be catastrophic.

The Third Offset Strategy

"*Therefore, one-hundred victories in one-hundred battles is not the most skillful. Subduing the other's military without battle is the most skillful.*"

-*Sun Tzu,* The Art of War

The United States military is currently employing the Third Offset Strategy to retain its role as the prominent military power in the world. The Third Offset Strategy is based almost entirely on space assets. An offset strategy is some means of compensating for a disadvantage in a military competition by changing the competition to play to the strengths of the strategy's employer, negating the opponent's inherent advantages. It is a competitive strategy that seeks to maintain competitive advantage over potential adversaries over long periods of time, while preserving peace where possible.

The two previous offset strategies employed by the United States military were both used during the Cold War against the Soviet Union. During the Cold War, the Soviet Union had a distinct advantage in number of active military personnel and conventional military equipment. The United States military rendered that advantage irrelevant by developing a nuclear arsenal and unpreventable second-strike capability. Nuclear weapons could destroy a virtually unlimited number of conventional military assets and render the impact area uninhabitable for decades. Since the US retained the ability to launch such a strike even in the event of global devastation to itself and its allies, the offset succeeded in rendering any conflict with the United States unwinnable or pyrrhic.

The Second Offset Strategy was the invention of intelligent, long-range munitions. As the Soviet nuclear capability kept pace with the US capability and led to a standoff called "mutually assured destruction," willingness to jump from conventional to nuclear action was akin to a bluff, with neither side knowing whether or not the other was bluffing. To continue offsetting numerical superiority in Soviet conventional forces, the US developed long-range, smart munitions capable of accurately striking Soviet conventional forces before the Soviet forces would be within detection range of US forces. The threat of this technology and the Soviets' economic inability to invest sufficiently to develop an equivalent capability helped to ensure the integrity of Western Europe's borders until the collapse of the Soviet Union.

The Third offset Strategy uses space capabilities, such as GPS and constellations of reconnaissance satellites, to provide the US military with globally accurate positioning, navigation, timing, and targeting for allied and opposing forces. This capability, coupled with a retained advantage in conventional military assets, gives the United States military a massively asymmetric advantage over all of the other militaries in the world. However, should the security of such assets fail, a major part of the US' military advantage would vanish. For example, should the confidentiality of satellite-provided positioning data for friendly forces fail, the enemy would know the location and form of our military as well as we did. Failure of information integrity could lead to soldiers being tricked into going off course. Examples of this may have already occurred [10] [11]. Should the data from US space assets become unavailable on the battlefield, US conventional forces would then face a "slugfest," wherein their conventional assets would be pitted against those of a foe who is likely numerically superior. Given the forward deployment of the US military in most contemporary engagements, the enemy would then have "home field advantage," and the certainty of US military victory might be in doubt.

Way of Life

Space-based assets are very important, also, for much of the enabling technologies that facilitate our modern way of life. Radio, television, and the internet are just a few of the communications media that depend on satellite technology. These media provide us with entertainment, as well as information from the local weather reports that we use to decide how to dress for the day to the research papers that we reference in developing cancer drugs. If this information should become unavailable or unreliable, there is no tracing the amount of damage that could be done to every facet of life ranging from individual safety to the global economy.

Attack Vectors and Vulnerabilities of Space Assets

The Vulnerabilities

Military

The United States of America has the most powerful military in the history of the world. It possesses assets so destructive they could render vast swaths of the Earth uninhabitable for centuries. With this power comes the onus of a terrible responsibility: the responsibility to ensure that these assets are available, that they are properly-functioning, and most importantly, that they are *never* in danger of unauthorized use by a rogue party. In light of these facts, the following excerpt from an article [12] about the 2015 Chaos Communication Camp (hereafter shortened to Chaos) where groups of hackers were able to intercept Iridium satellite message, is very potent:

> *"The Iridium satellite network consists of 66 active satellites in low Earth orbit. Developed by Motorola for the Iridium company, the network offers voice and data communications for satellite phones, pagers, and integrated transceivers around the world.* ***The largest user of the Iridium network is the Pentagon.***
>
> *'The problem,' Sec Explained, 'isn't that Iridium has poor security. It's that it has no security.' "*
>
> -*J. M. Porup,* It's Surprisingly Simple to Hack a Satellite

The Iridium satellite network was built in the 1980s and was already obsolete by the time it was launched. Any motivated high school student could Intercept, modify, or fabricate Iridium messages. The reason why hacking Iridium is so easy is that messages are sent in plaintext format using the GSM standard, whose specification is completely public. Iridium was designed before security – especially security for a system as remote as a satellite constellation -- was a major consideration. The designers and customers for the constellation believed that satellites in space would be too difficult to hack, regardless of the software capabilities of an adversary. The gamble was that ordinary civilians and rival nation states would lack the sophistication to communicate with Iridium. Fast forward thirty years and we can buy off-the-shelf components, such as the rad1o [13] software-defined radio that the Chaos hackers used to eavesdrop on Iridium's unencrypted messages. These devices were so small that they were used as badges at the conference. There is also substantial concern within the Air Force Space Command that other assets within, for example, the Air Force Satellite Control Network might be vulnerable to similar attacks. Consequently, the Air Force is seeding numerous business development opportunities to develop remedial technologies for this problem.

Small Satellites

One of the primary focuses in cyber security for space assets at present is another technology that has been enabled by the drastically reduced cost of sophisticated, commercial, off-the-shelf hardware: small satellites. There are currently hundreds of research and industrial groups around the globe working to build standards and buses for cubesats, nanosats, and microsats (We will refer to these three designations collectively as small sats.). Many of these groups are seeking to perform interesting space science experiments from these comparatively affordable platforms, while others (including and especially the military) are looking to employ massive fleets of small, inexpensive satellites for space situational awareness, as well as orbital debris tracking and cleanup.

The concern with these small sats is that 'security as an afterthought' will prevail in this domain as it has in commercial software. Small sat companies are competing to produce the first standard buses and communications protocols. In this environment, where being the first to market with a usable technology means the difference between life and death for a nascent company, security concerns are often brushed aside. With the impending proliferation of small satellites and the importance of the missions for which they'll be depended, this could mean a disaster that affects the lives of people on Earth and the safety of other space assets, which may be some combination of expensive, irreplaceable, vital to national security, or vital to quality of life.

Advanced Persistent Threats

A final topic that is of great importance in military space cyber security is the advanced persistence threat. An advanced persistent threat (APT) is a stealthy set of hacking processes that continuously affect a system over time. APTs are most often used to exfiltrate vital information from a business or government target over a long period of time. Because these threats must remain undetected while dialing home for information exfiltration, they require a high degree of sophistication and are most often the work of (actually sometimes used synonymously with) nation-state-sponsored hackers.

In the space domain, NASA has been a primary target for APTs aimed at cyber espionage. Given NASA's status as the most advanced space program in the world, foreign governments have strong motivation to steal NASA's intellectual property. This theft bypasses the decades and billions of dollars of R&D required for another country to develop the technology themselves. Consequently, hackers are hard at work developing cyber espionage APTs such as those in the Red October and Cloud Atlas malware families. Chinese hackers have used such remote access toolkits to steal the plans for advanced US weapons systems, including: the F-35 Joint Strike Fighter, the FA-18, the Patriot Missile System, RQ-4 Global Hawk drones, the P-8 Poseidon Reconnaissance Aircraft, the UH-60 Blackhawk helicopter, the littoral combat ship, the Aegis Ballistic Missile Defense System, and the Army's Terminal High Altitude Area Defense (THAAD) Missile Defense System. They have also used these APTs to attack US TRANSCOM, the agency responsible for moving US troops and military equipment around the world.

NASA drove home the direness of the situation in their FY 2012 Security Audit Report [13]:

> *"Increasingly, NASA has become a target of a sophisticated form of cyber attack known as advanced persistent threats (APTs). APTs refer to those groups that are particularly well resourced and committed to steal or modify information from computer systems and networks without detection. The individuals or nations behind these attacks are typically well organized and well funded and often target high-profile organization like NASA. Moreover, even after NASA fixes the vulnerability that permitted the attack to succeed, the attacker may covertly maintain a foothold inside NASA's system for future exploits.*
>
> *In FY 2011, NASA reported that it was the victim of 47 APT attacks, 13 of which successfully compromised Agency computers. In one of the successful attacks, intruders stole user credentials for more than 150 NASA employees – credentials that could have been used to gain unauthorized access to NASA systems. Our ongoing investigation of another such attack at JPL involving Chinese-based IP addresses has confirmed that the intruders gained full access to key JPL systems and sensitive user accounts. With full system access 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*

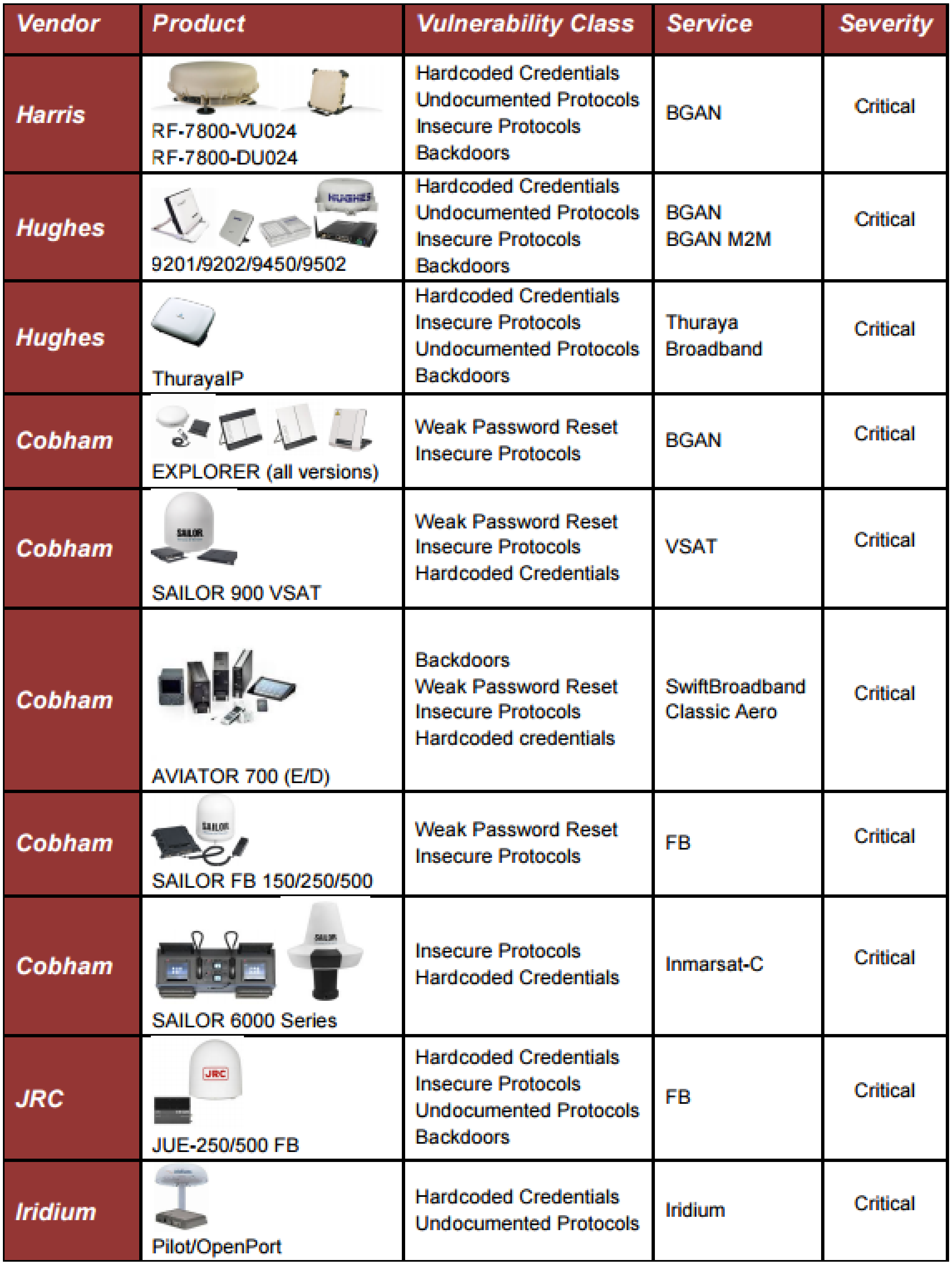
> *and compromise other NASA systems; and (4) modify system logs to conceal their actions. In other words, the attackers had full functional control over these networks."*

As described in NASA's report, APTs can be used to steal sufficient information over time for foreign agents to take control of US space assets. Indeed, Chinese hackers have already demonstrated the ability to gain control over weather satellites controlled by the National Oceanic and Atmospheric Administration (NOAA) [14].

The vulnerabilities responsible for enabling these threats are divided into three categories: software vulnerabilities, hardware vulnerabilities, and insider threats. Insider threats are threats caused by individuals who have been granted trusted access to the internal network. Insider threats can be either unintentional (e.g., clicking on a link in a spear-phishing email) or intentional (e.g., rogue military personnel, spy, or disgruntled employee turned traitor). Although these threats are tremendously interesting and important, we will focus instead on the technological vulnerabilities, and in particular, on the software vulnerabilities. The reason for our focus on software is that these are the easiest vulnerabilities to exploit remotely. Hardware exploitation, especially hardware exploitation of military infrastructure, requires site access.

The most important software vulnerabilities afflicting military space systems are, not surprisingly, the same vulnerabilities that have plagued civilian computer systems for decades. In particular, backdoors, hardcoded passwords, remote code execution (RCE), insecure protocols, spoofing, hijacking, SQL injection, insecure authentication, and file upload flaws are of primary concern.

In a 2014 security posture evaluation for US mission-critical space assets, IOActive discovered that these major vulnerabilities were present in *ALL* of the most widely deployed Inmarsat, Iridium, and Thuraya satellite communications (SATCOM) terminals. These vulnerabilities would allow a malicious actor to intercept (break confidentiality), manipulate (break integrity), or block (break availability) of SATCOM assets. In some cases, attackers could remotely take control of the physical terminal used to communicate with a satellite. For example, the Hughes BGAN M2M terminal has an 'admin code' backdoor that could be exploited using malware. This backdoor would allow an attacker to send an SMS message for an AT command to the satellite through the terminal. Figure 1 summarizes IOActive's investigation of SATCOM terminals used by the US military. Figure 1 summarizes the results.



Vendor	Product	Vulnerability Class	Service	Severity
Harris	RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

Figure 2: Vulnerabilities that IOActive discovered in common military SATCOM equipment

Finally, there is the threat that the hardware used to construct these systems could be used to deliver a hardware attack. This vector has recently been at the focus of cyber security news on account of its use in Mirai botnets. In particular, Chinese manufacturer, XiongMai Technologies' line of IoT products have hardcoded default passwords in their firmware. The Mirai malware logs into these firmware backdoors to take control of these devices and incorporate them into massive botnets that are capable of delivering devastating DDoS attacks. More to the point for military applications, components with hardware vulnerabilities can be intentionally incorporated into military products by malicious actors to enable one nation state to compromise the military capabilities of another. Thus, the US government regulates which components can be manufactured and sold in which places around the world through policies such as the International Traffic in Arms Regulations (ITAR) and export control.

Civilian

The same vulnerabilities that afflict military satellites also afflict many civilian satellites. Denial of service attacks on civilian satellites are possible by compromising their ground segments and flooding them with traffic, or, in the case of insecure protocols, simply by broadcasting strong enough signals from the Earth. Such attacks could seriously impact global trade, deny the forecasting required for early warnings of storms and other natural disasters, and prevent the use of civilian GPS.

Concerns about the vulnerability of GPS are not just restricted to DoS attacks on their satellites. Professor Todd Humphreys of the University of Texas at Austin recently demonstrated that he could hack both the military and civilian versions of GPS. Humphreys' technique is delicate, but well within the capabilities of would-be enemy nation states. It requires computing the ephemeris data for the GPS constellation (i.e., which satellites will be located at which points around the globe and when). GPS uses a form of positioning called triangulation (spherical surface triangulation here – please see non-Euclidean geometry for more details – thanks Gauss!). This triangulation requires a lock from at least three satellites to provide a latitude and longitude estimate.

Each satellite in the GPS constellation has its own code that it transmits along with the GPS-relevant data. Humphreys' technique uses the satellites' ephemeris data and a radio antenna to transmit the same codes as the visible satellites. The catch is that he can transmit data of his choosing from his data in a process called GPS spoofing. In order to prevent his spoofing signals from being detected as such, he begins by transmitting data that is identical to the real satellite data. This produces position estimates that overlap. Then he turns up the power on the signal from his radio and slowly moves his transmitted data away from the actual location. This process is called drag off and in practice, Humphreys has demonstrated that the technique can be used to crash UAVs and to lure yachts hundreds of miles off course. [9]

Defenses

Stakeholders have been very slow to realize the vulnerability of vital assets. When one considers the degree to which space technologies pervade and enable our modern way of life, these vulnerabilities could lead to any number of catastrophic events. For example, high-precision clocks on the GPS constellation are used in stock market trading and the US power grid. A malevolent actor, who was able to gain unauthorized access to a satellite and break either the integrity or the availability of this information could shut down the stock market or disable large parts of the power grid.

Classes of Attacks

The types of attack to which satellites are vulnerable fall into two primary categories: physical attacks and computer-system attacks. Physical attacks are those directed either directly against the satellite's physical bus or transmitted signals. The vectors for physical attacks vary greatly. For example, the act of transmitting signals that mimic a satellite’s or ground control station’s signals but contain false information, or “spoofing,” is a physical attack, as is jamming. But physical attacks also include anything from anti-satellite missiles to a “spray-paint attack, wherein” one satellite gets close enough to another satellite to spray paint its optics, rendering them blind. As these physical attack vectors are widely varied, a large number of diverse security measures are required to counteract them.

Computer System Attacks

Computer system attacks, on the other hand, are attacks that affect the computing systems present on a satellite. The ultimate goal in these attacks is unauthorized access to the satellite’s instruments, bus, and data. Common vectors for these attacks are the introduction of malware into hardware in the supply chain, and compromise of the ground units that communicate with satellites, including the ground control stations of, for example, the Air Force Satellite Control Network and NASA, or field-deployed SATCOM radios. These ground systems have many of the same software vulnerabilities that plague other computer systems. These vulnerabilities may be particularly prevalent in the space sector because the majority of the satellites and ground stations on which modern technology depends are decades-old and may use highly vulnerable, legacy software and protocols. This is particularly concerning because the space segment of space systems was believed to be beyond access by malicious actors, and as a result most security in the space segment relies on a secure ground segment. If the ground segment should be breached, the space segment is virtually unprotected. Moreover, given the lack of design with security in mind and the remoteness of space assets, security that is to be built into a spacecraft’s systems will have to be installed via remote software update, and mitigation strategies that must be introduced during the architecture and design phases of software deployment will not be available.

The evidence that space assets across the globe are vulnerable to cyber attack is incontrovertible. The fact that these space assets are being targeted is also beyond contestation. The catastrophic damage that a rogue nation states or other malevolent actor, such as a terrorist organization, could cause by attacking space systems in seeking to gain military advantage, gain publicity for their cause, gain financial advantage, showcase their skills, or just cause damage is difficult to overstate. With this being understood, let us examine the actions that we can take to secure our space assets.

Policies and Governance

Cyber security, and in particular cyber security of space assets, is a global issue. Cyber security is also a field of details. The details of a system’s design and implementation are highly specific technical matters from which vulnerability to cyber attacks arise. Although paradigms exist for engineered software systems, and some of these have overarching design weaknesses that lead to security problems, the details of a particular instance of vulnerability may depend on the specifics of implementation. As a result, catching and fixing security issues is a time-consuming process that requires a great deal of expertise. The time and expertise required to do this are often at odds with the market factors – in particular being the first to market on a limited budget – that are now beginning to drive the “new space” industry.

Due to the international, distributed nature of the problem and the fact the vastness of the potential places and ways that security issues can arise in software, hardware, the physical world, and with the humans who interact with the system, it is clear that wisdom gained in cyber security matters must become common wisdom. Best practices, vulnerabilities, exploits, and countermeasures must be shared openly between stakeholders in government and industry. Projects such as Mitre’s CWE and CVE databases [15], [16] and the Open Web Application Security Project (OWASP) [17] are a good start in this direction, but they have drawbacks for space cyber security. First, they're not specifically aimed at space cyber security, which is a field with its own special set of issues and circumstances. Second, they are used mostly by cyber security workers and not well known among the space community.

Currently, there is no international body corporate that represents the interests of the global space community in cyber security, but the need for one is discussed in detail in a report from the Chatham House think tank of the government of the United Kingdom [18]:

> *"Development of a flexible international space and cybersecurity regime is urgently required; this arrangement should be managed initially by an international 'community of the willing' – a limited number of able states and other critical stakeholders within the international space supply chain and insurance industry. Such a regime would avoid the inevitable delays in agreement and implementation associated with any regulated, centralized and directive approach developed by an international body – the International Telecommunication Union (ITU) for example – that would give the advantage to attackers as latter are unencumbered by compliance with relatively timeconsuming legislative controls. The new, agile regime would provide focus to rapid, active response mechanisms, and as a side benefit the body that coordinates and oversees it could also be tasked by the coalition to achieve market traction nationally and internationally for products and services related to cybersecurity in space.*
>
> *The proposed regime would thus provide a vehicle for practical leadership in delivering enhanced security within the whole of the global space sector, upstream and downstream and at all levels of the supply chain. It would also act, inter alia, as an independent convener, providing oversight and guidance, and could undertake gap analyses for security processes, review concepts of operations and procedures, determine the roles of associate organizations, assist in insurance risk assessments, and secure funding for capability development projects."*

The existence of this cybersecurity regime would provide the stakeholders with a dedicated, agile, and expertly knowledgeable organization dedicated to protecting space assets and the space domain.

Technical Solutions to Problems

In addition to the establishment of a space cybersecurity regime to disseminate research and best practices, there are some simple but very easy measures that can be taken to combat the technical issues with space assets that expose them to unauthorized, remote takeover. NASA's 2011 report entitled *Inadequate Security Practices Expose Key NASA Network to Cyber Attack* [19] declared the vulnerability of their mission-critical and sensitive data systems to internet-based attacks:

> *"Computer servers on NASA's Agency-wide mission network had high-risk vulnerabilities that were exploitable from the Internet. Specifically, six computer servers associated with IT assets that control spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable. Moreover, once inside the Agency-wide mission network, the attacker could use the compromised computers to exploit other weaknesses we identified, a situation that could severely degrade or cripple NASA's operations. We also found network servers that revealed encryption keys, encrypted*

> *passwords, and user account information to potential attackers. These data are sensitive and provide attackers additional ways to gain unauthorized access to NASA networks."*

Figure 1 shows the security issues that IOActive found with many SATCOM radios. The most common issues are very common suspects in firmware: hardcoded passwords, weak password resets, backdoors, insecure protocols, and undocumented protocols. That these vulnerabilities are already significant is evidenced by the Iridium satellite hack, which was enabled by a sufficiently powerful software defined radio and an insecure protocol. These vulnerabilities are easily exploited to grant access to whichever systems they reside in. They could allow a malevolent actor to gain control of any of the SATCOM devices listed in Figure 1. Fortunately, they are all easily fixed. The key is to perform static and/or dynamic analysis on the system, e.g., by using Veracode's static analysis service or OWASP's LAPSE+, to become aware of any undocumented protocols, hardcoded passwords in the firmware, backdoors, or password reset rules. Once discovered, these issues are very simply remedied. The issue of changing from an insecure to a secure protocol may require substantial software updates to satellites, which given the nature of satellite communication can be time-consuming and costly, but it is a soluble problem, provided that decision makers are convinced of the importance outweighing the inconvenience.

Other web-based vulnerabilities that facilitate remote access to satellites are mostly those that compromise user credentials because any attempt to control a satellite will require authorized access. Broken user credentials are likely to allow a malevolent actor to establish an advanced persistent threat in a satellite network. Aside from the standard training of personnel against social engineering attacks, such as spear phishing, organizations should perform code analysis and penetration testing to enumerate places where their infrastructure is vulnerable to credential compromising. The most common example of such a vulnerability is vulnerability to SQL injection, which can usually be detected using automated static or dynamic analysis (CWE 89). Once discovered, using an "accept known good" input validation strategy and minimally detailed error messages should work. If it's an option in the ground segment, restructuring architecture to use libraries that are not vulnerable to SQL injection would work.

The pattern of using code analysis to reveal known vulnerabilities and then choosing known methods to remove them at the design, architecture, or implementation level could be repeated ad infinitum. Indeed, as the NASA report specified that there were servers that revealed encryption keys, encrypted credentials, and user information, one can guess that a thorough static or dynamic code analysis would return a list of vulnerabilities probably including at least one of: SQL injection, missing encryption, cross-site scripting, use of a risky/broken cryptographic algorithm, hard-coded cryptographic keys, and buffer overflow. These vulnerabilities are all easily remedied and are not advanced attacks; however, if left unchecked, they leave space assets open to potentially devastating cyber attacks for which the enemy would not need to invest any development time.

We recommend that code analysis, penetration testing, and subsequent remediation of vulnerabilities that leave space assets vulnerable to high-likelihood, high-cost exploitation, especially those on the OWASP Top 25 List, be undertaken as soon as possible. Upgrading from insecure to secure protocols should also be done, where possible. Closing back doors and blocking messages from undocumented protocols should also be done, as it is a key vulnerability in a large amount of firmware used in SATCOM devices.

In close relation to closing backdoors, blocking undocumented protocols, and in conjunction with the need for oversight on the global supply chain, space stakeholders should remain vigilant over all stages in their supply chains, lest untrustworthy partners or individual actors within those partners emplace malware or backdoors for later exploitation. This is a principal way to establish and advanced persistent threat in a satellite network.

In addition to code analysis, forensic analysis of satellite hacks that have occurred, developing cyber war games and experimental systems to train personnel to defend space assets from zero-day threats and other advanced hacking techniques in real-time are under way [7] [20]. A major goal for space asset owners and stakeholders should be to develop the in-house expertise to "think like attackers" well enough to anticipate threat vectors before attackers so that systems can be hardened against them ahead of time, using an expanding repertoire of defense-in-depth strategies. This process can be aided by the abovementioned global space cyber security regime. One effort to develop this technique is cyber wargaming for space systems, and it is to this end that the demonstration accompanying this report relates. In particular, artificial intelligence systems are being designed to emulate attacker behavior, and live humans are being used to combat these AIs. More sophisticated cyber attacker AI speaks to more knowledgeable designers, and network defense systems that are successfully deployed against them indicate a growing expertise in defense.

Cyber defense of space assets is a current hot topic for research, and interest is poised to explode. Stay tuned.

Conclusion

Space assets are far more vulnerable to cyber attack than originally thought, and this realization has been slow, placing efforts to defend space assets well behind efforts to compromise them. The range of attack vectors that could potentially be used against space assets is vast, but the defensive effort is picking up steam. The three steps that space asset stakeholders must take to successfully defend their resources are: (1) to establish an agile, global regime that can provide training, intelligence, and knowledge sharing between stakeholders; (2) to perform code analysis and penetration tests to expose known vulnerabilities in existing infrastructure that can be shored up by relatively simple means. Once complete, this will ensure space asset safety against a wide range of basic attacks *that would currently succeed*. This will force adversaries to expend massive amounts of time and resources in an attempt to find successful exploits. (3) Aided by the established global regime, stakeholders must undertake research efforts into defense-in-depth design, and that enable them to anticipate vulnerabilities and exploits so that they may seize the initiative from attackers and design protocols, software, and spacecraft buses that are hardened against cyber attack.

Works Cited

[1] B. Krebs, "DDoS on Dyn Impacts Twitter, Spotify, Reddit," 16 October 2016. [Online]. Available: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.

[2] B. Krebs, "KrebsOnSecurity Hit with Record DDoS," 16 September 2016. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

[3] M. Riley, B. Elgin, D. Lawrence and C. Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," 17 March 2014. [Online]. Available: http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

[4] M. Gruss, "US Space Assets Face Growing Threat From Adversaires, Stratcom Chief Warns," Space News, 28 February 2014. [Online]. Available: http://spacenews.com/39669us-space-assets-face-growing-threat-from-adversaries-stratcom-chief/. [Accessed 25 November 2016].

[5] A. Carter, "The Department of Defense Cyber Strategy," The US Department of Defense, Washington, DC, 2015.

[6] C. Baylon, "Challenges at the Intersection of Cyber Security and Space Security," Chatham House, London, 2014.

[7] N. Cohen, W. Wheeler, R. Ewart and J. Betser, "Spacecraft Embedded Cyber Defense- Prototypes and Experimentation," in *Proceedings of the 2016 AIAA Space Forum*, Long Beach, CA, 2016.

[8] O. o. t. P. o. t. U. S. o. America, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.," 2016. [Online]. Available: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[9] M. Psiaki and T. Humphreys, "Protecting GPS from Spoofers Is Critical to the Future of Navigation," *IEEE Spectrum,* 2016.

[10] J. Keller, "Iran-US RQ-170 Incident Has Defense Industry Saying 'Never Again' to Unmanned Vehicle Hacking," Military Aerospace, 3 May 2016. [Online]. Available: http://www.militaryaerospace.com/articles/2016/05/unmanned-cyber-warfare.html.

[11] S. LaGrone, "Iran Seizes Two US Navy Riverine Patrol Boats, Tehran Pledges to Release Crews," United States Naval Institute News, 12 January 2016. [Online]. Available: https://news.usni.org/2016/01/12/breaking-iran-seizes-two-u-s-navy-riverine-patrol-boats-iran-pledges-to-release-crews.

[12] J. M. Porup, "It's Surprisingly Simple to Hack a Satellite," 2015. [Online]. Available: http://motherboard.vice.com/read/its-surprisingly-simple-to-hack-a-satellite.

[13] P. K. Martin, "NASA Cybersecurity: An Examination of the Agency's Information Security," NASA, 2011.

[14] M. Flaherty, J. Samenow and L. Rein, "Chinese Hack U.S. Weather Systems, Satellite Network," 2014. [Online]. Available: https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053- 65cea7903f2e_story.html.

[15] MITRE, "Common Weakness Enumeration," MITRE, 2016. [Online]. Available: https://cwe.mitre.org/index.html.

[16] MITRE, "Common Vulnerabilities and Exposures," MITRE, 2016. [Online]. Available: https://cve.mitre.org/.

[17] OWASP, "OWASP," OWASP, [Online]. Available: https://www.owasp.org/index.php/Main_Page.

[18] D. Livingstone and P. Lewis, "Space, the Final Frontier for Cybersecurity?," Chatham House, UK, London, UK, 2016.

[19] P. K. Martin, "Inadequate Security Practices Expose Key NASA Network to Cyber Attack," NASA, Washington, DC, 2011.

[20] T. Llanso and D. Pearson, "Achieving Space Mission Resilience to Cyber Attack: Architectural Implicatons," in *Proceedings of the 2016 AIAA Space Forum*, Long Beach, CA, 2016.

[21] R. Santamarta, "A Wake-up Call for SATCOM Security," IOActive, 2014.

[22] C. Bartholomew, D. Blumenthal, P. Brookes, R. Cleveland, R. D'Amato, J. Fiedler, P. Mulloy, D. Shea, M. Wessel and L. Wortzel, "US-China Economic and Security Review Commission," US Congress, Washington, DC, 2011.

[23] B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in *Proceedings of the 2011 International Confrence on the Internet of Things and 4th International Conference on Cyber, Physical, and Social Computing*, 2011.

[24] D. Storm, "Hackers Exploit SCADA Holes to Take Full Control of Critical Infrastructure," 2014. [Online]. Available: http://www.computerworld.com/article/2475789/cybercrime-hacking/hackers-exploit-scada-holes-to-take-full-control-of-critical-infrastructure.html.

[25] T. Humphreys and et al., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," in *Proceedings of the ION GNSS Conference*, 2008.

[26] A. K. Sood and R. Enbody, "US Military Defense Systems: The Anatomy of Cyber Espionage by Chinese Hackers," Georgetown Journal of International Affairs, 19 December 2014. [Online]. Available: http://journal.georgetown.edu/u-s-military-defense-systems-the-anatomy-of-cyber-espionage-by-chinese-hackers/.

[27] J. Pecharich, A. Viswanathan, S. Stathatos, B. Wright and K. Tan, "Mission-Centric Cyber Security Assessment of Critical Systems," in *Proceedings of the 2016 AIAA Space Forum*, Long Beach, CA, 2016.

[28] D. Fischer and et al, "Making Space-Link Security Work: Auxiliary Services to enable the CCSDS Space Data-Link Security," in *Proceedings of the 2016 AIAA Space Forum*, Long Beach, CA, 2016.