Satellite Infrastructure Security and Resilience

CS 8803: Critical Infrastructure Security and Resilience

Aviva Smith and Gayathri Rajakumar

March 27, 2022

Satellites are integral to the operation of the government, military, private sector, and civilian life of most developed countries around the world. As satellite infrastructure becomes more fundamental to the function of global society, malicious cyber attackers will seek to exploit the vulnerabilities of such systems. Assuring their security and resilience is a must for any country seeking to gain an edge in space. Global powerhouse, such as the U.S., have long held superiority in space will have to invest in cutting edge satellite technology and space policy innovation to maintain their lead as rising powers such as China and long-standing competitor Russia rapidly close the gap in space dominion [23].

According to NASA, a satellite is a body that orbits another body in space. They can be natural (planets, moons, stars, etc.) or artificial (machines launched into space), but within the scope of this paper, 'satellite' will specifically refer to a man-made machine intentionally launched into orbit around another body in space [1]. In this paper, we will examine satellite infrastructure security and resilience through several faucets. We will briefly explore the watershed moments in the political and technological evolution of satellites. We will also cover some of the most memorable cyberattacks launched against satellites and the collateral damage they caused, as well as the incidental damage caused by collisions which are becoming more prevalent due to the accumulating waste in space. After that, we will analyze the security measures meant to protect satellites from malicious actors and understand the resiliency plans formulated by relevant organizations and departments. Lastly, we will explore the policies regarding the potential

promotion of the space sector to the status of the 17th critical infrastructure sector recognized by CISA.

Since the former Soviet Union successfully launched the first satellite Sputnik 1 into space in 1959, satellites have been a symbol of political, technological, and scientific superiority on the global stage. By being the first to successfully put an artificial satellite into orbit, Russia established itself as a long-term space power which the U.S. immediately challenged to maintain their lead on the world stage [2,3].

According to the UCS Satellite Database, as of September 2021, approximately 4,550 satellites orbit the Earth, 2,788 of which are operated by the United States. Of these satellites, 33 are for civilian needs, 2,359 for commercial use, 167 for government operations, and 229 for military projects. Primary competitors China and Russia hold 499 and 169 satellites respectively, and with their own rapidly growing space initiatives, that number is projected to rise exponentially. There are also 1,240 satellites floating in orbit that are owned by a variety of other nations with their own space programs. Furthermore, with private sector space operations becoming more ubiquitous, space will grow more crowded [5].

Satellites, have a long history, and despite their remoteness, they operate at the core of many technological frameworks. Their capabilities are simultaneously overestimated and underestimated as they exist at the intersection of two of the most challenging mediums – atmospheric space and cyberspace. With time, this distinction has become more convoluted [4]. Many segments of society are dependent on satellite infrastructure and their dependence is increasing as nations invest more into space operations. They are too expensive to lose due to negligence, so extra measures are taken to secure them. As they become more integral with the

function of other critical infrastructures, more capital and resources will be invested to ensure their durability and effectiveness [8].

Major Brian Stewart whom we interviewed in early March says that the significant monetary investment is required to construct satellites as they are to be sent into one of the most unforgiving environments accessible to humans. Not only does such a machine have to be capable of operating at full capacity limited repair, but it must also be equipped with technology sophisticated enough to support the mission for its expected duration [9].

Large satellites such as the European Space Agency's Envisat observation satellite can cost $3 billion to construct, while other satellites can be produced more cheaply, albeit with more limited functionality. The cost of launching a satellite is also dependent on the level of orbit to which it is intended to be sent. Launching a satellite to Low Earth Orbit (LEO) can cost a mere several thousands of dollars, while launching as far as the Geosynchronous Orbit (GEO) is far more expensive [9].

In part due to the absence of laws surround appropriate conduct, space is said to be the next major front for military operations and technological expansion. Major global powers are competing for space superiority and organizing programs to promote their agendas. However, it is unlikely that countries would take military action against each other's space lest such actions lead to retaliation on their own resources [12,13,14]. Major Stewart said that space has always been militarized as it was previously used to test nuclear weapons. Although this created long term problems, it has motivated nations to organize guidelines for permissible behavior in space. Satellites were included in these agreements because they allow parties to survey each other in space. They also serve as benign entities that are not to be attacked unless countries are officially launching a military offensive [9].

Along with the evolving cybernetwork that makes modern satellite infrastructure possible, there also comes new forms of exploitation. Satellites are lofty targets for malicious cyber attackers, so their security is of utmost importance. Cyberattacks are a very economical and viable threat that presents enticing alternatives to missiles and other more easily detectable anti-satellite methods as they leave behind very little evidence and origin attribution is incredibly challenging.

Nations such as the U.S., China, and Russia attempt to secure their satellites and space infrastructure with the best equipment available. Since it may be too challenging for ill-equipped hackers to hijack such satellites, they can target less secure satellites and use them as weapons against their more secure counterparts. One possible scenario is seizing control of one satellite and using it as a projectile to collide with another satellite or orientating the satellite in a damaging trajectory [14,15]. Nation-state actors also are motivated to disrupt one another's space operations. Jamming or corrupting the transmissions of a GPS constellation/satellite or testing the launch of hypersonic missiles are methods of exercising technical and political superiority [19].

While nation-states can equip criminal hackers with the best resources to exploit satellite vulnerabilities, independent or contract hackers are also proving to be a threat. With jamming and control-seizing technologies becoming more affordable and prevalent in the technology market, they have become more accessible to criminals [12]. So far there have not been almost any cases of a cyberattack destroying a satellite, but nevertheless, there are several notable cases of satellites being exploited by hackers.

In 1998, the first recorded cyberattack against a satellite involved hackers seizing control of U.S.-German ROSAT astronomy satellite. They angled its solar panels directly towards the sun and burned out the battery, rendering the satellite useless. To date, this was the first and only incident of its kin [12]. In another attack in 2007, hackers gained access to Landsat-7 satellite, but

did not wrest control away from the satellite crew. No damage was done but the cyber systems were clearly exploited and proven vulnerable [20]. In the following year, one of the most major attacks ever recorded happened when hackers seized control of NASA Terra EOS earth observation system satellite for 2 minutes in June and again for 9 minutes in October. Again, no damage to the satellite was reported, but the relatively short span of time between incidents on the same machine roused controversy about whether existing security standards were sufficient [20].

Beyond cyberthreats, satellites also face serious environmental threats caused by entities without malicious intent. Such threats include space debris comprised of asteroid remains, "dead" satellites that have floated into wrong orbits, and live satellites whose path of orbit intersects with that of other satellites. Collisions between satellites or space debris create more space debris which create additional threats of collision. According to Dr. Mariel Borowitz whom we interviewed in mid-March, the excessive debris in space poses the greatest threat to space sustainability. When space exploration first began, there were no real initiatives in place to collect the left behind space trash. Since the U.S. was the primary power in space, the debris was initially considered a tedious cost of operation, but when other parties began launching active space operations, space debris became a more tangible threat to peaceful operations [11, 13].

In November 2021, Russia destroyed one of its own satellites which shattered into 1500 trackable pieces with other debris spread throughout. Though it was not a direct attack on other satellites in the immediate sphere, the remains could have destroyed objects in the surrounding airspace. Although this is problematic because the destruction of dead satellites using missiles or ASATs leaves a significant of debris, it is still a common practice. [19] Though there are initiatives to clean up space, most notably new programs set up by China, the rise in international competition

in space has generated even more trash; hence, it is difficult to clean up old debris when new debris is being generated daily [11].

Secure and resilient architecture design plays a significant role in preparing satellites for whatever they may contend with. An individual satellite is compartmentalized into several segments designed to accommodate a limited set of operations to assure effective load balancing of tasks. This cataloging is also useful for assessing the types of threats that can be launched for approaching contingency plans. In the U.S., most satellites can be compartmentalized into the following three segments. More granular models have been proposed by organizations such as NIST, but these models still follow this segmentation [21].

The Space Segment consist of the satellite platform, related payloads, and the 'bus' which includes the command controls, information processing, etc. The space segment is the physical satellite hovering in orbit. The Ground Segment consists of the terrestrial based facilities where human operators can automate and manage the satellite functions. It can be distributed across several separate facilities and does not have to be housed near the facility where the Space Segment is launched. The Link Segment is responsible for transmitting data between the Space Segment and Ground Segment. The Link Segment must be secured by NSA approved encryption schemes while maintaining precise, real-time data transmission [21, 22]. Each segment of satellite infrastructure is susceptible to different types of cyberattacks. These attacks can be split into different categories based upon how they are launched and how they disrupt the system. This critical knowledge is needed to assess how segments are vulnerable and how they can be reinforced. The Ground Segment is prone to Malware, Trojan, and DDoS attack; the Space Segment is prone to MitM, zero-day, and ransomware attacks; and the Link Segment is prone to GPS jamming, eaves dropping, spoofing/hijacking attacks [24]. Accessing the cyber vulnerability

of satellites is a complex process. According to Sean O'Melia and Richard Skowyra at MIT Lincoln Laboratory who the first author interviewed in mid-March, there is not a definitive way to "measure" the severity of cyber vulnerabilities as there are too many attack surfaces to account for. If it were possible to perform a quantitative measurement to score a satellite's security performance, then the danger of cyberthreats would be negligible. Instead of attempting to quantify the security of a satellite based upon the vulnerability of the attack surface, they suggest numerous experiments are run to assess whether a satellite is secure against previously encountered threat models. In addition to testing with the threat models, there is a tiered system used to measure how well supplied an attacker is. Based upon this system, threat models can be tested to assess how effective they would be against attackers with varying resources available [10].

With the groundwork laid, a serious question must be posed: what are the consequences if a satellite or collection of satellites were to fail? It would be catastrophic if a GPS constellation were to fail. There would be significant delays in navigation, location detection, and broadcast transmissions, and globally specific clocks would be messed up. Utility grid operations, stock exchanges, data centers, and cellular networks all rely on the most precise clocks and location info in the world – the failure of satellites would throw these systems into chaos [25]. Furthermore, as the world becomes more reliant on 5G communications, eavesdropping, data corruption, and network jamming are potential threats. Though companies have argued that satellite infrastructure is merely used to boost communications speeds to meet demand and these satellites are handled by specialized third parties specializing, there is concern that exploited satellites could leak private information. This debate has sparked controversy across the tech industry [12].

Over the last seven decades, multiple schools of thought have been formed with the intent to shape the future of America's strategic space operations. The most prominent schools of thought

are the following: Space Sanctuary, Space Dominance, Space Survivability, and Space Superiority [14]. Space Sanctuary, the oldest school of space related thought in America, advocates for military operations in space, but argues against space weaponization altogether as part of avoiding the risk of nuclear war. While some experts advocate this more conciliatory approach, others feel that recent global events preclude this plan from being an option [16,17,18]. Space Dominance seeks for American hegemony in space. It argues for control over critical orbits, accessibility, and the protection of existing assets while expanding space initiatives and combating rivals' expansion efforts. It is an aggressive, militaristic plan, but has been argued to be the most viable option for any country seeking to control the space arena. However, it could provoke aggressive action from other nations if it is perceived as an intent to weaponize space. This approach was favored by the Trump Administration [13,16]. Space Survivability is a more passive approach which encourages decreasing reliance on remote satellites while enhancing anti-satellite attack (ASAT) infrastructure. Due to America's increasing dependence on satellites, this plan of action is said to be unreliable as it is much more challenging to drawdown space operations once they've been implemented [16]. Space Superiority, like Space Dominance, embraces more militaristic action in space but promotes a defensive, cautionary approach. It angles to deter aggressive parties from encroaching upon U.S. space action, while maintaining our current trajectory. Arguably, it is a more strategically subtle defense, but because it has no active goal, it could detract from the momentum necessary to make further progress in space. This school of thought was favored by the Obama Administration [16].

Several treaties have been created to facilitate secure space operations and promote a resilient political atmosphere. The Outer Space Treaty is the first treaty concerning space that has 110 state-parties on October 10, 1967. This treaty bans the stationing of Weapons of Mass Destruction

(WMD) and prohibits military activities on celestial bodies. Furthermore, it focuses primarily on peaceful exploration and use of space. Though this is a significant event for promoting space laws, the sophistication of space systems calls for laws that govern the attacks on space systems.

We have seen a myriad of incidents affecting companies and nations that are believed to have highly secure systems; cyberattacks appear inevitable despite huge efforts to combat them. However, effective laws will help us to protect our systems. The laws against cyberattacks have evolved since the Computer Fraud and Abuse Act (CFAAA) in 1985. The laws evolved as the lawmakers understood and defined computer systems and what constitutes an attack. We have come a long way since the CFAA, but only recently have lawmakers started considering the security of space systems as an integral part of space security.

The United States' National Space Policy addresses the nation's goals and commitment towards space activities. On December 11, 2017, President Trump signed the Space Policy Directive 1 (SPD 1) which is a change in the national space policy from the Obama administration. President Trump also signed an executive order to re-establish National Space Council. Among the various SPDs published, SPD 5 is focused on this paper. It is the nation's first comprehensive cybersecurity policy for space systems. This was issued in September 2020 by the Trump administration. It lays out five cybersecurity principles for space systems. Currently, a Presidential Directive aimed at implementing and improving cybersecurity in space systems is under review, but it is expected that the Biden administration will most likely retain SPD 5 with some modifications that ensure security. This SPD was welcomed by many industry veterans and highly ranked government officials. The National Space Council will now be headed by Vice President Kamala Harris and will prioritize the protection of space systems. These steps will ensure commercial satellites also have high integrity and can avoid cyberattacks.

Although there are laws for cyberattacks in general, it is difficult to enforce them as attribution is exceedingly difficult in cyberattacks and not all countries have extradition laws. The cybersecurity community has a lot of work to make sure that these laws are enforced, and the criminals pay their price. This is particularly important to satellite security as well because cybersecurity is the most dangerous threat to satellites right now.

U.S. is one of many nation states with high stakes in the race to secure space. Even in 1960s, 90% of military intelligence was collected using satellites. There are many systems that rely on satellites and any incident, malicious, or otherwise, on satellites can cause significant loses. Brian Scott, the director of critical infrastructure security for the National Security Council asserted that a cyber-enabled attack on the Global Positioning System alone would result in losses of $1 B (about $3 per person in the US) a per day to the United States.

The current goal of the United States is to ensure survivability in space. With many actors entering space, deterrence will act as a key factor in thwarting cyber-attacks. The major actors in space that might be of concern to the United States are Russia and China as well as non-state-funded actors. In the current political climate, establishing a long-term goal for satellite security will help the U.S. maintain its power. In our interview with Major Stewart, he mentioned that the U.S. is playing a short game, China is employing a 1000-year strategy and Russia is acting as an expansionist power. In our interview with Dr. Borowitz, she mentioned that the creation of a U.S. Space Force can be seen as an aggressive move by rival nations and could be an invitation for more attacks. This reinforces the idea that any political move might have a significant impact on the relationships between the nations. The declaration of space assets as vital national interests by the U.S. shows the nation's commitment towards satellite security and will help in maintaining the status quo in space.

CITATIONS

[1] "What Is a Satellite?" Edited by Ashley Campbell, *NASA.gov*, NASA, 5 Sept. 2018, https://www.nasa.gov/directorates/heo/scan/communications/outreach/funfacts/txt_satellite.html.

[2] History.com Editors. "The Space Race." *History.com*, A&E Television Networks, 22 Feb. 2010, https://www.history.com/topics/cold-war/space-race.

[3] Sagdeev, Roald. "United States-Soviet Space Cooperation during the Cold War." *NASA.gov*, NASA, 28 May 2008, https://www.nasa.gov/50th/50th_magazine/coldWarCoOp.html.

[4] Sathyanarayanan, A. "Types of Satellites: What Is Satellite, Types and Uses of Satellites." *EDUCBA*, 30 Mar. 2021, https://www.educba.com/types-of-satellites/.

[5] "UCS Satellite Database." *Union of Concerned Scientists*, Union of Concerned Scientists, 22 Jan. 2022, https://www.ucsusa.org/resources/satellite-database.

[6] "CISA Launches a Space Systems Critical Infrastructure Working Group." *Cybersecurity and Infrastructure Security Agency CISA*, CISA, 13 May 2021, https://www.cisa.gov/news/2021/05/13/cisa-launches-space-systems-critical-infrastructure-working-group.

[7] O'Connor, Peggy. "Designating Space Systems as New U.S. Critical Infrastructure Sector." *INSA*, 11 Feb. 2021, https://www.insaonline.org/designating-space-systems-as-new-u-s-critical-infrastructure-sector/.

[8] Waterman, Shaun. "DHS Weighs How to Protect Increasingly Critical Space Systems." *Via Satellite*, 29 Nov. 2021, https://www.satellitetoday.com/cybersecurity/2021/11/19/dhs-weighs-how-to-protect-increasingly-critical-space-systems/.

[9] Major Brian Stewart, Ph.D. Student in Georgia Institute of Technology School of International Affairs

[10] Ingols, K W, and R W Skowyra. Massachusetts Institute of Technology, Lexington, MA, 2019, *Guidelines for Secure Small Satellite Design and Implementation: FY18 Cyber Security Line-Supported Program*, https://apps.dtic.mil/sti/citations/AD1087142. Accessed 16 Mar. 2022.

[11] Honrada, Gabriel. "Space Trash: US Military Aims to Cleanse the Heavens." *Asia Times*, 9 Feb. 2022, https://asiatimes.com/2022/02/space-trash-us-military-aims-to-cleanse-the-heavens/.

[12] Tucker, Patrick. "The NSA Is Studying Satellite Hacking." *Defense One*, Defense One, 20 Sept. 2019, https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/.

[13] Dr. Marial Borowitz, Ph.D., Associate Professor in Georgia Tech Sam Nunn School of Intrnational Affairs

[14] Sean O'Melia, Technical Staff, MIT Lincoln Laboratory

[15] Richard Skowyra, Technical Staff, MIT Lincoln Laboratory

[16] Weichert, Brandon J., and Mackubin Thomas Owens. *Winning Space: How America Remains a Superpower*. Republic Book Publishers, 2020.

[17] DeBlois, Bruce M. Massachussetts Institute of Technology, Lexington, MA, 2019, *Space Sanctuary : A Viable National Strategy*, https://apps.dtic.mil/sti/citations/AD1087142.

[18] "The End of Sanctuary in Space." *War Is Boring*, 7 Jan. 2015, https://warisboring.com/the-end-of-sanctuary-in-space/.

[19] Swallow, Edward, and Samuel S Visner. "Space Is Critical - It's Time We Act like IT - via Satellite -." *Via Satellite*, 11 Jan. 2022, https://www.satellitetoday.com/opinion/2022/01/11/space-is-critical-its-time-we-act-like-it/.

[20] Paganini, Pierluigi. "Hacking Satellites ... Look up to the Sky." *Infosec Resources*, 18 Sept. 2013, https://resources.infosecinstitute.com/topic/hacking-satellite-look-up-to-the-sky/.

[21] Scholl, Matthew, and Theresa Suloway. NIST, 2022, *Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)*, https://csrc.nist.gov/publications/detail/nistir/8270/draft. Accessed 1 Mar. 2022.

[22] "Competing in Space." *National Air and Space Intelligence Center*, A Product of the National and Space Intelligence Center, Dec. 2018, https://www.nasic.af.mil/About-Us/Fact-Sheets/Article/1738710/competing-in-space/.

[23] Borowitz, Mariel, et al. *National Security Implications of Emerging Satellite Technologies*. Aug. 2020, https://atlantaglobalstudies.gatech.edu/publications/pub/6674.

[24] Baram, Gil, and Omree Wechsler. "Cyber Threats to Space Systems." *Joint Air Power Competence Centre*, Tel Aviv University, https://www.japcc.org/cyber-threats-to-space-systems.

[25] Scoles, Sarah. "GPS Isn't Very Secure. Here's Why We Need a Backup." *Wired*, Wired, 2 Mar. 2018, https://www.wired.com/story/spoof-jam-destroy-why-we-need-a-backup-for-gps/.

[26] Baksh, Mariam. "Biden Administration Likely Retaining Trump Doctrine on Cybersecurity in Space." *Nextgov.com*, Nextgov, 5 May 2021, https://www.nextgov.com/cybersecurity/2021/05/biden-administration-likely-retaining-trump-doctrine-cybersecurity-space/173840/.

[27] Committee on National Security Systems, 2012, *NATIONAL INFORMATION ASSURANCEPOLICY FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS*, https://www.hsdl.org/?view&did=726945. Accessed 18 Mar. 2022.

[28] The United Nations Treaties on Outer Space. New York: United Nations, 1984.

[29] "Space Policy of the United States." *Wikipedia*, Wikimedia Foundation, 14 Mar. 2022, https://en.wikipedia.org/wiki/Space_policy_of_the_United_States.

[30] Space Domain Mission Assurance: A Resilience Taxonomy: a White Paper.

[31] "Space Segment: Constellation Arrangement." *GPS.gov*, 12 July 2021, https://www.gps.gov/systems/gps/space/.