INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

Risk to Critical Infrastructure

Due to Dependence on Access to Space-based Capabilities

Institute for Homeland Security

Sam Houston State University

Jim Platt

Abstract

This paper is intended for owners and operators of US Critical Infrastructure with core business functions reliant on access to space-based capabilities. While the paper will discuss risk to space assets, the intent is not to address the security and resilience of the space systems, but rather to highlight the risk to space-based assets so that companies choosing to use space-based can make more informed risk-based decisions.

The commercial space industry is in its infancy. The World Economic Forum and McKinsey & Company report projects that the commercial space industry will grow from $630 billion in 2023 to over $1.8 trillion by 2035. Many of the new capabilities will only be feasible because we have access to space. If GPS is an exemplar, space-based capabilities may replace existing terrestrial based systems, the terrestrial based systems they replace will fall into disuse and eventually cease to operate. Each time this occurs, our dependence on access to space will grow.

Space has unique risks such as when systems fail there is no possibility for on-site repair. The Russian attack through the Viasat-KA satellite and the CrowdStrike outage of July 19, 2024 both required on-site repairs. Similar incidents effecting satellites might leave satellites permanently disabled and systems dependent on those satellites requiring significant re-engineering. CISA Director, Jen Easterly, commenting on the CrowdStrike outage stated, “I mean obviously, we want to prevent, but it really is about building resilience into our networks and our systems so that we can withstand significant disruption, at least drive down the recovery time to be able to provide services.” This is especially important for systems reliant on access to space-based systems.

Companies adopting space-based capabilities may assume those who are capable of building and operating satellites are capable of protecting their satellites. Satellite companies face cyber threats like all companies and each company has its own risk profiles. According to a representative from the Office of the National Cyber Directorate, some space operators view cybersecurity as a “drag on operations”.

As the companies adopt space-based capabilities they must conduct effect analysis to not only identify potential benefits but also potential risks. The concepts in Executive Order 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services* should be applied to the use of all space-based capabilities, not just GPS.

About the Author: Jim Platt the founder and president of Strategic Risk Integration (2024). He spent two decades leading risk management programs for the Army and the Cybersecurity and Infrastructure Security Agency. Primary author of DHS report assessing options to offer backup Position, Navigation and Timing (PNT) capabilities provided by GPS. The report led to a shift in national policy with the issuance of EO 13905, Strengthening National Resilience Through Responsible Use of PNT Services. The EO established the shared responsibility of the Federal Government and Operators of Critical Infrastructure to mitigate GPS disruptions.

From 2020 to 2024 led interagency group organized under the White House’s National Science and Technology Council to assess and mitigate risk to critical infrastructure from extreme space weather.

These efforts led to an updated Implementation Plan for mitigating space weather, shifting national efforts from a vulnerability-based approach to a risk-based approach.

He established and led the Space Systems Critical Infrastructure Working Group, the only forum in DHS specifically designed to bring together space systems operators, infrastructure operators and government officials to collaborate on security and resilience issues related to space. Education: BS Management and Computer Science; MA, Leadership, Georgetown University; MBA, Virginia Commonwealth University

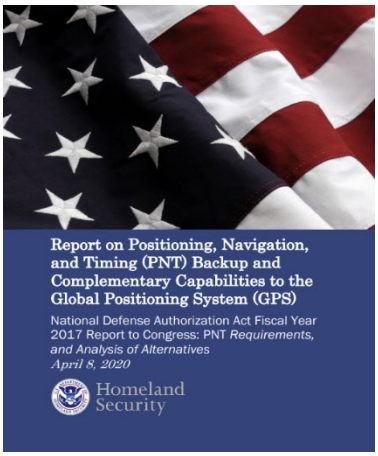
Introduction and Overview:

This paper is intended for owners and operators of US Critical Infrastructure with core business functions reliant on access to space-based capabilities. While the paper will discuss risk to space assets, the intent is not to address the security and resilience of the space systems, but rather to highlight the risk to space-based assets so that companies choosing to use space-based can make more informed risk-based decisions.

Over the past two decades significant attention has been paid to infrastructures growing dependence on the world's best-known space-based capability, the US Global Navigation Space Systems (GNSS) known commonly as GPS. In 2024 there is an estimated 6 billion GPS in the world. Few people and businesses realize how much they rely on GPS, and how much their daily routines and functions would be disrupted if we no longer had access to GPS.

In 2011 the Department of Homeland Security published a National Risk Estimate related to one of the first commercially adopted space systems, GPS. DHS reported that "U.S. Government and private sector experts concluded that portions of the Nation's critical infrastructure are increasingly reliant on GPS and GPS-based services. In the short term, the risk to the nation is assessed to be manageable. However, if not addressed, this threat poses increasing risk to U.S. national, homeland, and economic security over the long term." (Department of Homeland Security, 2015)

The risk associated with dependence was reaffirmed in a 2018 DHS report from the newly formed National Risk Management Center. Two of the key findings from the report were:



- The critical infrastructure sectors heavily reliant on PNT (meaning disruption would cause significant costs, delays, or degradation of functions and service) include communications, information technology, transportation, emergency services, energy, surveying and mapping, and financial services.
- Critical infrastructure systems that would cease to operate due to GPS disruptions will do so because of design choices associated with a lack of information, cost, efficiency, and other considerations—not because of a lack of available options. In other words, business decisions, the lack of a federal mandate, and potentially an underappreciation of the risk associated with GPS dependence are factors in the lack of resilience to GPS disruption.

Challenges of adopting non-space-based systems as highlighted in the DHS report may provide insight into the future. As we adopt space-based capabilities, will industry be willing to fund terrestrial capabilities that provide less efficient products in the name of resilience?

Two years later, on December 9, 2021, during a meeting of the Space-based Position, Navigation and Timing National Advisory Board (PNTAB), Caitlin Durkovich, National Security Council Director for Response and Resilience stated that GPS was still a significant single point of failure in our country. (Space-Based Positioning, Navigation and Timing Advisory Board, 2022, pp. 24-28)

Operating from space, GPS has proven to be so efficient and effective that providing backup capabilities has proven extremely difficult. On December 15, 2004, President Bush signed National Presidential Security Memorandum-39 (NSPD-39)*, U.S. Space-Based Position, Navigation, and Timing Policy*. NSPD-39 directed the Secretary of Transportation to "In coordination with the Secretary of Homeland Security, develop, acquire, operate, and maintain backup position, navigation, and timing capabilities that can support critical transportation, homeland security, and other critical civil and commercial infrastructure applications within the United States…" (Bush Whitehouse, 2004) Almost two decades later, there are no definitive plans to provide backup capabilities for GPS. In fact, we are more dependent today than at any time in the past, and with each passing day, we are becoming more dependent.

GPS is an example of how a few assets in space can provide services to users around the world. With just 24 satellites GPS is able to provide 24/7/365 service to an unlimited number of users around the world. (US Space Operations Command, 2023). When first GPS Satellite was launched in February 1978 (US Coast Guard Navigation Center, 1995), launching and maintaining space systems was the purview of just a few governments.

Over the past decade technological advances have driven down the cost of placing satellites in orbit. Space is no longer the primary purview of nations. Now private companies are designing, launching and operating satellites delivering services direct to consumers and spawning new industries worth billions. How much economic benefits will the space industry bring? The World Economic Forum and McKinsey & Company report Space: *The $1.8 Trillion Opportunity for Global Economic Growth* (World Economic Forum, 2024) projects that the commercial space industry will grow from $630 billion in 2023 to over $1.8 trillion by 2035. Many of the new capabilities will only be feasible because we have access to space. If GPS is an exemplar, space-based capabilities may replace existing terrestrial based systems, the terrestrial based systems will fall into disuse and eventually cease to operate. Each time this occurs, our dependence on access to space will grow.

Reliance on space-based capabilities is already a reality. In 2023 the Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center (NRMC) highlighted that all sixteen Critical Infrastructure Sectors in the United States and all 55 National Critical Functions (NCF) had some level of dependency on space-based capabilities. The NRMC defines NCFs as "functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." (Cybersecurity and Infrastraucture Security Agency, 2019). Put simply, all of the infrastructure and the functions that they provide to the US citizens can be impacted by the loss of access to space-based capabilities.

Too often the focus regarding space-based capabilities is on the space craft themselves. These vehicles and the systems that keep them operating are technological marvels. While the construction and operation of spacecraft are big business, the economic benefit they drive dwarf the cost to build and operate the system. The US government's budget for GPS in 2023 was just over $1.83 billion dollars. (National Space-Based Coordination Office, 2022). This funding went to a relatively small group of companies who provide the needed technical expertise to operate GPS and enhance its capabilities.

By far the greatest economic impact greater impact comes from the use of the GPS signals by billions of users around the world, not the building and operation of the satellites. There have been

numerous attempts to quantify the economic impacts of GPS. In June of 2019 the Department of Commerce released a report prepared by RTI International. *Economic Benefits of the Global Positioning System.* Figure 1 summarizes their findings related to economic benefits of GPS for the Private Sector. (RTI International, 2019, pp. ES-2)

Table ES-1. Summary Economic Benefits of GPS for Private-Sector Use, 1984 to 2017

Sector	Specific Analytical Focus	Benefits ($ million)
Agriculture	Precision agriculture technologies and practices	$5,830
Electricity	Electrical system reliability and efficiency	$15,730
Location-based services	Smartphone apps and consumer devices that use location services to deliver services and experiences	$215,702
Mining	Efficiency gains, cost reductions, and increased accuracy	$12,350
Maritime	Navigation, port operations, fishing, and recreational boating	Negligible
Oil and gas	Positioning for offshore drilling and exploration	$45,922
Surveying	Productivity gains, cost reductions, and increased accuracy in professional surveying	$48,124
Telecommunications	Improved reliability and bandwidth utilization for wireless networks	$685,990
Telematics	Efficiency gains, cost reductions, and environmental benefits through improved vehicle dispatch and navigation	$325,182
Total		**$1,354,830**

The United States Department of Commerce estimated $1 billion / day to the US economy. The United Kingdom estimated 1 billion British Pounds per day to its economy. Just two of the worlds' economies would experience billions of dollars of impact per day if GPS were lost. Considering GPS is a global utility we would expect many billions of dollars of loss per day should GPS be disrupted.

In 2020 the United States issued Executive Order 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services.* EO 13905 was a bold step forward. The EO recognized that GPS could be disrupted and placed users of GPS on notice that they bore a responsibility to ensure their operations could continue should GPS be disrupted.

A year later the Trump Administration issued NSPD-7 to replace NSPD-39. This regulation generally left the requirements to build a backup in place, though little progress has actually been made towards fielding other systems. The policy reenforced user's responsibilities to prepare for and manage disruptions to PNT services but it also cautioned users to consider the risks of using other PNT systems. "However, the United States Government does not assure the reliability or authenticity of foreign PNT services. Although foreign space-based PNT services may be used to complement civil GPS service, receiver manufacturers should continue to improve security, integrity, and resilience in the face of growing cyber threats."

Problem Statement

Why was such a drastic step needed? Shouldn't all business be prepared for loss of a key business input? We will explore these questions and draw potential parallels to the emerging space economy?

Philosopher George Santayan is credited with the saying "Those who cannot remember the past are condemned to repeat it." Over the past three decades US and global infrastructure has become dependent on a single space-based system, GPS. GPS has been adopted and integrated into every critical infrastructure sector. Despite known vulnerabilities in the GPS signal and warnings by the US

Government that GPS could be lost, many critical infrastructure systems will be degraded or disrupted if access to GPS is interrupted.

The commercial space race is in full gear. Companies are building spacecraft to deliver services that are more efficient than those delivered by terrestrial means, and they will also deliver new capabilities that will enhance our way of life. Given the unique nature of space-based capabilities, will US infrastructure find itself similarly dependent on these space-based capabilities as we are on GPS? Can industries prepare for short term disruptions to space-based capabilities as the nation assesses long term risk?

Discussion

Experience has shown that to effectively manage risk you must define the problem. Failing to effectively define the problem can, and often does, lead to ineffective mitigations and the unnecessary expenditure of resources. Rather than a broad statement of loss of space-based capabilities, which does little to help users manage risk, we will focus on two scenarios.

- The space system is functioning normally, but the user cannot receive or process the signal
- The space system is no longer functioning

Scenario 1: The space system is functioning normally, but the user cannot receive or process the signal

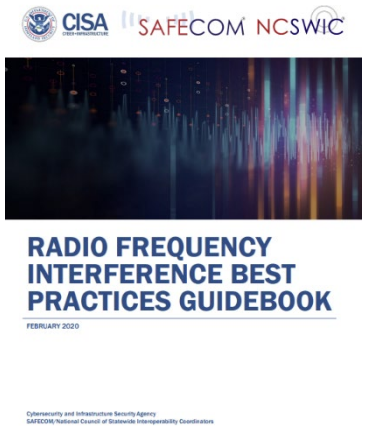
On February 24, 2022 Russia invaded Ukraine. In the early stages of the invasion the Russian's launched a cyber-attack through the ViaSat KA-SAT satellite disabling SATCOM modems in tens of thousands of critical infrastructure systems across Europe. No longer able to communicate with control centers, many critical infrastructure assets went offline. Since many of these systems' sole means of communication was through space, they would remain offline until on-site repairs were carried out. Similar to the findings from the 2018 DHS report on GPS. Technology existed to mitigate the loss of communications, but companies chose not to do so. Infrastructure companies chose Satellite based communications because other forms of communication were either unavailable or not economically feasible. In many cases the sole means of communication with these assets was through the ViaSat satellite. Once these communication channels were disabled, on site repair and mitigation was the only option.

The most notable and widely publicized impact was the disruption of power generation in Germany. Thousands of wind turbines went offline until communications could be reestablished. In many cases this meant dispatching crews to each site to conduct onsite repairs or replace modems. (O'Neill, 2022) On March 30, 2024, ViaSat announce that it had shipped nearly 30,000 modems to enable users to come back online. With nearly 30,000 assets impacted, full restoration was both time and resource intensive.

While the effects were felt across Europe the 30,000 modems only represented one segment of the total number of customers serviced by ViaSat. In the March 30 statement ViaSat report "This incident was localized to a single consumer-oriented partition…. The residential broadband modems affected use the "Tooway" service brand." (Viasat Inc, 2022) This incident demonstrates the potential impact that a single segment of a satellite can have on critical infrastructure.

Key points for industry to consider

- Enterprise Risk Management (ERM*)* Industries and companies with space-based dependencies should include this risk in their (ERM) process.
- Identify critical space-based dependencies. Are critical functions within the business enterprise dependent on access to space-based systems? In the case of the Russian attack, clearly wind turbines were dependent on space-based communications. Approximately 5,800 wind turbines went offline effecting over 10GW of power generation. (Cyber Peace Institute, 2022). Priority for restoring critical capabilities should be specified in service level agreements with the service provider. As reported Viasat shipped nearly 30,000 modems to companies in the month after the incident. Companies such as that provide critical services, such as energy, should ensure their service level agreements give them priority for support, such as receiving modems.
- Develop PACE plans for critical communications. Are Primary, Alternate, Contingency, and Emergency (PACE) plans available for critical communications, including space-based/enabled communications? For critical business and safety of life operations companies should plan for multiple modes of communication. In the case of space-based communications options may be limited as space-based communications are often used when alternate less expensive modes are not available. Discussion of a PACE plan can be found at the DHS website for emergency communications.



https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf. While this guidebook is specifically targeted to public safety entities and deals with radio frequency interference, its basic principles are applicable to any company that relies on communications for core business functions.

- Assess effectiveness of mitigations. Assess and document how systems will respond to disruption of space-based communications (Egan, 2022). Not all systems cease to function when communications are lost. In 2022 GPS was jammed in the Denver area for approximately 33 hours. Systems in and around the Denver airport could not receive the GPS signal. GPS not only provides location, but it also provides a highly accurate timing signal used by communications and IT networks to synchronize geographically dispersed nodes. The DHS report on the incident stated "No accidents or injuries occurred because of the GPS interference incident. However, several critical infrastructure sectors were degraded. Many systems that detected the event had resilient alternate timing built in for backup or fail-over timing and experienced minor or no degradation of services." This highlights that with proper planning users can mitigate, to some extent, the temporary loss of communication with space systems. The full report can be found at https://www.cisa.gov/sites/default/files/2023-02/CISA-Insights_GPS-Interference_508.pdf.
- Establish fault validation and recovery procedures. Are there procedures in place to validate the fault to ensure proper mitigation actions are employed? Communications with satellites can be disrupted for numerous reasons: faulty equipment, signal jamming or atmospheric interference,

to name a few. In the case of the Denver incident there were reports of operators replacing GPS receivers assuming the receiver was at fault when in fact the root was jamming. Operators should work with their service providers to ensure they understand fault detection procedures so they can expedite restoration of normal operations.

On the negative side. However, like mitigations against the loss of GPS, both the government and industry may be unwilling to incur the expense to mitigate disruption. Companies usually choose space-based communications because there are no other communication channels available,

Scenario 2: Long Term loss of space systems

As mentioned in the introduction the global space economy is expected to grow to $1.8 trillion by 2035. Users around the world will connect to Satellites in Low Earth Orbit on a routine basis and in many cases will not even know that their communications are being routed through space satellites.

It will not just be commercial entities that are benefiting from the expansion of space-based capabilities. Countries around the world see both the economic and military value of space. According to Maj. Gen. Judd Blaisdell, the Air Force's director of space operations and integration "Space is the ultimate high ground and gives American forces a tremendous advantage on the battlefield…We must dominate space, because it would be very difficult to conduct a war without our space assets and the capabilities they provide."

In the 20th Century space was the purview of nation states. Only nations could afford the huge expenses of developing and deploying spacecraft. Space companies we reliant on defense and other government contracts to operate. Over the past decade this dynamic has changed. Commercial entities see the value in space and are developing capabilities at a pace never attainable under the government procurement systems. Now major government agencies, such as the Department of Defense, are actively seeking to adopt commercial space systems rather than relying on bespoke, DoD Specific Capabilities. (Department of Defense, 2024)

The Department of Defense recognizes that use of commercial space systems may create risk to those space systems. According to the 2024 DoD Commercial Space Strategy, DoD is assessing extending financial protection to "commercial entities employing solutions in support of military operation." (Department of Defense, 2024, p. 4) If enacted, will the protection extend to users of those systems or only the system providers.

The military use of commercial space systems may increase risk to US critical infrastructure. Should a major conflict arise, will our adversaries be able, or even willing to discriminate between satellites supporting the military and those operated or used by the military. Indications are that they may not be so inclined. On March 1, 2024, Assistant Secretary of Defense for Space Policy John F. Plumb testified to the House Armed Services Committee that Russia was developing a nuclear counter-space technology. He stated that most satellites (especially those in low earth orbit (LEO)) aren't hardened against a nuclear detonation, making them especially vulnerable to damage. While the effects of a nuclear detonation in space could vary based on factors like the detonation type and location, satellites in the blast zone would likely be destroyed. He also suggested a sufficiently powerful nuclear detonation in the right location **could render LEO unusable for up to a year.**

It is not only the US that has concerns about nuclear weapons in space. Maj. Gen. Michael Traut, head of German Space Command, stated at the 2024 Munich Security Conference that "if somebody dares to explode a nuclear weapon in high atmosphere or even space, this would be more or less the end of the usability of that global commons."

It is not just nuclear attacks that can impact satellites. The US Government has significant concerns regarding cybersecurity of space systems. In 2023 The Office of National Cyber Directorate (ONCD) from the White House conducted listening sessions with space industry leaders to sense the state of cybersecurity in the space industry. On June 6, 2023, Nicholas Leiserson, assistant National Cyber Director for Cyber Policy and Programs in the Office of the National Cyber Director, provided a summary of the listening sessions at CyberSatGov.

Mr. Leiserson reported that "there is a lack of expertise at the intersection of aerospace and computer engineering and cybersecurity. Cyber experts for space systems are like "unicorns."" In addition, he indicated that "(Space System) Operators can see cybersecurity as a drag, and something that slows missions down or takes up precious power and bandwidth…" Will the lack of cyber-security/aerospace "unicorns" and a culture that sees cybersecurity as a "drag on operations" create unrealized risk for critical infrastructure operators who are depending on space-systems to support essential functions? A more detailed summary of the Mr. Leiserson comments can be found at https://www.satellitetoday.com/government-military/2023/11/06/oncd-assistant-director-says-white-house-is-incentivizing-long-term-space-cybersecurity-investments/

The CrowdStrike incident of July 19, 2024, would have been significantly worse if the error impacted satellites. An error in software update impacted over 8.5 million computers worldwide and caused over $5 billion in direct losses to fortune 500 companies (Lyngaas, 2024). Whiles some companies were able to recover in a few days, for others it took over a month to fully recover as IT personnel needed to physically access to computers to bypass the "Blue Screen of Death".

If a similar event affected space systems, our ability to recover those systems is questionable. Currently, there are no onsite maintenance capabilities for satellites and even if they existed, the time required to access satellites would be extensive and expensive. This is why critical infrastructure operators must be resilient and not just hope that space systems are protected and won't be disrupted. In August the Director of CISA, Jen Easterly stated at Blackhat "I mean obviously, we want to prevent, but it really is about building resilience into our networks and our systems so that we can withstand significant disruption, at least drive down the recovery time to be able to provide services." These comments are directly applicable to critical infrastructure systems reliant on access to space.

Way Forward

Critical Infrastructure Operators

- **Identify the use of space-based capabilities and assess risk.** Organizations have already adopted satellite based SCADA system to control remote assets where terrestrial broadband is not available. The risk here is relatively easy to identify and assess. As more space-based capabilities come online and become common place their use may be overlooked, and the risk underappreciated. Risk assessments for critical systems, networks and assets should include an evaluation of space dependencies and associated risks.

- **Don't assume Space Systems are Secure and Resilient:** Space is a harsh operating environment, and the commercial space industry is in its early stages. Companies seeking to provide space-based services are in a race to be the first providers for a particular service. To achieve this, they may or may not place a high priority on security and resilience of their space system. As the US government has stated, some space operators view cybersecurity as a "drag on operations".
- **Design Critical Infrastructure systems to manage the temporary disruption of space-based systems.** There are many threats and hazards to space systems. Solar flares, radiation, atmospheric disturbances, cyber-attacks, equipment malfunctions, operator error and geopolitical threats. Critical Infrastructure system should be designed to degrade gracefully when access to space system is compromised.
- **Understand risk to space systems.** Establish information sharing relationships to understand risks to space systems. Companies should work through industry trade organizations or their Critical Infrastructure Information Sharing and Analysis Center (ISAC) to receive threat updates from the Space ISAC and CISA. Companies with high dependence on space should apply to join the Space ISAC.
- **Include risk to space in all hazards planning**. If space is critical to your operations conduct the same level of risk assessment as you would any other critical input (power, communications, water, etc.). Critical reliance on space-based systems must be included in your Enterprise Risk Management Plan and risk should be mitigated to acceptable levels based on corporate risk tolerance.

State Governments

- **Plan for Disruption of Space-based capabilities.** States plan for a myriad of threats and hazards and are best situated to understand the essential services needed by their residence. States should assess which critical systems cannot operate when there is wide-spread disruption of space-based systems. The Russian attack through the ViaSat system could serve as an initial planning scenario. If this situation happened in the US, which companies would have had priority for receiving new modems from ViaSat? Are there plans to coordinate prioritization at a national level to avoid the situation in COVID where states were bidding against other states for supplies?

Federal Government

- **Monitor for unacceptable concentration of risk in space-based systems**. GPS is a single point of failure for the US and many countries because it is efficient and cost effective. GPS enabled the US and other governments to discontinue other PNT services. Because space assets can provide ubiquitous coverage across the US and the globe they will create economies of scale. The reduced cost created by the economies of scale and the benefit of having operational systems in approved orbits and access to finite frequencies may limit the ability of other systems to compete effectively creating a single point of failure in a company.
- **Develop national response plans to address the loss of critical space-based capabilities.** A new model for responding to loss of space-based capabilities may be needed. With natural disasters such as hurricanes, there are well established procedures to flow in resources to restore critical services in the impacted areas, power lines are restrung, data centers reroute traffic, damaged hardware is replaced, and cellular networks are brought in on trailers. If space is lost, restoration

may be impossible for years. There are no stockpiles of satellites. There are limited launch capabilities and existing satellites would now be space debris and would need to be removed before new satellites are placed in orbit. There are no capabilities to remove space debris at scale. When space is no longer available, governments and companies will need to revert to terrestrial systems.

- There is no question that space-based systems provide capabilities that enhance our way of life. Satellites improve our ability to communicate, increase agricultural production, forecast weather and many other functions that we rely on to operate our society. The incremental adoption of space-based capabilities and the ubiquitous access to products enabled by space through cell phones may create a false sense of security related to the difficulty of operating in space and the potential risk.

As the companies adopt space-based capabilities they must conduct effect analysis to not only identify potential benefits but also potential risks. The concepts in Executive Order 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services should be applied to the use of all space-based capabilities,* not just GPS.

References

Bush Whitehouse. (2004, Dec 15). *U.S. Space-Based Positioning, Navigation, and Timing Policy, Fact Sheet.* Retrieved Jul 30, 2024, from GPS.GOV: https://www.gps.gov/policy/docs/2004/

Cyber Peace Institute. (2022, Jun). Retrieved from Case Study - Viasat: https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

Cybersecurity and Infrastraucture Security Agency. (2019, Apr 01). *National Critical Functions*. Retrieved Jun 15, 2024, from National Critical Functions Set: https://www.cisa.gov/national-critical-functions-set

Department of Defense. (2024). *2024 DOD COMMERCIAL SPACE INTEGRATION STRATEGY.* Washington, DC: Department of Defense. Retrieved from https://media.defense.gov/2024/Apr/02/2003427610/-1/-1/1/2024-DOD-COMMERCIAL-SPACE-INTEGRATION-STRATEGY.PDF

Department of Homeland Security. (2015, Nov 30). *Resilient Navigation and Timing Foundation.* Retrieved Jul 14, 2024, from RNT.ORG: https://rntfnd.org/wp-content/uploads/DHS-National-Risk-Estimate-GPS-Disruptions.pdf

Egan, M. (2022). *A Retrospective on 2022 Cyber Incidents in the Wind Energy.* Boise State University: A Retrospective on 2022 Cyber Incidents in the Wind Energy. Retrieved Aug 1, 2024, from https://scholarworks.boisestate.edu/cgi/viewcontent.cgi?article=1002&context=cyber_gradproj

Lyngaas, S. (2024, Jul 24). *We finally know what caused the global tech outage - and how much it cost*. Retrieved Aug 15, 2024, from CNN.com: https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html

National Space-Based Coordination Office. (2022, April 22). *Fiscal Year 2023 Program Funding*. Retrieved Aug 01, 2024, from GPS.GOV: https://www.gps.gov/policy/funding/2023/

O'Neill, P. H. (2022, May 10). *Russia hacked an American satellite company one hour before the Ukraine invasion*. Retrieved Aug 14, 2024, from MIT Technical Review: https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/

RTI International. (2019, Jun 06). *New Report Reveals Economic Benefits from Private Sector Use of GPS.* Retrieved from RTI International: https://www.rti.org/sites/default/files/gps_finalreport618.pdf?utm_campaign=SSES_SSES_ALL_Aware2019&utm_source=Press%20Release&utm_medium=Website&utm_content=GPSreport

Space-Based Positioning, Navigation and Timing Advisory Board. (2022, Apr 20). *National Space-Based Positioning, Navigation, and Timing Advisory Board.* Retrieved Jul 11, 2024, from GPS.GOV: https://www.gps.gov/governance/advisory/meetings/2021-12/minutes.pdf

Statista. (2023, Jan 27). *Statista*. Retrieved Jun 14, 2024, from Subscribers in the direct satellite-to-device market worldwide from 2020 to 2030: https://www-statista-

com.ezproxy.shsu.edu/statistics/1362432/direct-satellite-to-device-market-subscribers-worldwide/

US Coast Guard Navigation Center. (1995, Jul 15). *US Coast Guard Navigation Center.* Retrieved Aug 5, 2024, from GPS Constellation: https://www.navcen.uscg.gov/sites/default/files/pdf/gps/geninfo/FOC-1995.rtf

US Space Operations Command. (2023, Feb 28). *Global Positioning System*. Retrieved Aug 13, 2024, from Space Operations Command, Space Force: https://www.spoc.spaceforce.mil/About-Us/Fact-Sheets/Display/Article/2381726/global-positioning-system

Viasat Inc. (2022, Mar 30). *KA-SAT Network cyber attack overview*. Retrieved from Viasat.com: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

World Economic Forum. (2024, Apr 8). *Space: The $1.8 Trillion Opportunity for Global Economic Growth.* Retrieved Jul 25, 2024, from World Economic Forum: https://www3.weforum.org/docs/WEF_Space_2024.pdf

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Platt, Jim. (2024). Risk to Critical Infrastructure Due to Dependence on Access to Space-Based Capabilities (Report No. IHS/CR-2024-1032). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/VXF8Y