NATIONAL SECURITY SPACE ASSOCIATION

NATIONAL SECURITY SPACE ASSOCIATION
MOORMAN CENTER FOR SPACE STUDIES

America's Asymmetric Vulnerability to Navigation Warfare: Leadership and Strategic Direction Needed to Mitigate Significant Threats

Marc J. Berkowitz

July 18, 2024

Executive Summary

The U.S. Global Positioning System (GPS) provides continuous positioning, navigation, and timing (PNT) services to civil, commercial, and national security users throughout the world. GPS is a global utility integral to economic development and growth, transportation safety, critical infrastructures, and U.S. and international security.

Unfortunately, GPS has been surpassed as the premier space-based PNT system in the world and is vulnerable to a variety of threats. Further, the United States does not have a reliable and resilient terrestrial backup to GPS, while China, Russia, and other nations do have backups for PNT services.

This paper examines America's asymmetric vulnerability to navigation warfare (Navwar) as well as provides actionable recommendations to mitigate such vulnerabilities and reestablish U.S. leadership in space-based and terrestrial PNT. The following is a summary of its key findings and recommendations:

- While several U.S. presidents have issued policy guidance regarding PNT management, programs, and activities and the U.S. Congress has enacted statutes codifying aspects of policy into law, little progress has been made on their implementation.

- Despite ongoing GPS modernization activities and augmentation systems, there are numerous shortfalls in U.S. PNT capabilities. Such shortfalls involve system performance, survivability, and resilience.

- GPS is essential to America's society, economy, and security. It is relied upon by all sixteen critical infrastructure sectors and enables Americans' way of life. The economic value of GPS to the nation is trillions of dollars and the impact of its disruption or loss is incalculable.

- GPS is a lynchpin of space-enabled, precision strike warfare and contributes to making space power the leading-edge of U.S. information-age military power.

- Navwar operations against the system could have significant consequences for all elements of U.S. national power with severe political, socioeconomic, and security impacts upon the nation's status, influence, prosperity, and security. Significant disruption or loss of PNT services would be a catastrophe.

- Russia and China are acquiring or operating various cyber, electronic warfare (EW), kinetic energy, directed energy, nuclear, and orbital ASAT or counterspace weapons systems. Iran and North Korea operate cyber, EW, and missile capabilities which can interfere with space assets and operations. All four nations have conducted Navwar operations against GPS.

- GPS was designed for survivability, endurance, and operational continuity. It is among the most resilient U.S. national security space systems. Nonetheless, GPS is not necessarily survivable against all dangers.

- There are numerous potential approaches to improve the resilience of U.S. PNT services. While many are being evaluated by the federal government, the United States still does not operate a resilient and reliable alternative PNT service.

- Unmitigated GPS vulnerabilities could result in potentially profound domestic and international implications if exploited by an adversary (or adversaries). Critical infrastructures, national essential functions, and military forces could be at grave risk.

The United States must rapidly develop and implement a comprehensive, whole of nation, strategy to redress its asymmetric vulnerability to Navwar and restore U.S. leadership in space-based and terrestrial PNT. To achieve those objectives, the President should promulgate a national PNT strategy and

implementation plan which urgently directs the following courses of action and Congress should provide adequate resources for the plan's execution:

- The Department of Defense (DoD), Department of Homeland Security (DHS), and Department of Transportation (DoT) should continue to resource the identification and assessment of GPS dependencies, interdependencies, and vulnerabilities in collaboration with the national security, homeland security, and transportation, maritime, and aviation safety industrial bases.

- DoT should resource the development, procurement, fielding, operation, and sustainment of modern, secure, and robust civilian GPS signals.

- DHS, DoT, and the Department of Commerce (DoC), in consultation with the Federal Communications Commission, the Federal Energy Regulatory Commission, and the private sector, should develop regulatory requirements and financial incentives for critical infrastructure owners and operators to employ more than a single source of precise PNT, user equipment (UE) which are resistant to interference, and the capability to sustain normal operations for at least thirty days in the event of an extended space-based PNT service disruption.

- The Department of State (DoS) and DoC should reform export control regulations to allow U.S. firms to sell adaptive antenna technology.

- DoD should urgently resource and accelerate the acquisition, deployment, operation, and sustainment of cyber and radiation hardened GPS IIIF or other spacecraft with higher power, reprogrammable digital payloads, and M-code signals to rapidly improve the GPS constellation's resilience, direct measures to accelerate and complete the OCX program, rapidly deploy and integrate multi-GNSS UE into U.S. force structure, and synchronize GPS segments.

- DoD should resource the development, procurement, deployment, operation, and sustainment of a dynamic, layered, space defense-in-depth with a mix of passive and active measures to counter adversary ASAT and counterspace weapons systems.

- DoS, DoD, and DoT should pursue international cooperation with Europe, Australia, Japan, and India to establish compatible, interoperable, and trusted GNSS services.

- DoT, DHS, and DoC should work with the private sector to develop, field, operate, and sustain multiple complementary terrestrial PNT services. The first step, which should be achieved as soon as possible, is the acquisition of such services to protect federal systems and applications.

Focused leadership, properly empowered and resourced, is essential to the national PNT strategy's success.

Introduction

The U.S. Global Positioning System (GPS) provides continuous positioning, navigation, and timing (PNT) services to civil, commercial, and national security users throughout the world. After being launched in 1978, it set the international standard for Global Navigation Satellite System (GNSS) services and reinforced the United States' standing as the world's leading spacefaring nation. The system enables an unlimited number of users with civilian or military GPS receivers to determine their three-dimensional position, velocity, and time 24 hours a day, in all weather, with a precise and accurate common reference grid.

Unfortunately, GPS has been surpassed as the premier space-based PNT system in the world. Both the People's Republic of China's Beidou and European Union's Galileo satellite navigation systems are more accurate and/or provide better coverage in parts of the world than GPS. Indeed, the U.S. National Space-based Positioning, Navigation, and Timing Advisory Board warned last year that "GPS's capabilities are now substantially inferior to those of China's Beidou."[1] China's system, for example, has a larger satellite constellation, more ground antennas, signal post-processing, and a text messaging service for communications which makes it better than GPS, Galileo, and Russia's GLONASS satellite navigation system.[2]

Moreover, GPS is vulnerable to a variety of threats. Foreign powers have anti-satellite (ASAT) or counterspace, electronic warfare (EW), and cyber weapons for navigation warfare (Navwar). The system may also be vulnerable to severe solar weather, such as coronal mass ejections, as well as wide area and localized EW jamming and spoofing by non-state actors (e.g., terrorist groups, transnational criminal organizations), and cyber-attacks by hackers. While the system has many resilience features, neither the U.S. public nor private sectors have mitigated all its vulnerabilities. Further, the United States does not have a reliable and resilient terrestrial backup to GPS, while China, Russia, and other nations do have backups for GNSS services.[3]

Consequently, U.S. critical infrastructures, national essential functions, and military forces would be at grave risk if GPS services were interrupted or lost. The domestic and global consequences of such an event would be profound. This paper examines America's asymmetric vulnerability to Navwar. First, it summarizes U.S. policy, guidance, and law on PNT, describes GPS and discusses its utility. Next it examines current and emerging threats to GPS, the system's resilience, and the potential implications of interference with its PNT services. Finally, it provides actionable recommendations to mitigate vulnerabilities to Navwar threats and reestablish U.S. leadership in space-based and terrestrial PNT.

Policy, Guidance, and Law

Since the 1980s, several U.S. Presidents have issued policy guidance regarding PNT management, programs, and activities. The U.S. Congress has also enacted statutes codifying aspects of policy into law. The Presidential directives and statutes have been consistent over time while also evolving to address changes in the domestic and international environments. This includes guidance for the United States to maintain its leadership in the service, provision, and use of GNSS, encourage worldwide use of GPS for peaceful purposes,

---

[1] "Summary Report of the 27th National Space-Based PNT Advisory Board Meeting," November 16-17, 2022 https://www.gps.gov/governance/advisory/recommendations/2023-01-PNTAB-27-chair-memo.pdf

[2] See, for example, Jesse Khalil, "China's BeiDou Challenges US GPS Dominance, GPS World, October 26, 2023, https://www.gpsworld.com/chinas-beidou-challenges-u-s-gps-dominance/#:~:text=The%20BeiDou%20constellation%20is%20newer,places%2C%20including%20the%20developing%20world; and David H. Millner, et. al., "BeiDou: China's GPS Challenger Takes Its Place on the World Stage," Joint Forces Quarterly, 105, April 14, 2022, https://ndupress.ndu.edu/Media/News/News-Article-View/article/2999161/beidou-chinas-gps-challenger-takes-its-place-on-the-world-stage/

[3] Salem Gebrekidam, et. al., "One Satellite Signal Rules Modern Life. What Happens if Someone Knocks it Out?" The New York Times, March 28, 2024, https://www.nytimes.com/2024/03/28/world/asia/as-threats-in-space-mount-us-lags-in-protecting-key-services.html; and Mitch Narins, "The Global Loran / eLoran Infrastructure Evolution," Presentation to the Space-based PNT Advisory Board, June 3, 2014), https://www.gps.gov/governance/advisory/meetings/2014-06/narins.pdf

engage other nations providing space-based PNT services to ensure compatibility with GPS, promote transparency in the provision of civilian services, and enable market access to U.S. industry.[4]

Following the Soviet Union's downing of Korean Airlines flight 007, which had flown off course while enroute from Anchorage, Alaska to Seoul, South Korea, in 1983, **President Reagan directed the U.S. government to "provide continuous civilian access to GPS, free of direct user fees."**[5] This subsequently became domestic law in 1998.[6] In conjunction with guidance to provide free access to information for the development of user equipment (UE) and a record of reliable service, the free-to-the-user policy for civil, commercial, and scientific purposes spurred investment and innovation in GPS technology as well as widespread use of the system for myriad civilian applications.

In 1996, **President Clinton issued a directive stating the intention to "discontinue the use of GPS selective availability (SA**)," i.e., the technique for deliberate degradation of the GPS civilian signal's accuracy, "within a decade in a manner that allows adequate time and resources for our military forces to prepare fully for operations without SA."[7] In recognition of the system's increased importance to civil and commercial users, President Clinton later directed that SA be turned to zero in 2000.[8] To mitigate potential risks of expanded access to the dual (civilian and military) uses of the system, he directed development of "measures to prevent the hostile use of GPS and its augmentations to ensure that the United States retains a military advantage without unduly disrupting or degrading civilian uses."[9]

Following the 9/11 terrorist attacks on the United States, President George W. Bush promulgated policy guidance in 2004 which recognized that the continued growth of GPS-related services "presents opportunities, risks, and threats to U.S. national, homeland, and economic security."[10] Consequently, he directed the improvement of "capabilities to deny hostile use of any space-based positioning, navigation, and timing services, without unduly disrupting civil and commercial access to civil positioning, navigation, and timing services outside an area of military operations, or for homeland security purposes."[11] Additionally, **President Bush directed the Secretary of Transportation, in coordination with the Secretary of Homeland Security, to:**

> **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, in the event of a disruption of the Global Positioning System or other space-based positioning, navigation, and timing services.**

In 2010, **President Obama directed investment in "domestic capabilities and support of international activities to detect, mitigate, and increase resiliency to harmful interference to GPS, and**

---

[4] Space Policy Directive 7, "The United States Space-Based Positioning, Navigation, and Timing Policy," The White House, January 15, 2021, https://www.gps.gov/policy/docs/2021/

[5] "Statement by Deputy Press Secretary Speakes on the Soviet Attack on a Korean Civilian Airliner," The White House, September 16, 1983, https://www.reaganlibrary.gov/archives/speech/statement-deputy-press-secretary-speakes-soviet-attack-korean-civilian-airliner-1

[6] 10 U.S.C. § 2281, National Defense Authorization Act for FY 1998, "Global Positioning System," https://www.govinfo.gov/content/pkg/PLAW-105publ85/pdf/PLAW-105publ85.pdf#page=279

[7] Presidential Decision Directive/National Science and Technology Council 6, "U.S. Global Positioning System Policy," The White House, March 28, 1996, https://clintonwhitehouse3.archives.gov/WH/EOP/OSTP/NSTC/html/pdd6.html

[8] "Statement by the President Regarding the United States' Decision to Stop Degrading Global Positioning System Accuracy," The White House, May 1, 2000, https://clintonwhitehouse3.archives.gov/WH/EOP/OSTP/html/0053_2.html

[9] "U.S. Global Positioning System Policy."

[10] "U.S. Space-Based Positioning, Navigation, and Timing Policy," Fact Sheet, The White House, December 15, 2004, https://www.gps.gov/policy/docs/2004/#:~:text=The%20President%20authorized%20a%20new,%2C%20scientific%2C%20and%20commercial%20purposes.

[11] Ibid.

identify and implement, as necessary and appropriate, redundant and back-up systems or approaches for critical infrastructure, key resources, and mission-essential functions."[12] In 2018, **Congress passed the National Timing Resilience and Security Act directing the Department of Transportation (DoT) to build a "land-based, resilient, and reliable alternative timing system" by 2020**.[13]

"Long-standing lack of progress on issues important to U.S. national, homeland, and economic security."

Additionally, **current policy guidance, issued by President Trump in a series of executive orders and directives in 2020 and 2021, focused on mitigating PNT-related risks and threats to U.S. national, homeland, and economic security**.[14] This includes direction to:

- Develop and operate GPS and its supporting infrastructure, including software, using risk-based, cybersecurity-informed engineering to mitigate evolving malicious cyber activities that could manipulate, deny, degrade, disrupt, destroy, surveil, or eavesdrop on space system operations as well as maintain an effective and resilient cyber survivability posture throughout the space system lifecycle;
- Improve the performance of United States space-based PNT services, including developing more robust signals that are more resistant to disruptions and manipulations consistent with United States and allied national security, homeland security, and civil purposes.
- Improve the cyber security of GPS augmentations as well as federally owned GPS-enabled devices, and foster commercial space sector adoption of cyber-secure GPS-enabled systems;
- Allow continued use of allied and other trusted international PNT services in conjunction with GPS to enhance the resilience of PNT services;
- Invest in domestic capabilities and support international activities to detect, analyze, mitigate, and increase resilience to harmful interference with GNSS;
- Identify and implement, as appropriate, alternative sources of PNT for critical infrastructure, key resources, and mission-essential functions;
- Promote the responsible use of U.S. space-based PNT services and capabilities in the civil and commercial sectors including the utilization of multiple and diverse complementary PNT systems or approaches for national critical functions to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of U.S. critical infrastructures; and
- Protect the radiofrequency spectrum used by GPS and its augmentations, and work with U.S. industry to investigate additional areas of the spectrum which could increase GPS and PNT resilience.

---

[12] "National Space Policy of the United States of America," The White House, June 28, 2010, https://www.nasa.gov/wp-content/uploads/2015/01/national_space_policy_6-28-10.pdf

[13] "National Timing and Resiliency Act of 2018," https://www.congress.gov/115/plaws/publ282/PLAW-115publ282.pdf#page=86

[14] "Executive Order 13905, "Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services," The Federal Register, February 19, 2020, https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing; "National Space Policy of the United States of America," The White House, September 9, 2020, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf; Space Policy Directive 5, "Cybersecurity Principles for Space Systems," The White House, September 10, 2020, https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems; and Space Policy Directive 7, "The United States Space-Based Positioning, Navigation, and Timing Policy."

Many of these actions have been consistently directed since 2004. Little progress has been made on most despite the sometimes publicly expressed views of senior U.S. government officials.[15] The long-standing lack of progress on issues so important to U.S. national, homeland, and economic security demonstrates the imperative to reevaluate and reset the way PNT policy, guidance, and programs are led and executed.

System Description

GPS is owned by the U.S. Department of Defense (DoD) and designed, developed, procured, operated, and sustained by the U.S. Space Force (USSF). It was preceded by the U.S. Navy's Timation program, the U.S. Air Force's 621B technology program, and the Advanced Research Projects Agency's Transit navigation satellite system.[16] GPS reached initial operating capability in 1993 and full operating capability in 1995.[17]

The system is comprised of space, control, and user segments.[18] The USSF is responsible for the space and control segments as well as common UE for more than one service, while other military branches acquire UE for their unique applications and commercial enterprises produce a wide variety of civilian UE. The GPS space segment consists of a minimum of 24 operational satellites, although the USSF has been flying 31 for more than a decade. Spacecraft are deployed in 6 equally spaced planes in nearly circular medium Earth orbit (MEO) at an altitude of about 20,200 kilometers (12,550 miles).[19] They orbit the Earth every 12 hours and are spaced so that at least 6 satellites are in view of users anywhere in the world.

The current constellation is a mix of old and new spacecraft – 6 GPS IIR, 7 IIR-M, 12 Block IIF, and 6 IIIs.[20] The IIR-M satellites added a second civil signal L2C, M- (for military) code signals for anti-jamming, and flexible power.[21] IIF spacecraft added a third civil signal on L5 frequency as well as advanced atomic clocks.[22] GPS III satellites added a fourth civil signal on L1C and IIIF vehicles will have up to 60 times greater anti-jam capability, an accuracy-enhancing laser retro-reflector array, and new digital navigation as well as search and rescue payloads.[23] They will also have a more resilient satellite bus and enhanced cyber security features.

---

[15] See, for example, House Transportation Committee Letter to Deputy Secretary of Defense Work and Deputy Secretary of Transportation Mendez August 31, 2015, http://rntfnd.org/wp-content/uploads/Congressional-Letter-to-PNT-Executive-Committee.pdf, and Letter to Congressman Garamendi from Deputy Secretary of Transportation Mendez and Deputy Secretary of Defense Work, December 8, 2015, https://rntfnd.org/wp-content/uploads/DSD-and-Dep-DOT-reply-to-Mr.-Garamendi.pdf

[16] See, for example, Brad Parkinson, et. al., "The Origins of GPS and the Pioneers Who Launched the System, GPS World, May 1, 2010, https://www.gpsworld.com/origins-gps-part-1/; Daniel Perry, "NRL Launched First Time-Based Navigation Satellite in 1967," May 31, 2023, https://www.nrl.navy.mil/Media/News/Article/3411925/nrl-launched-first-time-based-navigation-satellite-in-1967/; "Transit Satellite," Smithsonian, https://www.gps.gov/policy/docs/2021/; and "Transit Satellite: Space-based Navigation," Defense Advanced Research Projects Agency, https://www.darpa.mil/about-us/timeline/transit-satellite

[17] U.S. Space Force, "Global Positioning System Fact Sheet," February 2023, https://media.defense.gov/2023/Feb/10/2003159890/-1/-1/1/GPS%20FACTSHEET.PDF

[18] "The Global Positioning System," https://www.gps.gov/systems/gps; Global Positioning System Precise Positioning Service Performance Standard (Washington, D.C.: Department of Defense, 2007), https://www.gps.gov/technical/ps/2007-PPS-performance-standard.pdf; Global Positioning System (GPS) Civil Monitoring Performance Specification, 3rd ed., (Washington, D.C.: Department of Transportation, 2020), https://www.gps.gov/technical/ps/2020-civil-monitoring-performance-specification.pdf; and Defense Science Board Task Force, The Future of the Global Positioning System, (Washington, D.C.: Department of Defense, 2005), https://dsb.cto.mil/reports/2000s/ADA443573.pdf

[19] "The Global Positioning System: Constellation Arrangement," https://www.gps.gov/systems/gps/space/

[20] "The Global Positioning System: Current and Future Satellite Generations," https://www.gps.gov/systems/gps/space/

[21] Ibid.

[22] Ibid.

[23] "GPS III/IIIF: The New Generation of Positioning, Navigation and Timing," Lockheed Martin, https://www.lockheedmartin.com/en-us/products/gps.html

The GPS control segment consists of a master control station, operated by the USSF's Delta 8 at Schriever Space Force Base (SFB), Colorado, an alternate master control station at Vandenberg SFB, California, 6 dedicated and 10 shared monitor stations, and 11 ground antennas located around the world.[24] The monitor stations track all GPS satellites in view and collect ranging information from the satellite broadcasts. The monitor stations send the information they collect from each of the satellites to the master control station which computes precise orbits. That information is formatted into updated navigation messages and transmitted to each satellite via ground antennas, which also transmit and receive satellite control and monitoring signals.

The user segment is comprised of receivers, processors, and antennas which enable terrestrial and space uses of GPS signals from satellites in view. In addition to calculating and displaying the user's position, velocity, and time, some UE display additional data, such as distance and bearing, to selected waypoints or digital charts. DoD has encountered numerous challenges acquiring modernized GPS capabilities resulting in the lack of synchronization among the system's space, control, and user segments.[25] This has prevented use of the system's full functionality. The next generation operational control system (OCX) intended to modernize the GPS control segment is over budget and more than seven years behind schedule.[26] Similarly, an insufficient number of M-code receivers are being procured to support U.S. military operations.[27]

The GPS concept of operation is based upon satellite ranging or time difference of arrival.[28] Users determine their position on Earth by measuring their distance from the satellites in view which serve as reference points. Each GPS satellite transmits an accurate position and time signal. UE process the data from 4 or more satellites to provide the 3 dimensions of latitude, longitude, altitude, and then time. Calculations of how position changes with time provide measures of velocity.

"There are shortfalls in U.S. PNT capabilities."

Despite ongoing GPS modernization activities, however, there are shortfalls in U.S. PNT capabilities. These include:

- **Assured, real-time PNT in physically impeded environments (e.g., indoors, urban canyons, underground facilities);**
- **Sufficient accuracy and integrity in electromagnetically impeded environments including operations during spoofing, jamming, and natural and unintentional interference;**
- **Higher accuracy with high integrity; timely notification/alarming when PNT performance is degraded or misleading, especially for safety-of-life applications or to avoid collateral damage;**

---

[24] "The Global Positioning System: Control Segment," https://www.gps.gov/systems/gps/control/

[25] See, for example, GPS Modernization: Space Force Should Reassess Requirements for Satellites and Handheld Devices (Washington, D.C.: Government Accountability Office, 2023), https://www.gao.gov/assets/d23106018.pdf; GPS Modernization DoD Continuing to Develop New Jam Resistant Capability, But Widespread Use Remains Years Away (Washington, D.C.: Government Accountability Office, 2021), https://www.gao.gov/assets/gao-21-145.pdf; Selected Acquisition Report, Next Generation Operational Control System (OCX) (Washington, D.C.: Department of Defense, 2023), https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Selected_Acquisition_Reports/FY_2022_SARS/OCX_SAR_DEC_2022.pdf; GPS Alternatives: DoD Is Developing Navigation Systems But Is Not Measuring Overall Progress (Washington, D.C.: Government Accountability Office, 2022), https://www.gao.gov/assets/d22106010.pdf; and Jesse Khalil, "GPS OCX Delays Continue, GPS World, February 16, 2024, https://www.gpsworld.com/gps-ocx-delays-continue/

[26] Ibid.

[27] Ibid.

[28] Global Positioning System Precise Positioning Service Performance Standard, Global Positioning System (GPS) Civil Monitoring Performance Specification, and The Future of the Global Positioning System.

- **Ensuring PNT services, including supporting Information Technology (IT) infrastructure and supply chain are protected from cyber threats;**
- **Ability to accurately locate sources of intentional and unintentional interference in a timely manner; and**
- **Insufficient resilience and survivability when GPS services are unavailable or untrusted.[29]**

In addition, the U.S. has several capabilities to augment GPS. Such augmentation systems utilize information and data from GPS to improve, for example, the accuracy, integrity, and availability of its PNT services. They include the space-based wide area, ground-based, and aircraft-based augmentation systems operated by DoT's Federal Aviation Administration to support aircraft navigation across North America. The National Aeronautics and Space Agency's Jet Propulsion Laboratory also collects data that could be used to establish an internet-based High Accuracy and Robustness Service that could be accessed by many mobile and fixed GPS users.[30] Further, it is common for civilian UE, such as cell phones, to have an augmentation stack that exploits cell towers, television signals, accelerometers, geographic information services (GIS) databases, ionospheric model predictions, etc.

Utility

GPS was originally designed to provide two levels of service – a standard positioning service for public use and an encoded precise positioning service for national security use. The standard service was intended to provide civilian users with a less accurate positioning capability with SA than the precise service. In 2000, as noted, President Clinton directed deliberate degradation of accuracy for the non-military signals to be discontinued. In 2007, President Bush accepted DoD's recommendation to end procurement of GPS satellites with SA capability.[31]

Consequently, GPS has grown into a global utility since reaching full operational capability in 1995. It is now integral to economic development and growth, transportation safety, critical infrastructures, and U.S. and international security. More than four billion users worldwide depend on the system's PNT signals for location (determining the longitude, latitude, and altitude of a position within 30 feet or less), navigation (moving from one location to another), velocity (determining the speed of an object within a fraction of a mile per hour), timing (calculating time within one millionth of a second), tracking (monitoring the movement of people and objects), and mapping and charting (creating maps and charts of the world).

"American society has been transformed by the availability of GPS."

The invention of PNT technology led to the creation of a wide range of applications. Over four decades, American society has been transformed by the availability of GPS. New enterprises have been established and existing businesses have radically altered their staffing, training, equipment, and procedures. In the Defense Department, GPS enabled precision strike has altered policy, strategy, doctrine, operations concepts, and weapons systems.

---

[29] The Global Positioning System: GPS Applications," https://www.gps.gov/applications/; Federal Radionavigation Plan 2021 (Washington, D.C.: Departments of Defense, Transportation, and Homeland Security, 2021), https://www.navcen.uscg.gov/sites/default/files/pdf/2021_Federal_Rdionavigation_Plan.pdf

[30] National Space-Based Positioning, Navigation, and Timing Advisory Board White Paper, "GPS High Accuracy and Robustness Service (HARS)," May 5, 2023, https://www.gps.gov/governance/advisory/recommendations/2023-05-white-paper-GPS-HARS.pdf

[31] "Statement by the Press Secretary," The White House, September 18, 2007, https://csps.aerospace.org/sites/default/files/2021-08/GPS%20SA%20discontinued%2018Sep07.pdf

"The harm to the U.S. economy that would result if GPS services were lost is incalculable."

GPS services are essential to America's society, economy, and security. They enable Americans' way of life. Attempts have been made to estimate the economic value of GPS to the nation. The Department of Commerce (DoC), for example, estimates that the economic benefits of private sector use of GPS services to the U.S. economy between 1984 and 2017 was $1.4 trillion.[32] **The harm to the U.S. economy that would result if GPS services were lost is incalculable.[33]**

All sixteen of the formally designated U.S. critical infrastructure sectors rely upon GPS. The following are some examples:[34]

- Food and Agriculture — GPS enables precision farming to optimize use of fertilizers, herbicides, and pesticides which improve crop yields and help protect the environment. Combined with GIS and remote sensing, GPS also enables improved land and water use for agriculture. In addition, commercial fishing fleets use GPS to navigate to fishing locations as well as track fish migrations.

- Energy — GPS increases the reliability and efficiency of power grids' transmission and distribution, supervisory control and data acquisition (SCADA) systems, and offshore oil and gas exploration and drilling. SCADA, a computer-based system for gathering and analyzing real-time data to monitor and control equipment that deal with critical and time-sensitive materials or events, is widely used in pipeline monitoring and control, remote equipment and asset monitoring, and control of production, pumping, and storage, offshore platforms and onshore wells, refineries, and petrochemical stations.

- Emergency Services — GPS enhances the efficiency and effectiveness of emergency services as well as disaster relief operations. It helps first responders accurately navigate to emergencies, manage forest fires, and conduct search and rescue operations. In conjunction with GIS and remote sensing, GPS enables search teams to create maps of disaster areas for rescue and conduct aid operations.

- Financial Services — GPS enables operational analytics, market transparency, compliance, and automated trading. Precise, synchronized time supports the processing and analytics of hundreds of millions of financial transactions a second. Accurate time stamps also demonstrate that transactions are executed in the proper sequence and comply with U.S. and international market regulations.

- IT and Telecommunications — GPS is used to operate IT systems and synchronize telecommunications. It improves the reliability and bandwidth utilization of wireless networks. This includes the development and management of the Internet of Things (IoT) connecting and exchanging an immense quantity of real-time sensor data from devices such as smartphones, laptops, home appliances, and automobiles. Cellular networks use GPS to synchronize base stations enabling mobile handsets to share radio spectrum efficiently. It is also used to disassemble, deliver, and reassemble data packets and hand over calls from one cell tower to another as phones move.

- Transportation — GPS improves the safety, efficiency, and tracking of land, rail, maritime, and flight operations. The trucking industry uses GPS-enabled telematics to increase efficiency, decrease costs,

---

[32] Economic Benefits of the Global Positioning System (GPS) (Gaithersburg, Md: National Institute of Standards and Technology, 2019), https://www.nist.gov/system/files/documents/2020/02/06/gps_finalreport618.pdf

[33] Dana Goward, "The Billion-Dollar-a-Day Mistake?" GPS World, May 25, 2022, https://www.gpsworld.com/the-billon-dollar-a-day-gps-mistake/

[34] See, for example, Ibid; "The Global Positioning System: GPS Applications," https://www.gps.gov/applications/; Federal Radionavigation Plan 2021; Michael Lombardi, An Evaluation of Dependencies of Critical Infrastructure Timing Systems on the Global Positioning System (GPS), NIST Technical Note 2189 (Washington, D.C.: Department of Commerce, 2021), https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2189.pdf; and NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System (GPS) (Washington, D.C.: National Security Telecommunications Advisory Committee, 2008), https://www.cisa.gov/sites/default/files/publications/NSTAC%20GPS%20Report_0.pdf

> and reduce environmental impacts through improved vehicle dispatch and navigation. Passenger and freight railroads utilize GPS-based positive train control systems to prevent collisions, derailments, and incursions into work zones. GPS also increases the efficiency and safety of aviation across all phases of flight as well as maritime operations in the open ocean and more congested inland waterways, harbors, and ports. In addition, it supports mapping, charting, and geodesy, weather forecasting, and iceberg tracking.

The operation of other space systems which support U.S. critical infrastructures also rely upon GPS. It supports space launch and range operations by enabling range safety and autonomous flight termination at spaceports.[35] GPS also enables high precision orbit determination and attitude solutions.[36] Consequently, it enables efficient control of satellite constellations, automated station-keeping on-orbit, and formation flying of spacecraft.

Moreover, the United States and our allies rely on GPS to enhance the operational effectiveness of armed forces. It increases the precision, accuracy, safety, and effectiveness of military operations in all (land, maritime, air, cyberspace, and outer space) domains. GPS generates information and data which are integral to command, control, communications, computing, intelligence, surveillance, reconnaissance, blue force tracking, search and rescue, targeting, and weapons delivery.[37] The system's PNT services thus have increased America's ability to project power anywhere in the world with precision, speed, and lethality.

During the 1991 Persian Gulf conflict, for example, U.S. armed forces employed GPS to navigate in the featureless desert terrain. GPS played a critical role in the "left hook" of armored and airborne forces which involved their maneuver from positions in Kuwait to strike deep to the Euphrates river in Iraq.[38] Through flanking and envelopment, the U.S. forces were able to cut off Iraqi forces in Kuwait and destroy much of the Republican Guard.

Subsequently, the utility of GPS for weapons delivery was highlighted by the second Gulf War. The U.S. Air Force did not have to conduct as many sorties and expend large numbers of ordnance to prosecute a single target as it did in previous conflicts. This reduced the risk to flight crews and extent of collateral damage. During Operation Iraqi Freedom, the U.S. employed GPS-enabled precision-guided munitions which allowed only a single weapon to destroy a target.[39] The system enabled delivery of 5,500 GPS-guided Joint Direct Attack Munitions to about 10 feet with minimal collateral damage. This was almost one-fourth of the total 29,199 bombs and missiles coalition forces released against Iraqi targets.[40]

The information and data generated by GPS are essential for the conduct of effective non-linear, multi-domain, military operations. The system enables the maneuver, synchronization, and massing of effects from dispersed forces. PNT services provided by GPS are also critical to achieving information and decision superiority over an adversary. **In short, GPS is a lynchpin of space-enabled, precision strike warfare.** The capabilities provided by the system have contributed to making space power the leading-edge of U.S. information-age military power.

---

[35] Ibid.

[36] "Cybersecurity Principles for Space Systems."

[37] The Future of the Global Positioning System.

[38] Donald P. Wright, "Deception in the Desert: Deceiving Iraq in Operation DESERT STORM," in Christopher M. Rein, ed., Weaving the Tangled Web (Fort Leavenworth, KS: Army University Press, 2018), https://www.armyupress.army.mil/Books/Browse-Books/iBooks-and-EPUBs/Deception-in-the-Desert/#:~:text=In%20what%20eventually%20became%20known,off%20Iraqi%20forces%20in%20Kuwait

[39] See, for example, "The Evolution of GPS from Desert Storm to Today's Users," March 24, 2016, https://www.af.mil/News/Article-Display/Article/703894/evolution-of-gps-from-desert-storm-to-todays-users/

[40] U.S. Air Force, "Global Positioning System Fact Sheet," November 23, 2015, and U.S. Space Force, "Global Positioning System Fact Sheet," October 2020, https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197765/global-positioning-system/

Threats

The United States is engaged in a geostrategic contest with foreign powers which extends to outer space. Russia, China, Iran, and North Korea are led by autocratic regimes with revisionist or irredentist political aims seeking to change the international system. They act independently and collaborate to flout international law, ignore United Nations sanctions, undermine international norms of responsible behavior, and threaten or use armed force to achieve their political objectives. Consequently, America is confronting an unprecedented array of threats in the global security environment.[41]

The complex and dangerous operating environment in outer space mirrors the security environment on Earth. Those foreign adversaries have weapons systems with both reversible and irreversible effects to contest freedom of passage through and operations in space. According to unclassified intelligence reports, **Russia and China are acquiring or operating various cyber, EW, kinetic energy, directed energy, nuclear, and orbital ASAT or counterspace weapons systems.[42]** The U.S. government, as noted, also recently confirmed that Russia has developed and is preparing to deploy a nuclear-armed ASAT weapon on-orbit.[43] Additionally**, Iran and North Korea operate cyber, EW, and missile capabilities which can interfere with space assets and operations.[44] All four nations have conducted Navwar operations against GPS.**

"Russia has extensively interfered with GPS before and since its ongoing unlawful invasion of Ukraine."

Cyber and EW attacks against GPS could involve jamming uplinks, downlinks, or crosslinks, spoofing or corrupting data, sending unauthorized commands for spacecraft guidance and control, and injecting malicious code.[45] Russia has extensively interfered with GPS before and since its ongoing unlawful invasion of Ukraine. It repeatedly jammed unmanned aerial vehicles (UAVs) along Ukraine's border with Russia being used by the Organization for Security and Cooperation in Europe to monitor the Minsk agreement under which Russia committed to return the Donbas and Luhansk regions to Ukraine's control.[46] In 2021, Russia also spoofed the position of the U.K. Royal Navy's destroyer HMS Defender and the Royal Netherlands Navy's HNLMS Evertsen sailing in the Black Sea near Russia's naval base at Sevastopol.[47]

---

[41] See, for example, Annual Threat Assessment of the U.S. Intelligence Community (Fairfax, VA: Office of the Director of National Intelligence, 2024), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

[42] Defense Intelligence Agency, Challenges to Security in Space (Washington, D.C.: Department of Defense, 2022), https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf; National Space Intelligence Center, Competing in Space (Wright Patterson, AFB, Ohio, 2018), https://media.defense.gov/2019/Jan/16/2002080326/-1/-1/0/190115-F-NV711-0001.JPG; National Space Intelligence Center, Competing in Space, 2nd ed., (Wright-Patterson AFB, Ohio, 2024), https://www.spoc.spaceforce.mil/Portals/4/Images/2_Space_Slicky_11x17_Web_View_reduced.pdf; Space Threat Assessment 2023 (Washington, D.C.: Center for Strategic and International Studies, 2023), https://www.csis.org/analysis/space-threat-assessment-2023; and Secure World Foundation, Global Counterspace Capabilities: An Open Source Assessment (Washington, D.C.: Secure World Foundation, 2024), https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf

[43] "Press Briefing by Press Secretary Karine Jean-Pierre and White House National Security Communications Advisor John Kirby," The White House, February 15, 2024, https://www.whitehouse.gov/briefing-room/press-briefings/2024/02/15/press-briefing-by-press-secretary-karine-jean-pierre-and-white-house-national-security-communications-advisor-john-kirby-3

[44] Challenges to Security in Space; Competing in Space; Space Threat Assessment 2023; and Global Counterspace Capabilities: An Open Source Assessment.

[45] "Cybersecurity Principles for Space Systems."

[46] See, for example, Dana Goward, "Russia Ramps Up GPS Jamming Along with Troops at Ukraine Border," GPS World, April 21, 2021, https://www.gpsworld.com/russia-ramps-up-gps-jamming-along-with-troops-at-ukraine-border/

[47] See, for example, H.I. Sutton, "Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base," U.S. Naval Institute News, June 21, 2021, https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base#:~:text=Positions%20of%20Two%20NATO%20Ships%20Were%20Falsified%20Near%20Russian%20Black%20Sea%20Naval%

Further, since Russia's invasion of Ukraine, both sides have either jammed or spoofed PNT signals. Since Poland's deployment of an American provided Aegis anti-missile system along its northern border on the December 15, 2023, Russia has increased jamming and spoofing GPS in the Kaliningrad region, surrounding Baltic sea and neighboring states, eastern Finland, and the Black Sea.[48] Russian GPS jamming around Kaliningrad prompted Swedish Rear Admiral Eva Skoog Haslum to warn that it is endangering shipping and air travel in the region.[49] Similarly, the Foreign Ministers of Lithuania, Latvia, and Estonia recently warned that escalating Russian GPS jamming threatens to create an air disaster.[50]

China has also interfered with GPS in the Indo-Pacific region. It has deployed EW systems on ground, maritime, and air platforms for both offensive and defensive operations.[51] Some military aircraft and commercial airliners, including from Australia's Qantas airline, recently reported GPS jamming from Chinese warships in the South China Sea, Philippine Sea, and Indian Ocean.[52]

Similarly, Iran and North Korea have jammed or spoofed GPS for years. More than twenty aircraft flying near Iraq in 2023, for example, suffered acute navigation failures, including fake GPS signals, attributed to Iran.[53] In some cases, air traffic controllers had to provide pilots with radar vectors to their destinations. Since Hamas' unlawful invasion of Israel on October 7, 2024, and particularly in response to concerns about possible Iranian retaliation for strikes against Islamic Revolutionary Guard Corps' Quds Force commanders and operatives, Israel has reportedly interfered with GPS signals to prevent Iran or the terrorist groups it sponsors from being able to employ the system's PNT services for weapons delivery.[54] In addition, North Korea continuously jammed GPS for three days earlier this year to demonstrate its displeasure with annual U.S.-South Korean military exercises.[55]

Moreover, as noted, Russia's impending launch of a space-based, nuclear armed ASAT could endanger GPS. If deployed on-orbit, the nuclear ASAT would violate the 1967 Outer Space Treaty that prohibits "placing in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction."[56] A nuclear detonation in space might degrade or destroy a GPS satellite in proximity to the explosion as well as produce a blackout effect preventing communications with other spacecraft by interfering with radio and radar waves.[57]

20Base,-By%3A%20H%20I%20Sutton&text=The%20tracking%20data%20of%20two,away%2C%20USNI%20News%20has%20learned

[48] See, for example, Dana Goward, "As Baltics See Spike in GPS Jamming, NATO Must Respond," Breaking Defense, January 31, 1014, https://breakingdefense.com/2024/01/as-baltics-see-spike-in-gps-jamming-nato-must-respond,and Space Threat Assessment 2023.

[49] Patrick Tucker, "Russia's GPS Meddling In the Baltic Sea Demands NATO Action, Sweden's Naval Chief Says" Defense One, April 9, 2024, https://www.defenseone.com/threats/2024/04/russias-gps-meddling-baltic-sea-demands-nato-action-swedens-naval-chief-says/395607/

[50] "Russian GPS Jamming Threatens Air Disaster, Warn Baltic Ministers," Financial Times, April 28, 2024, https://www.ft.com/content/37776b16-0b92-4a23-9f90-199d45d955c3

[51] Military and Security Developments in the People's Republic of China (Washington, D.C.: Department of Defense, 2023), https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF

[52] See, for example, Maddie Saines, "Australian Aircraft GPS Receiver Jammed by Alleged Chinese Warships," GPS World, March 23, 2023, https://www.gpsworld.com/australian-aircrafts-gps-receiver-jammed-by-alleged-chinese-warships/

[53] See, for example, "Industry Concerned over GPS Interference Near Iran," Aviation Week Network, September 29, 2023, https://aviationweek.com/air-transport/safety-ops-regulation/industry-concerned-over-gps-interference-near-iran

[54] See, for example, Sune Engel Rasmussen, "Israel Scrambles GPS Signals as Country Girds for Potential Retaliation From Iran," The Wall Street Journal, April 4, 2024, https://www.wsj.com/world/middle-east/israel-scrambles-gps-signals-as-country-girds-for-potential-retaliation-from-iran-f653c918

[55] See, for example, Ji Da-gyum, "N. Korea Attempted to Disrupt GPS Signals on S. Korean Border Islands,"

https://www.koreaherald.com/view.php?ud=20240308050655

[56] "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies," https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

[57] Ibid.

While a nuclear-armed ASAT could only be used once against a GPS target, a nuclear-powered directed energy weapon could be used multiple times to damage or destroy specific GPS satellites. Russia and China have deployed ground-based lasers and are probably conducting research and development (R&D) on space-based directed energy weapons.[58] Further, a space-based EW weapon could be used multiple times with a range of effects. This includes disrupting communications with or operation of GPS satellites, damaging components on spacecraft, or interfering with terrestrial receivers. Such a weapon is technically feasible. Russia reportedly has conducted R&D on a space-based EW weapons platform powered by a thermionic reactor.[59] The Soviet Union previously operated radar ocean reconnaissance satellites powered by nuclear reactors.[60] A space-based EW weapon could have devastating impacts to the U.S. homeland. By denying GPS signals, it would degrade a wide variety of critical infrastructures and applications. The economy could be crippled and the effectiveness of military operations diminished.

"Merely the threat of disrupting GPS services might be enough to impact U.S. national security and foreign policy."

Merely the threat of disrupting GPS services might be enough to impact U.S. national security and foreign policy. Indeed, America may have already been subject to at least attempted "GPS blackmail." On November 15, 2021, prior to its invasion of Ukraine, Russia conducted a destructive test of a direct ascent, kinetic energy ASAT. The test generated thousands of pieces of orbital debris which endangered both American astronauts and Russian cosmonauts on the International Space Station as well as harmed space environmental sustainability.[61] Several days later Russian state media warned that if NATO crossed Russia's "red lines" they would destroy all 32 GPS satellites "blinding NATO." Despite 90,000 Russian troops massing along the border with Ukraine, U.S. officials decided against sending certain military equipment to Ukraine to avoid provoking Russia.[62]

Resilience

GPS was designed for survivability, endurance, and operational continuity. It is among the most resilient U.S. national security space systems. Resilience is the ability of an architecture to support the functions necessary for mission success, with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, conditions, and threats, despite hostile actions or adverse conditions.[63] The system is, of course, capable of withstanding natural hazards in space such as the radiation environment at MEO.

---

[58] Challenges to Security in Space; Competing in Space; Oskar Glaese, "China's Directed Energy Weapons and Counterspace Applications," The Diplomat, June 29, 2022, https://thediplomat.com/2022/06/chinas-directed-energy-weapons-and-counterspace-applications/; and Dwayne Day and Robert Kennedy, "Barbarian in Space: the Secret Space-Laser Battle Station of the Cold War," The Space Review, June 5, 2023, https://www.thespacereview.com/article/4598/1

[59] Bart Hendrickx, "Ekipazh: Russia's Top-Secret Nuclear-Powered Satellite," The Space Review,

October 7, 2019, https://www.thespacereview.com/article/3809/1

[60] In 1978, the USSR's Cosmos 954 radar ocean reconnaissance satellite failed and spread debris across northwest Canada. See Gus Weiss, "The Life and Death of Cosmos 954: A Radioactive Satellite Decays," Studies in Intelligence, Vol. 22 (Spring 1978), https://www.cia.gov/readingroom/docs/CIA-RDP80-00630A000100020001-7.pdf

[61] Russian Direct-Ascent Anti-Satellite Missile Test Creates Significant, Long-Lasting Space Debris," U.S. Space Command Office of Public Affairs, November 15, 2021, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/2842957/russian-direct-ascent-anti-satellite-missile-test-creates-significant-long-last/

[62] Ross Ibbetson and Will Stewart, "Russia Warns it Can Destroy NATO Satellites – Rendering Missiles Useless," Daily Mail, November 23, 2021, https://www.dailymail.co.uk/news/article-10233287/Russia-warns-destroy-NATO-satellites-White-House-says-concerns.html

[63] DoD Directive 3100.10, "Space Policy," (Washington D.C.: Department of Defense, 2016), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/310010p.PDF

The system's architecture is also resilient against certain human-made threats. The USSF provides physical security of the GPS master control station as well as its alternate to defend against terrorist, unconventional, and conventional attacks. As a proliferated (i.e., large number of satellites) and distributed (i.e., capability spread across multiple planes and geographic locations) space architecture able to cross-link data, GPS may have sufficient endurance to degrade gracefully against kinetic or directed energy weapons effects depending on the size of an adversary's arsenal. Radiation hardened components should afford the satellites some protection against transient radiation effects on electronics from a nuclear detonation in space. GPS also has certain cyber security as well as anti-jam and anti-spoof capabilities.[64]

Nonetheless, GPS is not necessarily survivable against all dangers.[65] Cyber-attack against the space or control segments could deny or corrupt PNT data, degrade the capability or lifespan of individual GPS satellites or the constellation, or possibly even take over control of space vehicles.[66] The latter might cause collisions that would impair the system and generate orbital debris.

EW jamming and spoofing of GPS apparently are less difficult than hacking into the system. GPS jamming devices, while illegal, are inexpensive and can be purchased on the internet. Such devices have proliferated around the world. There have been thousands of both unintentional and intentional jamming incidents where PNT services were disrupted or denied to civilian users. Spoofing is more consequential than jamming because of how long it takes users or devices to detect it.[67] Interfering with military and dual-frequency GPS receivers is more difficult.

Strikes by non-nuclear or nuclear-armed hypersonic, ballistic, or cruise missiles could damage or destroy the GPS master control station or its alternate as well as other parts of the control segment outside the continental United States. Additionally, a nuclear detonation in space designed to produce an electromagnetic pulse (EMP) would affect terrestrial receivers, processors, and antennas.[68] Semiconductors in such UE, for example, would fail when exposed to EMP.

There are numerous potential approaches to improve the resilience of U.S. PNT services. For example, utilization of allied and other trusted international GNSS capabilities, such as Europe's Galileo and Japan's QZSS regional system, could enhance the resilience of such services but not replace GPS. They also have vulnerabilities, however, to adversary Navwar capabilities. In addition, Iridium Communications recently announced that it had entered into an agreement to acquire Satelles to provide a global alternative satellite time and location service to complement GPS and protect against GNSS vulnerabilities using low-cost hardware that does not require outdoor antennas.[69]

During the Bush administration in 2006, a GPS independent advisory team (IAT) conducted a study for DoT and DoD which concluded that the federal government could upgrade the Loran radionavigation infrastructure. Loran was initially established during World War II using low-frequency hyperbolic radio to

---

[64] "GPS III/IIIF: The New Generation of Positioning, Navigation and Timing;" and "Global Positioning System (GPS) Selective Availability Anti-Spoofing Module (SAASM)," Director of Operational Test and Evaluation," https://www.dote.osd.mil/Portals/97/pub/reports/FY2011/af/2011gps.pdf?ver=2019-08-22-112333-690

[65] See. for example, Resilient Navigation and Timing Foundation, "Prioritizing Dangers to the United States from Threats to GPS: Ranking Risks and Proposed Mitigations," https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf

[66] "Cybersecurity Principles for Space Systems."

[67] National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions (Washington, D.C.: Department of Homeland Security, 2013), https://www.gps.gov/news/2013/06/2013-06-NRE-public-summary.pdf

[68] See, for example, Nuclear Matters Handbook (Washington, D.C.: Department of Defense, 2020), pp .167-183, https://www.acq.osd.mil/ncbdp/nm/NMHB2020rev/docs/NMHB2020rev.pdf and Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, April 2008, p. vi, https://apps.dtic.mil/sti/pdfs/ADA484672.pdf

[69] Press Release, "Iridium to Expand its Reach as a Global Alternative PNT Service with Acquisition of Market Leader Satelles," Iridium, March 4, 2024, https://investor.iridium.com/2024-03-04-Iridium-to-Expand-its-Reach-as-a-Global-Alternative-PNT-Service-with-Acquisition-of-Market-Leader-Satelles

support convoy operations in the Atlantic as well as naval and air operations in the Pacific theaters**. The IAT proposed transforming it into an enhanced Loran (eLoran) system for the same cost as decommissioning the terrestrial system. One of the IAT's key findings was that "eLoran is the only cost-effective backup for national needs; it is completely interoperable with and independent of GPS, with different propagation and failure mechanisms, plus significantly superior robustness to radio frequency interference and jamming."**[70]

Consequently, the IAT recommended that for at least the next twenty years, eLoran "be completed and retained as the national backup system for critical safety of life, national and economic security, and quality of life applications currently reliant on position, time, and/or frequency from GPS."[71] In 2010, however, President Obama terminated the Loran program stating that "year after year, this obsolete technology has continued to be funded even though it serves no government function and very few people are left who still actually use it."[72] This decision seemed to have been later reversed when the Obama administration promised members of Congress that it would pursue near-term opportunities "to support a timing-focused eLoran network, while also documenting the requirements for a more comprehensive complementary PNT capability for the nations critical infrastructure."[73] Despite this commitment, no project was established and no request for funding was ever included in the President's budget submitted to Congress. In contrast, the United Kingdom, China, South Korea, and Saudi Arabia either have or are upgrading their terrestrial PNT backup systems to eLoran.[74] Russia's Chayka system is equivalent to Loran-C and may be upgraded.[75]

The U.S. government has taken some steps towards identifying key GPS dependencies and potential mitigation solutions. The Department of Homeland Security (DHS), for example, conducted vulnerability and impact assessments for critical infrastructure due to unmitigated PNT vulnerabilities.[76] It also published a Resilient PNT Conformance Framework with guidance for defining resilient PNT UE intended to facilitate development and adoption of a common risk management framework for end users.[77] Additionally, DHS issued a Resilient PNT Reference Architecture which describes the application of resilience concepts for next-generation resilient PNT which provides example resilience techniques, modern cybersecurity principles, and reference designs.[78] In addition, DoD, DoT, and DHS have published sector-specific mitigation and backup capabilities in the event of disruptions of GPS services in the Federal Radionavigation Plan.[79] Such mitigations include, for example, DoT's operation of ground-based navigation aids for aviation and DoC's provision of a GNSS-independent source of Coordinated Universal Time.[80]

Moreover, both DoT and DoD have issued requests for proposals and contracts to investigate a variety of other PNT alternatives. DoT evaluated eleven commercial alternatives to government-owned and operated GPS which could serve as a backup to existing infrastructure. It concluded that a number

---

[70] Independent Assessment Team (IAT) Summary of Initial Findings on eLoran (Alexandria, VA: Institute for Defense Analysis, 2009), https://www.ursanav.com/wp-content/uploads/IDA-IAT-Report-on-eLoran-2009-1.pdf

[71] Ibid.

[72] "eLoran: The Never Ending Story?" Inside GNSS, June 15, 2009, https://insidegnss.com/eloran-the-never-ending-story/

[73] Letter to Congressman John Garamendi from Deputy Secretary of Transportation Mendez and Deputy Secretary of Defense Work.

[74] Gebrekidam, et. al., "One Satellite Signal Rules Modern Life. What Happens if Someone Knocks it Out?"; and Narins, "The Global Loran / eLoran Infrastructure Evolution." In addition to Loran, China is reportedly building hundreds of timing station and laying 12,000 miles of underground fiber optic cable to provide timing and navigation services independent of Beidou.

[75] Ibid.

[76] Cybersecurity and Infrastructure Security Agency, "Understanding Vulnerabilities of Positioning, Navigation, and Timing," 2023, https://www.cisa.gov/sites/default/files/2023-04/fs_positioning-navigation-timing-vulnerabilities_508.pdf

[77] Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework (Washington, D.C.: Department of Homeland Security, 2022), https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf

[78] Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture (Washington, D.C.: Department of Homeland Security, 2022), https://www.dhs.gov/sites/default/files/2022-06/22_0609_st_resilient_pnt_ra.pdf

[79] Federal Radionavigation Plan 2021.

[80] Ibid.

offered backup capabilities with widely varied performance and cost but "none of the systems can universally backup the positioning and navigation capabilities provided by GPS and its augmentations."[81] Consequently, the solution "should involve a plurality of diverse PNT technologies… Based on this demonstration, those technologies are LF and UHF terrestrial and L-band satellite broadcasts for PNT functions with supporting fiber optic time services to transmitters/control segments."[82] Additionally, the Space-based PNT Advisory Board observed that techniques for enhancing UE, including new signals and signal processing, integration with inertial sensors, and use of adaptive antennas were well known and recommended that export control regulations be modified or eliminated to enable critical infrastructure protection and safety applications.[83] In addition, DoT recently awarded contracts totaling more than $7.2 million to nine complementary PNT technology vendors to conduct real-world field tests of commercial PNT technologies to facilitate adoption into systems that depend on secure and reliable PNT services.[84] The awards provide funding for instrumentation, testing, and evaluation of complementary PNT technologies at field test ranges in conjunction with critical infrastructure owners and operators to facilitate their adoption and improve PNT resiliency.

DoD has initiated R&D on several alternatives examining both relative PNT technologies which use onboard sensors to track the position of a platform and keep time without the use of an external signal as well as absolute PNT technologies which use external sources of information, other than GPS, to determine the position of a platform, geo-referenced to Earth.[85] These include the U.S. Navy's Automated Celestial Navigation System, PNT Upgrade to the Cooperative Engagement Capability, and AN/WSN-12 Inertial Navigation System, the U.S. Army's Dismounted Assured Position Navigation and Timing System, Mounted Assured Positioning, Navigation and Timing System, and Alternative Navigation and Assured Precision Weapons and Munitions, the USSF's Navigation Technology Satellite-3, and DoD's Critical Time Dissemination program.[86] The U.S. Air Force also demonstrated the utility of eLoran as a terrestrial PNT alternative. In January, the 366th Fighter Wing Innovation Cell STRIKE WERX hosted an eLoran demonstration at Mountain Home Air Force Base, Idaho.[87]

In addition, the Department of the Air Force recently used "quick start" authorities to begin a new, resilient "GPS lite" program.[88] The initiative is designed to begin engineering studies and initial development work before Congress authorizes and approves funding for the program. It will explore the feasibility of using commercial technologies to build smaller and less expensive GPS satellites for a distributed network that can augment the traditional Global Positioning System which can be refreshed more frequently.[89] The Defense Information Systems Agency also invited vendors to compete for the Proliferated Low Earth Orbit Satellite-Based Services contract for commercial satellite services that provide high-speed

---

[81] U.S. Department of Transportation, Report to Congress, National Timing Resilience and Security Act Roadmap To Implementation, 2021, https://www.transportation.gov/sites/dot.gov/files/2021-01/NTRSA%20Report%20to%20Congress_Final_January%202021.pdf

[82] U.S. Department of Transportation, Complementary PNT and GPS Backup Technologies Demonstration Report, January 2021, https://www.transportation.gov/sites/dot.gov/files/2021-01/FY%2718%20NDAA%20Section%201606%20DOT%20Report%20to%20Congress_Combinedv2_January%202021.pdf

[83] Tim Murphy, "Toughening Via Reducing Export Restrictions on GNSS Adaptive Antennas," Space-Based PNT Advisory Committee, May 3, 2023, https://www.gps.gov/governance/advisory/meetings/2023-05/murphy.pdf

[84] "Department of Transportation Awards $7 million for Complementary Positioning, Navigation and Timing Technologies," July 3, 2024, https://www.transportation.gov/briefing-room/department-transportation-awards-7-million-complementary-positioning-navigation-and

[85] GPS Alternatives: DoD Is Developing Navigation Systems But Is Not Measuring Overall Progress.

[86] Ibid.

[87] Airman Keagan Lee, "Innovation Cell Hosts eLoran Demonstration," https://www.mountainhome.af.mil/News-Photos-Videos/Article-Display/Article/3681900/innovation-cell-hosts-eloran-demonstration/

[88] Sandra Erwin, "Air Force Selects Space Programs for 'Quick Start' Initiative, Space News, April 16, 2024, https://spacenews.com/air-force-selects-space-programs-for-quick-start-initiative/#:~:text=Resilient%20GPS&text=The%20program%20is%20led%20by,actual%20budget%20for%20the%20program.

[89] Sandra Erwin, "Space Force Eyes Faster Satellite Development with Commercial Tech," Space News, April 15, 2024, https://spacenews.com/space-force-eyes-faster-satellite-development-with-commercial-tech/

broadband, Earth imaging, and alternative PNT solutions.[90] Similarly, the Defense Innovation Unit has created a new portfolio to integrate nascent technology into military operations and is starting the effort with a solicitation to industry for quantum sensors which can provide alternative PNT capabilities.[91]

Furthermore, the USSF is investigating GPS alternatives. The SpaceWERX's Alternative PNT program, for example, is seeking proposals to improve PNT resilience and plans to award as many as twenty Small Business Innovation Research contracts to prototype and demonstrate such PNT technologies.[92] In 2021, the National Guard recognized the challenges it and other first responders would have responding to domestic contingencies in GPS-denied or manipulated environments. The Nationwide Integration of Timing Resilience for Operations (NITRO) project was initiated as a rapid protype and fielding effort. It has deployed to eight states as of this writing. If fully deployed and expanded, NITRO has the potential to both reinforce GPS and serve as an alternative PNT service. The project does not seem to have found favor within the Defense Department, however, and its future is unclear.[93] **The bottom line, however, is that the United States still does not operate a resilient and reliable alternative PNT service.**

"The system's unmitigated vulnerabilities could result in potentially profound domestic and international implications …"

Implications

Given the breadth and depth of dependencies on GPS services as well as the range of threats, **the system's unmitigated vulnerabilities could result in potentially profound domestic and international implications if exploited by an adversary (or adversaries).** Indeed, neither the full extent of dependencies nor interdependencies among the sectors depending on GPS are sufficiently understood.[94] **Depending on their severity and duration, among other factors, Navwar operations against the system could have significant consequences for all elements of U.S. national power. Critical infrastructures, national essential functions, and military forces could be at grave risk. This could have severe political, socioeconomic, and security impacts upon the United States.**

First, disruption or loss of GPS services could adversely affect America's political prestige and international influence. U.S. preeminence in space activities and its associated strategic advantages, already being eroded by foreign rivals, could be significantly undermined. National pride as well as international admiration for U.S. scientific, engineering, and technological accomplishments exemplified by our space operations in general and GPS in particular could be diminished. International perception of diminished U.S. power could translate into reduced international influence on the decisions and actions of foreign nations, organizations, and individuals.

Second, the informational element of U.S. power also could be diminished. The services provided by the IT and telecommunication sectors could be degraded, some more gracefully than others. Cellular networks, calls to 911, and the IoT could have degraded service and might eventually cease to function. Similarly, U.S. space systems which collect and transmit information and data could be adversely impacted.

---

[90] Sandra Erwin, "The Race to Back up Vulnerable GPS," Space News, February 20, 2024, https://spacenews.com/the-race-to-back-up-vulnerable-gps/#:~:text=But%20GPS%20is%20susceptible%20to,inaccurate%20or%20misleading%20positioning%20information

[91] Mikayala Easley, "DIU Launches New Emerging Tech Portfolio, Solicits Industry For Quantum Sensing Capabilities," Defense Scoop, May 19, 2024, https://defensescoop.com/2024/05/09/diu-transition-quantum-sensors-emerging-technologies-portfolio/

[92] Ibid.

[93] "The Confusing Tale of NITRO" Institute of Navigation Newsletter, Spring 2024 https://www.ion.org/newsletter/upload/ION-Spring2024.pdf

[94] National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions.

Third, interruption or denial of PNT services provided by GPS could have adverse socioeconomic implications. Interference with a utility largely transparent to most Americans could come as a psychological shock if IT and telecommunications networks, electric grids, airports, health care services, and government services were impaired or lost. Moreover, disrupted functionality of financial markets, services, commerce, and trade could have major economic ramifications. As a DHS national estimate of the risks to critical infrastructures from GPS disruptions concluded, "economic losses, lowered consumer confidence, and safety-of-life issues are possible consequences."[95] Though incalculable, such losses could be in the tens, if not hundreds, of billions of dollars a day.[96]

Moreover, given the integration of GPS into critical infrastructures and their interdependencies, lengthy disruption just of the power grid, for example, could have cascading effects which unravel America's socioeconomic fabric. As an independent commission established by Congress concluded,

> Should significant parts of the electrical power infrastructure be lost for any substantial period of time… the consequences are likely to be catastrophic, and many people may ultimately die for lack of the basic elements necessary to sustain life in dense urban and suburban communities… Electrical power is necessary to support other critical infrastructures, including supply and distribution of water, food, fuel, communications, transport, financial transactions, emergency services, government services, and all other infrastructures supporting the national economy and welfare.[97]

Fourth, U.S. national and homeland defense as well as international security could be harmed. Interference with GPS services could have a deleterious effect on America's national essential functions as well as its ability to conduct safe, efficient, and effective military operations in all domains to defend U.S. national interests and support defense commitments to allies. U.S. national essential functions are preservation of constitutional government, visible leadership to the nation and world, national defense, maintenance of foreign relations, homeland protection, emergency response and recovery, maintenance of a stable economy, and provision of government services.[98]

Depending on its character, an intentional attack on GPS attributed to a terrorist group, nation, or group of nations could be considered a casus belli or act of war. Temporary, localized, reversible non-kinetic effects might not be considered an armed attack and act of war. Longer duration, generalized, or irreversible effects, particularly inflicted by kinetic, directed energy, or nuclear weapons, however, probably would be considered such a hostile act.

Without the common datum grid and time provided by GPS, the ability to execute national defense, homeland security, and intelligence activities which require interoperability, synchronization, or a high degree of accuracy would be reduced. Similarly, America's ability to project power with precision, speed, and lethality would be diminished if GPS services were either corrupted or denied. While the U.S. armed forces could continue to conduct combat operations without GPS, hostilities probably would last longer, cost more, and generate more fatalities, casualties, and collateral damage.

---

[95] Ibid.

[96] Goward, "A billion-Dollar-a-Day GPS Mistake?"

[97] Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures (April 2008), https://apps.dtic.mil/sti/pdfs/ADA484672.pdf. Also see, for example. National Infrastructure Advisory Council, Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation (Washington, D.C.: U.S. Department of Homeland Security, 2018), https://www.cisa.gov/sites/default/files/publications/NIAC%20Catastrophic%20Power%20Outage%20Study_FINAL.pdf; National Commission on Grid Resilience, Grid Resilience: Priorities for the Next Administration, (2020), https://gridresilience.org/wp-content/uploads/2020/11/NCGR-Report-2020-Full-v2.pdf

[98] Federal Emergency Management Agency, "National Essential Functions," 2020, https://www.fema.gov/sites/default/files/2020-07/fema_continuity-brochure_050720.pdf

"The United States must rapidly develop and implement a comprehensive, whole of nation, strategy to redress its asymmetric vulnerability to Navwar and restore U.S. leadership in space-based and terrestrial PNT."

Recommendations

The United States must rapidly develop and implement a comprehensive, whole of nation, strategy to redress its asymmetric vulnerability to Navwar and restore U.S. leadership in space-based and terrestrial PNT. Such a comprehensive approach would necessarily involve federal, state, local, and tribal governments as well as the private sector. The breadth and depth of dependence upon GPS and the system's vulnerabilities cannot be addressed solely by the federal government given that most critical infrastructures are owned and operated by private enterprises.

"Focused leadership, properly empowered and resourced, is essential to the national PNT strategy's success."

Such a comprehensive national strategy must address PNT capability shortfalls and mitigate vulnerabilities to plausible threats. Consequently, it must address all GPS segments, augmentation, and alternatives to provide reliable and resilient PNT services which will protect national, homeland, and economic security. To achieve those objectives, **the President should promulgate a national PNT strategy and implementation plan which urgently directs the following courses of action and Congress should provide adequate resources for the plan's execution:**

- **DoD, DHS, and DoT should continue to resource the identification and assessment of GPS dependencies, interdependencies, and vulnerabilities** in collaboration with the national security, homeland security, and transportation, maritime, and aviation safety industrial bases.

- **DoT should resource the development, procurement, fielding, operation, and sustainment of modern, secure, and robust civilian GPS signals.** This includes L1C, L2C and L5 civilian signals with advanced modulations and dataless channels for enhanced anti-jam capability, dual frequency coded civilian signals, civilian signal integrity monitoring and authentication, and a high accuracy civilian service.

- **DHS, DoT, DoC, in consultation with the Federal Communications Commission, the Federal Energy Regulatory Commission, and the private sector, should develop regulatory requirements and financial incentives for critical infrastructure owners and operators to employ more than a single source of precise PNT, UE which are resistant to cyber, EW jamming and spoofing,** and other means of interference in their critical infrastructures and associated applications, **and the capability to sustain normal operations for at least thirty days in the event of an extended space-based PNT service disruption.**

- **The Department of State and DoC should reform export control regulations to allow U.S. firms to sell adaptive antenna technology** for protection against interference and signal manipulation to civilian users, especially airlines, while maintaining critical national security anti-jam/anti-spoof controls.

- **DoD should urgently resource and accelerate the acquisition, deployment, operation, and sustainment of cyber and radiation hardened GPS IIIF or other spacecraft with higher power, reprogrammable digital payloads, and M-code signals to rapidly improve the GPS constellation's resilience, direct measures to accelerate and complete the OCX program, rapidly deploy and integrate multi-GNSS UE into U.S. force structure, and synchronize GPS segments.**

- **DoD should resource the development, procurement, deployment, operation, and sustainment of a dynamic, layered, space defense-in-depth** with a mix of passive and active measures to counter adversary ASAT and counterspace weapons systems.

- **The Department of State, DoD, and DoT should pursue international cooperation with Europe, Australia, Japan, and India to establish compatible, interoperable, and trusted GNSS services** utilizing GPS, Galileo, QZSS, and the Indian Regional Navigation Satellite System as a tool of foreign relations to strengthen international security as well as countervail China's use of Beidou to induce more international partners to participate in its Space Silk Road Initiative.

- **DoT, DHS, and DoC should work with the private sector to develop, field, operate, and sustain multiple complementary terrestrial PNT services** leveraging fiber optic, wireless, and other advanced technology to augment and backup GPS, increase the resilience of PNT services, and enhance national, homeland, and economic security. The first step, which should be achieved as soon as possible, is the acquisition of such services to protect federal systems and applications.

Focused leadership, properly empowered and resourced, is essential to the national PNT strategy's success.

Conclusion

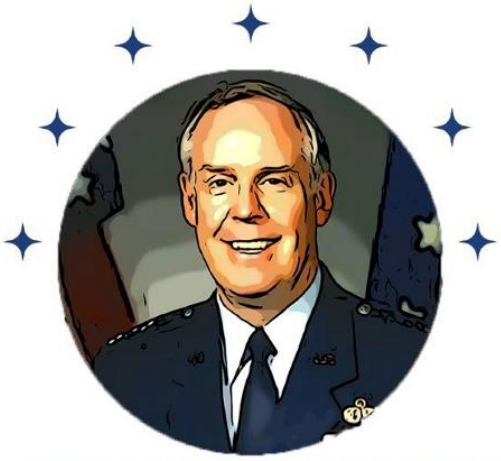
The United States has lost its position as owner and operator of the world's premier space-based PNT system, is overdependent upon the use of GPS for national security, homeland security, and economic security, has no reliable and resilient terrestrial backups to GPS, and has an asymmetric vulnerability to Navwar. Consequently, **America's critical infrastructures, national essential functions, and military forces are at grave risk.** Navwar operations against the system could have significant consequences for all elements of U.S. national power with severe political, socioeconomic, and security impacts upon the nation's status, influence, prosperity, and security.

Mitigating America's asymmetric vulnerability to Navwar and reestablishing U.S. leadership in space-based PNT should not be a polarizing or partisan political issue. While transparent and taken for granted by most Americans, reliable and resilient PNT services directly impact their well-being and security. **Significant disruption or loss of PNT services would be a catastrophe.** Despite executive and statutory direction over decades to address this problem, it remains unresolved. **Decisive leadership and swift action by both the Executive and Legislative Branches of the U.S. government are required to develop and execute a comprehensive strategy and implementation plan which will redress PNT capability shortfalls and mitigate vulnerabilities.** This should include focused and empowered leadership as well as the aforementioned courses of action and adequate resources to provide reliable and resilient PNT services to protect national, homeland, and economic security.

Marc J. Berkowitz is a member of the National Security Space Association's Advisory Board and an independent advisor to public and private sector clients. Previously, he served as the Assistant Deputy Under Secretary of Defense for Space Policy and Vice President for Strategic Planning at Lockheed Martin Corporation.

The views expressed herein are solely those of the author and do not reflect the views of the Association or its member companies.

We thank the Resilient Navigation and Timing Foundation for their sponsorship. We also thank you, our valued members, for your continued support of NSSA and the preservation and advancement of the national security space enterprise.



NATIONAL SECURITY SPACE ASSOCIATION
MOORMAN CENTER FOR SPACE STUDIES

NSSA is the only U.S. trade association dedicated solely to promoting the health and vitality of the U.S. national security space enterprise (Title 10 and Title 50) and its supporting industry partners. For more information, including how to join the Association, please visit us at www.nssaspace.org.