EXECUTIVE SUMMARY

Big Risks in Small Satellites

The Need for Secure Infrastructure as a Service

Harrison Caudill (harrison@hypersphere.org) – April 29, 2019

The United States relies heavily upon space-based infrastructure for everything from executing military operations, to hailing a taxi, to determining whether or not to bring an umbrella to the theater. Sudden loss of our orbital assets would be catastrophic to the strength of our economy[1], our ability to project power[2, p20-21], and the functioning of our civil society.[3, p3][4, III] Private companies are now launching hundreds (soon thousands) of small commoditized satellites each year as "New Space" grows.[5] Despite a lack of general awareness of the cybersecurity problem[2, p8], we are becoming ever more dependent upon our space assets, and our ability to protect them is rapidly declining.[6, §7p1] While this paper focuses on the smallsat revolution currently under way, its findings can be applied equally to most other space systems.

The United States is ill prepared for criminal cyberattacks directed at satellite infrastructure[7], and even less prepared for sophisticated state-sponsored efforts against our new constellations of privately-owned SmallSats. There are few security measures in place, and even fewer enforced regulations to protect these assets.[8, p5] Many regulatory recommendations being proposed, such as mandatory encryption, are inadequate. Immediate action is necessary to address the core security challenges of the space industry. By recognizing the immense ROI associated with a successful cyber attack we can begin to frame the security needs in their proper context.[4, p III, 20]

This paper discusses the specific challenges associated with securing orbital assets and offers policy recommendations to prepare us for the expansion of the space industry. It further proposes an efficient mechanism by which we can simultaneously enable market growth, ensure regulatory compliance, and mitigate the national security issues associated with this new phase of the space industry.

The Challenges of Space Security

Assets in space are unique in that, once deployed, builders and operators are unlikely to have direct access to the hardware again. The lack of physical access only intensifies the necessity of cybersecurity. Without the ability to unplug and reset the system, an intruder could potentially lock out the owners by changing the passwords, as it were. If that happens, the asset would then belong to the attacker; the owner would no longer have access. This threat represents an unacceptable risk to national security.[2, p23] Nation-states and criminals alike could potentially gain immediate control of critical strategic capabilities that they currently lack by hacking exposed satellites belonging to commercial entities. Worse yet, physical access may soon be granted to adversaries as satellite-servicing technologies are developed.[9, p13][10]

Recent security findings have shown that pre-existing space assets are vulnerable to attack.[6, §7p4] Openly discussed cyberattack methods are frequently less sophisticated than those already being employed by state actors, suggesting that America's satellite infrastructure may already be under attack. Security controls to combat such attacks vary wildly throughout the industry, ranging from practically non-existent, to best-effort large commercial organizations, to highly-secured government contractors. Many current

Revision: v1.0

policy recommendations meant to address vulnerabilities barely account for attack methods which have already been demonstrated, let alone sophisticated attacks which have not been observed or disclosed.[8, p2]

The greatest challenge to the development and deployment of appropriate security controls is the economic viability of doing so.[2, p13] Even the minimum necessary set of security controls and policies would likely be too much for most large companies to bear, to say nothing of small startups. Recognizing this key requirement, the recommendations below provide an efficient market-friendly solution that will not only ensure compliance, but also encourage market growth by actually decreasing startup and operational costs.

Recommendations

Strong new policies must be be developed and strictly enforced for the following:

1. Space assets relied upon by the DoD (eg. Commercial Weather)
2. Any space asset which would be of great value to an adversary if captured (eg. RADAR)
3. Anything deemed to be critical civilian infrastructure (eg. Internet of Things relays)
4. Any asset capable of being a physical threat (eg. Refueling Satellites)

The regulations necessary to provide even a minimum level of security would likely be too much for most companies to (at least willingly) bear without assistance. In order to ensure adoption of appropriate security standards by all market players, it is further recommended that incentives be created for two types of Infrastructure Service Providers:

1. Mission Operations Infrastructure Services
2. Communications Infrastructure Services

Just as wireless carriers are (nominally) tasked with securing their cell-phone networks, the listed types of Infrastructure Service Providers could ensure the existence of more secure (and more economical) alternatives to the current industry practice of vertical integration. Utilization of security-hardened versions of these services would greatly enhance the security posture of the industry while simultaneously decreasing entry barriers and increasing reliability.

Conclusion

Existing space systems owned by large organizations are vulnerable, small startup companies are even more likely to be vulnerable, and the stakes could not be higher. A single adversary could potentially neutralize critical military and civilian assets. A significantly higher level of cybersecurity protections are required to secure the industry.

A new class of space infrastructure is required to address the growing needs of the space industry, and the growing threat of cyber attack. Infrastructure as a Service has long been accepted in the computer and telecommunications industries. While it may be infeasible for all space companies to adopt minimum cybersecurity controls, a small number of Intrastructure Service Providers could readily do so. It is time for the space industry to take the next logical step in maturation.

Big Risks in Small Satellites

The Need for Secure Infrastructure as a Service

Harrison Caudill (harrison@hypersphere.org) – April 29, 2019

The space industry is experiencing a wave of commoditization and expansion akin to the computer industry's transition from mainframes to compute clusters. The number of new satellites launched each year continues to rise, with thousands of new satellites planned to be deployed over the next five years.[5][11] Typically, small satellites are used as part of a larger constellation, allowing any individual unit to fail without compromising the integrity of the constellation as a whole. Improved resistance to single points of failure combined with lower cost is driving several players to transition to constellations of smallsats.

The United States military relies heavily upon its space assets.[3, p3] Accordingly, Chinese and Russian military doctrines include counterspace weapons and tactics specifically to deny that advantage to their Western adversaries.[4, p20, 24] These nations are also actively developing their own space assets to mirror those capabilities that the United States already possesses, as well as expanding beyond.[2, p4] Outside of the military domain, the economic infrastructure of the United States relies heavily upon the continued functioning of US-controlled space assets. America's space infrastructure is a tempting target for adversaries. While kintic-kill anti-satellite missiles (ASAT) do exist, they are still expensive and rare. However, not only would it require hundreds of missiles to cripple a large constellation, it would also invite immediate retribution (as ASAT systems are anything but stealthy), and create a serious debris problem leading all closer to Kessler syndrome[1][12], indiscriminately denying access to aggressor and target alike. Cyberattacks represent a for more economical, straightforward and dangerously effective approach for bad actors.

The fundamental weakness in satellite security is inherent: you can't push a reset button. Nearly all security models make the assumption that the owners have physical access to the asset – an assumption which is hopelessly violated in space systems. While the advent of satellite servicing technologies presents an opportunity to remedy this limitation, it could just as easily exacerbate the problem if an adversary were to utilize that capability.[9, p13] In this environment, cybersecurity is paramount. Worse than losing an asset on which one depends is losing an asset and an adversary gaining it. The United States depends not only upon its own space assets, but also upon its adversaries either not possessing similar capabilities or at least needing time and money to acquire them. North Korea, for example, could acquire synthetic aperture RADAR capabilities by hacking an existing commercial constellation and Locking Out the owners.

Focusing strong new security regulations within Operations and Communications, opens the door for commercial Infrastructure Service Providers to bear the burden of implementation. With or without security, and whether using an external Service Provider or an in-house implementation, commands and data will likely flow through a Developer's Operations and Communications systems. As those two Infrastructure Services are reasonably consistent between organizations and missions, they represent excellent locations for standardization and implementation of security controls.

Space operations are no longer the exclusive domain of powerful nation-states[13] Criminal elements have already shown proficiency with cyberattacks of satellites[2] [7][14, p31-33,37-39][6, §7p1]; nation states

[1] A scenario in which satellite collisions cascade to the point where a debris belt is generated rendering those orbital regions useless for generations.

[2] IOActive found multiple vulnerabilities that could be exploited by criminals. Kaspersky labs found evidence of that actually occurring.

are known to be far more sophisticated. With cyberattacks against space systems on the rise[6, §7p1], this threat is very real and in need of immediate attention.

This paper proposes an economically viable solution to the lack of cybersecurity in the New Space industry. Because convenience and affordability are critical to compliance, this solution includes the development of Infrastructure Service Providers to offer secure and convenient alternatives to in-house design. First, applicable threat vectors are discussed. Next, recommendations are made to address them. Finally, a specific set of actions for the next six months are proposed.

Threat Model

Generally speaking, a constellation of satellites can be viewed as a compute cluster comprised of multiple independent systems.[8, p10] Satellites are, for the most part, computers with peripherals and network connections. The network connection doesn't work the same way, the usage model differs, and the stakes are higher, but the fundamentals are largely unchanged. The differences between space systems and traditional compute clusters must inform any space cybersecurity solution.

Lockout

Lockout, where an adversary permanently wrests control from the legitimate owner (Developer), is of utmost concern. If an attacker Locks Out a systems administrator, they have until someone can physically walk to the server and unplug it. That ultimate capability creates an incentive to be stealthy about successfully compromising a system. However, compromising a satellite and Locking Out the legitimate owner is the ultimate transfer of ownership. Political and military pressure could, theoretically, be applied to entities for hacking satellites – would the US really invade Iran if they were to hack a commercial weather-satellite constellation and Lock Out the owners? It is believed that "...if a future conflict were to occur involving Russia or China, either country would justify attacks against US and allied satellites as necessary...".[9, p13] With a history of cyberattacks against US infrastructure[15, p5], and an immense ROI for success, the problem of Lockout cannot be ignored.

Supply Chain

The reliability of vendor-supplied components and the vulnerability of supply chains to backdoors are both long-standing problems further exacerbated by the immaturity of New Space. While the introduction of surveillance equipment or other sabotage within a supply chain is not a new tactic[16] an additional risk worthy of consideration is that of reliability. Traditional space missions, with large budgets, are at least able to leverage a network of capable vendors; though even those vendors pay less attention to security than is warranted.[8, p5] This category of risk is recognized as being a major issue[17] and is at the heart of an ongoing struggle with China regarding the 5G wireless rollout.[18] While the defense industry may be taking steps to mitigate the problem, commercial organizations are far less sensitive to security than they are to profit. Newer constellations of cubesats face an immature supply chain and often find it more attractive and more effective to vertically integrate.[5, p21] Few companies, whether they are satellite component suppliers or operators, have the financial incentives necessary to develop secure systems with appropriate

emphasis on supply-chain validation. As observed in the IoT industry, without external stimulus, the market is likely to remain highly vulnerable to hardware backdoors and unreliable components.

Communications

Satellite communications systems are vulnerable to all of the same reliability and attack threats found on point-to-point wireless links on Earth such as interference, weather, interception, spoofing, as well as a host of standard networking security threats, and some threats unique to space operations. The wireless link is frequently directly between a base station (analogous to a cell tower) and the satellite (analogous to a cell phone). Alternatively, one can bounce the signal off of a relay satellite (analogous to a sat phone). Satellites using the Direct method will frequently be out of contact with a ground station under the control of the owner, and often find themselves within sight of a ground station owned by an adversary. This effect is similar to taking a long drive, and being exposed to a number of cell towers, and possibly some cell tower emulators.[19] Just like sat phones, satellites using the Relay Method may be able to launch with the latest hardware on them, but will still be limited by the hardware on the relay satellite, which is typically more expensive and longer lived; that means that any necessary hardware updates for a Relay system will be rolled out more slowly than for a Direct system. Wireless systems typically require a great deal of precision and care on Earth at the best of times; more attention, care, and protection is required for assets in orbit.

With wireless communications as the only means of contacting a satellite, reliability is vitally important. A satellite which cannot be contacted to execute a collision avoidance maneuver is just as dangerous as a satellite that is maliciously placed on a collision trajectory. The dearth of commercial Carriers, and prevalence of vertical integration makes reliability one of the largest risks in the industry. Many of the same methodologies used to improve reliability will also improve the security of the wireless link. Resistance to jamming, for example, works as well for unintentional jamming as for deliberate. With both China and Russia investing heavily in electronic counterspace capabilities (including jamming and cyberwarfare)[6, p 20, 24], it is crucial to ensure the security and reliability of the communications channel.

Operational Environment

Operations Systems, which ease the process of mission execution through simplification and automation, are necessarily granted levels of access to critical systems which can be dangerous if not properly protected. It is essential for Operations Systems to be empowered as they are tasked with managing constellations currently in excess of one hundred (soon to exceed one thousand) satellites. To do so, an Operations System may have access levels necessary to change encryption keys, reset passwords, or re-install operating systems. With that level of access, the system must be guarded against unauthorized and accidental command execution.

The space environment presents unique operational challenges leading to situations which consumer hardware will never encounter. The JAXA Hitomi satellite was able to spin fast enough that it physically broke apart.[20] In 1998 the ROSAT satellite was pointed at the sun causing physical damage.[14, p31] It was later revealed that the operational error was coincident to a cyber intrusion by Russia.[14, p31] Whether by accident or intention, a command that fell outside of the safe operational limits of the satellite was executed and physical damage resulted.

The operational system is typically also responsible for ferrying commands to a satellite, and receiving data from them. In all cases, the commands must be sanitized to ensure proper protection of the asset and of the environment. In cases where the data being collected is sensitive (such as imaging data for the DoD), then the data pathways must also be secured. Without proper security in the operations systems and software, attackers could potentially execute commands on the satellite and intercept resulting data.

Recommendations

It is recommended to utilize a combination of strong new security regulations[3] and market incentives to efficiently secure space systems, encourage innovation, and ensure continued US market leadership.

Given the critical nature of the systems to be protected, and the immense ROI of a successful attack, strong new security regulations must be drafted and enforced. However, even with light regulations and strict enforcement, there will still be issues of noncompliance without market-friendly infrastructure in place to assist with the compliance burden. [4][21, p1,10][2, p24]

Policy Recommendations

Enforceable minimum security standards and policies should be created and adopted, ensuring a strong cybersecurity posture for the following categories of assets:

1. **Space assets relied upon by the DoD:** If the USAF depends upon a commercial weather data provider to prepare for an operation, then that constellation represents a potential vulnerability. A commercial imaging system used for military operations may carry data that is just as sensitive as a spy plane.
2. **Space industry assets which would be of great value to an adversary if hacked:** North Korea is reported to be expanding its space-based Earth observation capabilities.[4, p32][22] Their counter-space aresenal also includes cyber methods. If they were to use their already sophisticated hacking teams to wrest control of a commercial SAR (Synthetic Aperture RADAR) constellation, then US military doctrine would be, at best, forced to transition to a contingency.
3. **Critical civilian infrastructure:** The United States' civilian population and economy depend quite heavily upon space infrastructure[2, p36], much as they depend upon utility companies. While the US' track-record with respect to protecting critical infrastructure from cyberattacks is checkered[23], it is worth protecting newly-constructed critical systems.
4. **Space assets capable of being a physical threat:** As use cases continue to expand, it is worth considering the offensive capabilities of a given satellite.[2, p23] For example, a refueling station would likely have propulsion on board and probably also have sufficient reaction mass to reach the geosynchronous belt. Even slow-moving satellites are travelling at $18,000mph$; if they are maneuverable, then they are as much a threat as any anti-satellite missile (ASAT).

[3] The author has specific policy and technical recommendations, but they are beyond the scope of this paper.

[4] Swarm Technologies, for example, was recently found to have deployed and operated satellites shortly after their application to do so was denied, resulting in what some consider an insubstantial fine, and a Consent Decree to come into compliance.

Market Incentives

It is recommend that the United States use a combination of grants, loans, and contracts to encourage two specific types of space-specific Infrastructure Service Providers be further developed and fully security hardened:

1. **Mission Operations Services:** The ability to execute missions in a clear, verified, and automated manner is critical to stable and secure operations. When performing virtually any task, humans think and act at a high level. In a similar manner, satellite operations are expressed in higher-level terms such as “Have all satellits boost their orbit when able” vs “Have satellite 42 fire its thruster for 3.6 seconds at next apogee”. Reliable mission execution and data management systems are of great value to the market, independent of any security benefits.
2. **Communications Services:** The communications system is one of the most critical and difficult systems to implement in a satellite. A regulated market operator will be far more capable of producing a reliable, secure, and compliant system than a multitude of satellite Developers each attempting to reinvent the wheel. Similar to terrestrial wireless Carriers, satellites could engage a wireless Carrier who would hold the license, own and operate the infrastructure, and ensure reliability and security.

Market Adoption & Encouragement

The two proposed types of Infrastructure Service Providers (Operations & Communications) represent a market-friendly mechanism for adoption of new security controls. Such a mechanism is critical for compliance. Not only would these services provide a great step forward for cybersecurity posture, they would also greatly improve the overall reliability and efficiency of America’s growing space infrastructure while simultaneously lowering the cost and time barriers for development.

Solution: Specialization of Trade

Just as any specialized Infrastructure Service Provider (an ISP being an example) enables industry growth, the proposed two Services:

- Will decrease the overall cost of compliance
- Will decrease the time necessary for implementation of a new space system
- Will greatly improve overall reliability and performance of new systems
- Have already been reviewed and tentatively accepted by regulators

By providing the necessary support to these two types of security-hardened Infrastructure Service Providers (Operations & Communications), the US can adequately prepare for the inevitable (and ongoing[4, p21][6, S7-1]) cyberattacks against its space infrastructure. A combination of regulatory and financial assistance (such as contracts, grants, and small business loans) can ensure the development of the necessary market-friendly Service Providers.

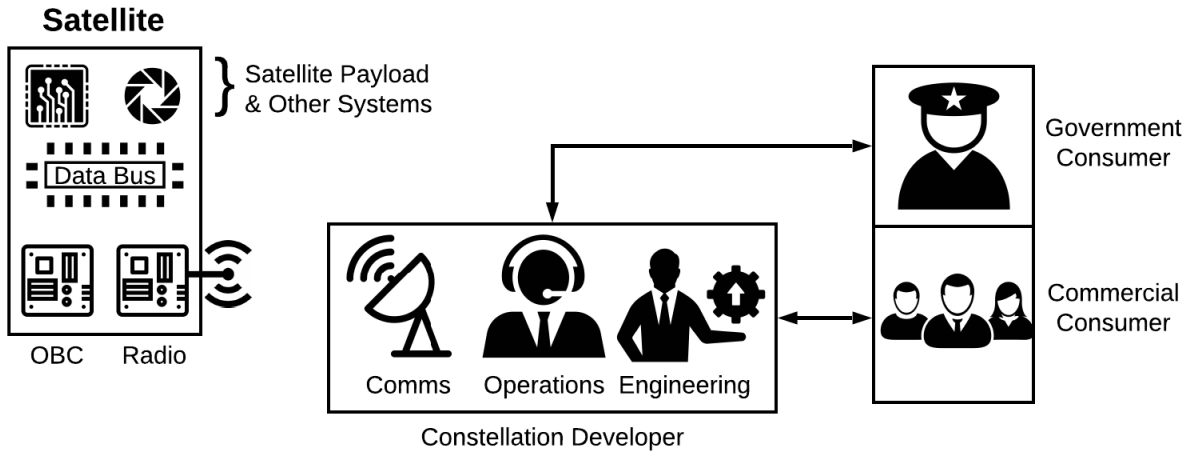

Figure 1: In a typical deployment, all end consumers (price-sensitive commercial customers and security-sensitive government customers alike) will work through the Developer's infrastructure. The entire security burden then falls on the Developer. All commands and all data flow through their systems.

Mechanics of a Space Mission

As a space mission is an enormously complex endeavor, we will restrict ourselves to a relatively straightforward example: that of a remote-sensing Earth-observation company. As shown in Figure 1, the end consumers of the remote sensing data (perhaps a shopping mall tracking the fullness of its parking lots) will contract with the Constellation Developer to image an area using one of its satellites. The Developer will add that mission to their queue in their operations center, which will use their communications system at the next available opportunity to assign the mission to an appropriate satellite. After being received by the satellite's radio, and relayed to its On-Board Computer (OBC), the observations will be executed at the appropriate time. Upon completion, the satellite will use an upcoming contact opportunity to downlink the data back to the customer via the Developer's infrastructure.

Adoption of the proposed security controls in the two recommended Infrastructure Services (either by internal implementation, or by contracting with a secure Service Provider) will lock down many of the available attack avenues, and data pathways involved in the lifecycle of a space mission. As shown in Figure 2, it is possible for sensitive customers, such as the DoD, to use the capabilities of the Developer's satellites in a secure manner without the Developer being required to implement the necessary security controls, and without the commands, data, and logs ever touching the Developer's systems. Commands to the spacecraft, and data returning from it are all passed through the secure Communications and Operations Services.

Operations

A proper Operations System will be capable of simplifying mission execution, but will also protect against unauthorized as well as accidental commands which may pose a danger. Once a satellite is commissioned and establishes a regular operational cadence, the vast majority of its time is likely to be

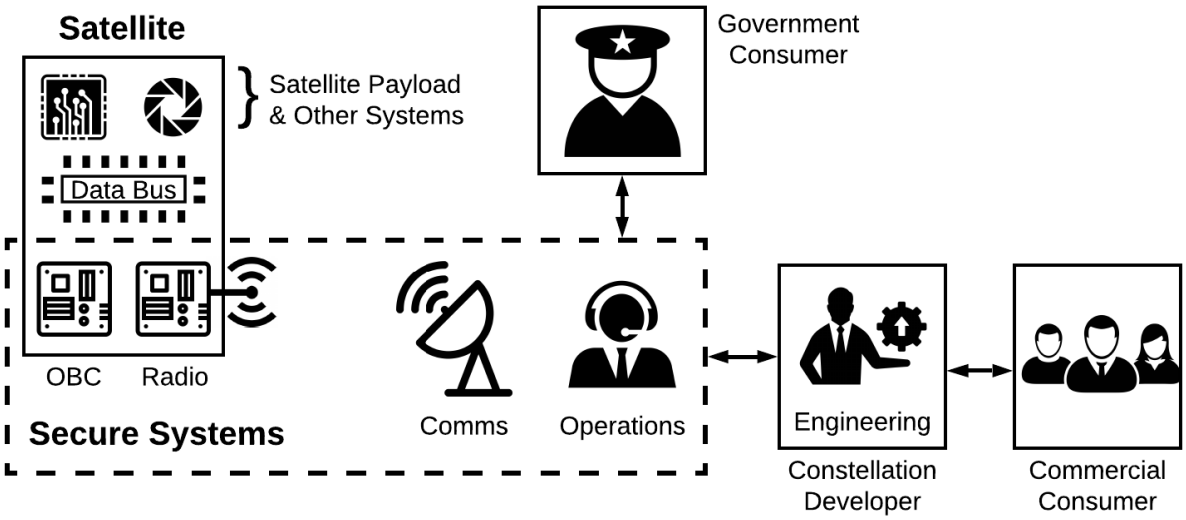

Figure 2: If utilized, then the two secure Service Providers as well as the accompanying satellite hardware (OBC and Radio) can lock down the critical data pathways. Security-sensitive customers, such as the DoD, would be able to utilize a direct connection to the secure operations center. The burden of security no longer falls on the Constellation Developer alone, as sensitive commands and data need not ever touch their infrastructure.

executing regular missions. In the example of the remote sensing system, that would mean observing targeted areas and downlinking the resulting data. With such a standard mission in place, it is possible for the Operations System to behave much like a firewall on a computer network by filtering out and flagging bad missions. For example, the DoD would be able to mandate that the remote sensing system not be used over the Pentagon, and have assurances that a responsible and security-hardened organization was overseeing compliance. Recently, it was discovered that a constellation of US satellites was providing capabilities to China as a service, while the technologies necessary to do so appears to be unavailable for export to China.[5][24] Operational monitoring and security is essential for any sensitive mission or critical capability.

Invariably, "Administrator" access will be required by the satellite Developer for actions such as software upgrades, and protecting that administrative pathway is essential. During times when Administrator access is required, there can be additional levels of security through the operations center for specific actions. For example, one privileged mission might be the collecting of system logs, upgrading software, or resetting a subsystem. Such actions will be necessary on a semi-regular basis, and must be supported in a reasonable manner. The Operations System can require, for example, that such missions occur during business hours, receive verbal approval from an operator at the company, or are executed with two-factor authentication. Ideally, all satellite operations can be defined as missions to be executed, and run through the secure operations center, and that operations center will be filtering, monitoring, and logging.

Ultimately, security-hardened Operations Infrastructure Services would be able to ensure sanity in the tasks transmitted to the satellite, and integrity of the resulting data all while guarding against cyberattack.

[5]While it is not clear that operational filtering as described here would have prevented this specific outcome, it is an excellent example of authorized operations potentially going beyond acceptable legal and/or ethical limits.

Secure Operations Services can be developed using combination of such standard techniques as rules-based access controls, multi-factor authentication, monitoring, and auditing. The Operations Service can also provide secure data and command pathways for sensitive customers, and standardized/trusted logging and recordkeeping.

One such company, KubOS, already exists, and is fully committed to seeing these recommendations become a reality. The economic model necessary to secure our space assets has already been demonstrated, and needs only the appropriate financial incentives necessary to evolve in a security-hardened manner.

Communications

Because of the issues surrounding physical access to the satellite, as well as the fundamentally exposed nature of the communications link, a secure communications system will be required. The communications system is the most likely location for Lockout to occur. Without that wireless link, the satellite is completely and totally unavailable to the Developer. The communications system is also the most vulnerable to Denial of Service through, for example, jamming.

There has been a great deal of recent effort regarding the easing of regulatory burdens.[25][26] While removal of unnecessary and unuseful regulatory barriers is appropriate, regulatory oversight and coordination exists for a reason. As more systems are deployed, and more players emerge, more and better regulations are called for. The FCC and ITU, for example, do important and enlightened work, and will remain important stakeholders.[27] Consider an extreme case: the Nuclear Regulatory Commission. Would it be prudent to make it easy for your neighbor to build an experimental nuclear reactor in their back yard after receiving a few million dollars in funding? A better way to consider this problem is to look at the Carrier Model. One does not need a license to use a cell phone as an end consumer. The Carrier Model for satellites was pioneered with the FCC by BStar Communications[6], and appears to have been subsequently adopted (in rhetoric if not in fact) by other players in the market.

Normalization

With the Communications and Operations Services more closely aligned with industry standards, the differences between satellites and computer clusters may be minimized, permitting the application of standard and robust systems. The security industry already spends billions of dollars each year securing networks, compute clusters, and endpoints.[28] If satellite constellations were normalized to behave more like traditional systems, then standard utilities become available not just for security, but also for basic operations. Networking systems could use IPv6 permitting the application of standard networking security utilities, for example. By normalizing the environment, one can leverage millions of man-hours of effort, and billions of dollars worth of research and development.

[6] In January of 2018, the author and lead counsel (Henry Goldberg) met with leadership at the FCC's Satellite Division (Jose Albuquerque and Karl Kensinger) along with several other FCC stakeholders. During that meeting the full details of BStar's Carrier Model were discussed and no significant problems were noted. BStar Communications was then invited to submit an application based on the Carrier Model for operating the first true wireless Carrier for space systems.

Summary

The economic barriers to a strong cybersecurity stance in the New Space industry can be all but eliminated by supporting two types of security-hardened Infrastructure Service Providers (Operations & Communications) and tailoring cybersecurity requirements to fall within their domains. An Operations Service Provider is capable of ensuring that command and data handling for satellite systems are done in a secure manner. Standard constellation management & operation would be available instantly to any new Developer. Similarly, a secure Communications Service Provider could offer a reliable, efficient, and secure link to any new satellite. Collectively, these two Infrastructure Services are sufficient to enact a critical set of essential security controls to most any space mission. The economic and regulatory viability of these two Service Providers has already been demonstrated. Because these two Services can be readily outsourced to an external Service Provider, industry participants would have no need to hire the necessary experts, and expend the necessary time and money to reap the benefits they supply.

The Next 6 Months: Getting to a First Draft

It is crucial that action be taken to develop specific security policy recommendations. Several industry participants and security experts already possess recommended policies at varying levels of completeness. A small working group of such experts should be assembled and empowered. That working group should include those with expertise in: space cybersecurity, physical security, space law, security policy, and national defense.

The next six months should be dedicated to producing a first draft of US Cybersecurity Policy recommendations with an eye towards outlining the needs of space infrastructure.

First Summit: Outline

An initial summit should be held with the express goal of creating the outline for a first draft of security policies and standards for space systems. The first step will be to grant the members an opportunity to work together to form an outline and a framework. Upon completion of the first summit, the working group should be in possession of a framework and an outline with which to work semi-independently on assigned sections.

Second Summit: First Draft

Once the members have completed their sections in coordination with industry, they should reassemble for a second summit with the goal of compiling a first draft of US Space Cybersecurity Policies. The members will have been in contact while drafting their individual contributions, and will have been able to work closely with industry at the same time. The net result of this process should be a set of policies that have seen industry, expert, and legal review.

Conclusion

Cyber threats have kept pace with the explosive growth in space technologies. The US must protect its current and future space assets. Typical security models assume physical access to the asset to be protected, and fall short when applied to space systems. Afterall, what good is encryption if a foreign adversary obtains the key, just once, and changes the locks? This nation depends upon its space assets for both military operations and civilian life. The loss of those assets would be catastrophic, and doubly so if they were lost to an adversary.

Space missions are notoriously complicated.Vendor networks for large satellites are established and capable, though frequently lacking in security; smallsat companies frequently lack any option, secure or otherwise. Few, if any, options exist for secure and auditable supply chains. Once a satellite has been deployed in orbit, it is dependent upon a complicated web of systems just for basic interaction over its wireless communications link. That link may be interfered with by accident or by deliberate jammming, it may be hacked and spoofed, and at the end of the day, it is still the only option available. If the Developer has passed those trials, they then must find a way to operate the satellite in a sane manner while navigating National Security issues, orbital collision avoidance, radio frequency collision avoidance, and prevention of unauthorized access and control.

Cybersecurity policies and regulations will only help if companies comply with those requirements. As it stands, any set of requirements that would be palatable to companies would be woefully inadequate, and any set of requirements that are sufficient would be economically infeasible for all companies to implement. However, a third option exists in which sufficient cybersecurity controls may be enacted while simultaneously decreasing time and monetary costs to new companies. If new cybersecurity policies are written to fall mostly within the Operations and Communications systems of a satellite constellation then it opens the door for third party Infrastructure Service Providers to solve the problem. It may be infeasible for all companies to enact sufficient security controls, but a small number of focused professional Service Providers could readily do so.

Focused professional Infrastructure Service Providers will be able to offer a more reliable and secure option than most vertically-integrated companies can afford. They will guarantee that even the smallest company with the biggest ideas, and the best innovation can still deploy their satellites, and make their waves. The biggest difference is that they can do more with less time and less money while being more reliable and more secure.

References

[1] J. Black. (2015, 09) The economic benefits of gps. [Online]. Available: https://www.gpsworld.com/the-economic-benefits-of-gps/

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

[3] W. L. Ross, "Driving space commerce through effective spectrum policy," U.S. Department of Commerce, Tech. Rep., 03 2019. [Online]. Available: https://www.ntia.doc.gov/files/ntia/publications/drivingspacecommerce.pdf

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

[5] "Nano/microsatellite market forecast, 9^{th} edition," SpaceWorks, Tech. Rep., 2019. [Online]. Available: https://www.spaceworks.aero/wp-content/uploads/Nano-Microsatellite-Market-Forecast-9th-Edition-2019.pdf

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

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

[8] G. Falco, "Job one for space force: Space asset cybersecurity," Cyber Security Project, Belfer Center, Tech. Rep., 07 2018. [Online]. Available: https://www.belfercenter.org/sites/default/files/files/publication/CSP%20Falco%20Space%20Asset%20-%20FINAL.pdf

[9] D. R. Coats, "Worldwide threat assessment of the us intelligence community," Office of the Director of National Intelligence, Tech. Rep., 02 2018. [Online]. Available: https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

[10] S. Erwin. (2018, 06) In-orbit services poised to become big business. [Online]. Available: https://spacenews.com/in-orbit-services-poised-to-become-big-business/

[11] M. WILLIAMS. (2019, 04) Spacexs starlink constellation construction begins. 2,200 satellites will go up over the next 5 years. [Online]. Available: https://www.universetoday.com/141980/spacexs-starlink-constellation-construction-begins-2200-satellites-will-go-up-over-the-next-5-years/

[12] D. J. Kessler and B. G. Cour-Palais, "Collision frequency of artificial satellites: The creation of a debris belt," *Journal of Geophysical Research: Space Physics*, vol. 83, no. A6, pp. 2637–2646, 1978.

[13] J. Porup. (2015, 08) It's surprisingly simple to hack a satellite. [Online]. Available: https://motherboard.vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite

[14] J. Fritz, “Satellite hacking: A guide for the perplexed,” *Bulletin of the Centre for East-West Cultural and Economic Studies*, vol. 10, no. 1, pp. 21–50, 05 2013. [Online]. Available: http://www.international-relations.com/CM2012/Satellite-Hacking.pdf

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

[16] D. Stover, “Spies in the xerox machine: how an engineer helped the cia snoop on soviet diplomats,” *Popular Science*, 01 1997. [Online]. Available: https://electricalstrategies.com/about/in-the-news/spies-in-the-xerox-machine/

[17] B. Schneier. (2018, 05) Banning chinese phones wont fix security problems with our electronic supply chain. [Online]. Available: https://www.washingtonpost.com/news/posteverything/wp/2018/05/08/banning-chinese-phones-wont-fix-security-problems-with-our-electronic-supply-chain

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

[19] B. Benchoff. (2016, 04) Build your own gsm base station for fun and profit. [Online]. Available: https://hackaday.com/2016/04/08/build-your-own-gsm-base-station-for-fun-and-profit/

[20] J. Foust. (2016, 04) Jaxa abandons efforts to recover hitomi satellite. [Online]. Available: https://spacenews.com/jaxa-abandons-efforts-to-recover-hitomi-satellite/

[21] F. C. Commission, “Fcc 18-184a1. fcc report and order,” Tech. Rep. File Number: EB-SED-18-00026685, 12 2018. [Online]. Available: https://docs.fcc.gov/public/attachments/FCC-18-184A1.pdf

[22] K. Vladimir. (2017, 12) North korean plans for two new satellite types revealed. [Online]. Available: https://www.nknews.org/2017/12/north-korean-plans-for-two-new-satellite-types-revealed/

[23] S. L. Erdman. (2018, 03) How vulnerable is the u.s. power grid to a cyberattack? 5 things to know. [Online]. Available: https://www.ajc.com/news/national/how-vulnerable-the-power-grid-cyberattack-things-know/YujzcltJ5wB2z8zJHyzPvI/

[24] K. O. Brian Spegele. (2019, 04) China exploits fleet of u.s. satellites to strengthen police and military power. [Online]. Available: https://www.wsj.com/articles/chinaexploitsfleetofussatellitestostrengthenpoliceandmilitarypower11556031771

[25] C. S. S. M. ASSOCIATION, “Fcc 18-86. streamlining licensing procedures for small satellites,” Tech. Rep. FCC Record Citation: 33 FCC Rcd 4152 (6), 07 2018. [Online]. Available: https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0417/FCC-18-44A1.pdf

[26] “Space policy directive-2, streamlining regulations on commercial use of space,” *Federal Register*, vol. 83-24901, 05 2018. [Online]. Available: https://www.whitehouse.gov/presidential-actions/space-policy-directive-2-streamlining-regulations-commercial-use-space/

[27] “Radio regulations,” International Telecommunications Union, Tech. Rep., 2016. [Online]. Available: https://www.itu.int/pub/R-REG-RR

[28] G. Pendse. (2018, 06) Cybersecurity. industry report & investment case. [Online]. Available: https://business.nasdaq.com/marketinsite/2018/GIS/Cybersecurity-Industry-Report-Investment-Case.html

[29] G. Falco, "The vacuum of space cybersecurity," 09 2018. [Online]. Available: https://www.researchgate.net/profile/Gregory_Falco/publication/327678396_The_Vacuum_of_Space_Cybersecurity/links/5ba06cfda6fdccd3cb5ef827/The-Vacuum-of-Space-Cybersecurity.pdf?origin=publication_detail

[30] "Space policy directive-3, national space traffic management policy," *Federal Register*, vol. 83-28969, 06 2018. [Online]. Available: https://www.federalregister.gov/documents/2018/06/21/2018-13521/national-space-traffic-management-policy

[31] T. C. Michael P. Gleason, "U.s. space traffic management: Best practices, guidelines, and standards," Center for Space Policy and Strategy, Tech. Rep., 08 2018. [Online]. Available: https://aerospace.org/sites/default/files/2018-08/Cottom-Gleason_U.S.%20Space%20Traffic%20Management_08272018.pdf

[32] J. Black. (2018) Our reliance on space tech means we should prepare for the worst. [Online]. Available: https://www.defensenews.com/space/2018/03/12/our-reliance-on-space-tech-means-we-should-prepare-for-the-worst/

[33] D. R. Coats, "Worldwide threat assessment of the us intelligence community," Office of the Director of National Intelligence, Tech. Rep., 05 2017. [Online]. Available: https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

[34] J. Didymus. (2012, 06) Texas college researchers hack us government surveillance drone. [Online]. Available: http://www.digitaljournal.com/article/327529

[35] J. R. M. Riley. (2018, 10) The big hack: Statements from amazon, apple, supermicro, and the chinese government. [Online]. Available: https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond

[36] S. K. R. Segal, "Hosted satellite payload procurement: A brief ḧow-toǧuide," Hogan Lovells, Tech. Rep., 03 2013. [Online]. Available: https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2017_2_2_gss_brochure.pdf

[37] M. Safyan, "Planet labs dove 3/4 data protection plan," Planet Labs, Tech. Rep., 06 2013. [Online]. Available: https://www.nesdis.noaa.gov/CRSRA/files/Dove%203%20and%204%20DPP%206-26-13.pdf

[38] "Licensing of private remote sensing systems," National Oceanic and Atmospheric Administration, Department of Commerce, Tech. Rep. 15 CFR §960, 2012. [Online]. Available: https://www.ecfr.gov/cgi-bin/text-idx?node=pt15.3.960

[39] "Department of defense (dod)defense industrial base (dib) cyber security (cs) activities," Department of Defense, Tech. Rep. 32 CFR §236, 2016. [Online]. Available: https://www.ecfr.gov/cgi-bin/text-idx?node=pt32.2.236

[40] K. Singh. (2019, 04) U.s. intelligence says huawei funded by chinese state security: report. [Online]. Available: https://www.reuters.com/article/us-usa-trade-china-huawei/u-s-intelligence-says-huawei-funded-by-chinese-state-security-report-idUSKCN1RW03D

[41] "Controlling space," *Aerospace America*, pp. 22–28, 04 2019. [Online]. Available: https://www.aiaa.org/docs/default-source/uploadedfiles/publications/other/aerospace-america-april-2019.pdf?sfvrsn=49882a68_0

[42] “Recommendation for space data system standards: Space data link security protocol,” The Consultative Committee for Space Data Systems, Tech. Rep. CCSDS 355.0-B-1, 09 2015. [Online]. Available: https://public.ccsds.org/Pubs/355x0b1.pdf

[43] “Standards for security categorization of federal information and information systems,” National Institute of Standards and Technology, U.S. Department of Commerce, Tech. Rep. 199, 02 2004. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[44] “Minimum security requirements for federal information and information systems,” National Institute of Standards and Technology, U.S. Department of Commerce, Tech. Rep. 200, 03 2006. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[45] “Security and privacy controls for federal information systems and organizations,” National Institute of Standards and Technology, U.S. Department of Commerce, Tech. Rep. 800-53-r4, 04 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4