NSI BACKGROUNDER

DECEMBER 2020

BEYOND GPS:
THE FRONTIER OF POSITIONING, NAVIGATION, AND TIMING SERVICES

By LORI GORDON AND BRYAN SMITH

THIS NSI BACKGROUNDER

1. **DESCRIBES** GPS' critical role and vulnerabilities in supporting national defense and critical infrastructure.
2. **MAPS** the policy and legislative direction for enhancing PNT resilience.
3. **CHARACTERIZES** contrasting industrial policies for improving GPS resilience and developing alternative PNT technologies.
4. **IDENTIFIES** key items to watch in the future.

GPS DEPENDENCIES, VULNERABILITIES & ALTERNATIVES

- **GPS' Critical Role.** The U.S. Global Positioning System (GPS) is a network currently made up of 31 medium earth orbit (MEO) satellites and multiple ground stations operated by the Department of Defense (DoD) that provides Positioning, Navigation, & Timing (PNT) services as a free, global utility.[1]
  - GPS is critical to U.S. and international safety, security, and prosperity and is used by billions of worldwide users in aviation, maritime, finance, electricity, mining, transport, telecommunications, and other sectors.[2]
  - GPS is also critical to U.S. and allied precision weapons systems, navigation, communications, and a wide array of other military functions.
  - If GPS were disrupted for an extended period, it would have a debilitating effect on national security, economic security, and public health and safety.[3] Moreover, new threats to GPS are continually emerging.

Lori Gordon is a Visiting Fellow at the National Security Institute at at George Mason University's Antonin Scalia Law School. She currently serves as the Civil Systems Protection Lead at The Aerospace Corporation, specializing in national and homeland security, cybersecurity, and infrastructure protection and leads a strategic initiative in PNT resilience. She is also an advisor to ISO, ANSI, and NIST technical working groups on topics ranging from commercial space standards to cybersecurity workforce to unmanned aerial systems.

Bryan Smith is a Senior Fellow at the National Security Institute at George Mason University's Antonin Scalia Law School. He held senior career positions in the government in national security and was a staff member of the House and Senate Intelligence Committees. He currently provides advisory services to industry, including in the PNT arena.

- **GPS Vulnerabilities.** GPS utilizes a weak signal that is subject to outage and denial,[4] including from environmental degradation; unintentional interference such as adjacent band spectrum interference; or intentional interference, such as hostile jamming, spoofing, or kinetic attack.[5]
  - In particular, jamming and spoofing equipment can be inexpensive and tactics involving this equipment are widely available—enabling adversarial exploitation of GPS signals through denial or manipulation of PNT data, and putting military operators and civil and commercial National Critical Infrastructure at risk.[6]
  - Notably, Russia has spoofed GPS to conceal leadership operations' movements in Russia, and disguise military operations in Syria and Crimea.[7]
- **PNT Alternatives.** Alternative sources of PNT include terrestrial beaconing systems, time-over-fiber, cellular and wireless signals, local terrestrial systems, and proliferated low earth orbit (LEO) satellite systems.[8]
  - These various alternatives have different strengths and limitations, and represent a range of technological maturity. Nonetheless, the Department of Homeland Security (DHS) has observed that several industry systems in commercial use may meet timing requirements for U.S. critical infrastructure.[9]
  - However, these systems have not been widely adopted, so the goal of establishing true PNT resiliency lies ahead.

U.S. POLICY DIRECTION

Beginning in 2004 with National Security Policy Directive (NSPD) -39 and accelerating in recent years, a series of Presidential Policy Directives, legislative actions, and Executive Orders have attempted to reduce GPS vulnerabilities and offer back-up PNT alternatives across the government and critical infrastructure sectors.

- **GPS Resiliency.** Beginning with NSPD-39, DoD's main focus has been on enhancing GPS resiliency itself rather than deploying altPNT capability.
  - The Air Force has invested over $2.0 billion in R&D to develop an "M-code" signal to enhance GPS's power, security, and jam-resistant features. It plans on investing another $500 million to integrate M-code on additional platforms.[10]
- **GPS Back-Ups.**
  - NSPD-39 directed the Department of Transportation (DoT) to establish and operate a GPS back-up for critical infrastructure. The FY 2017 and 2018 NDAAs (Sections 1618 and 1606 respectively) pushed DoD, DoT, and DHS to assess their PNT needs, identify GPS alternatives, and ultimately to demonstrate effective back-up and complementary PNT capabilities for critical infrastructure and national security activities. These directives were all agnostic concerning the particular technology solution pursued.
  - The National Timing Resilience and Security Act of 2018 (NTRSA) provides different direction. It specifies thirteen technical requirements for a GPS back-up, which essentially define the E-Loran system. E-Loran is a potential modernized network of the legacy LORAN infrastructure—a radio-based "long range navigation" system deployed in World War II— that would transmit a powerful, low frequency, high-precision timing signal highly resistant to jamming.[11] NTRSA directs DoT to establish this system.
- **Market Solutions.** Executive Order 13905 (2020) promotes a technology-neutral, chiefly market-driven approach to resilient PNT, in which agencies or critical infrastructure sectors determine their technical requirements for GPS alternatives or back-ups and rely on a competitive marketplace to meet them.

NAVIGATING TO GPS ALTERNATIVES

Three basic models have been advanced in different parts of the federal government to provide for increased PNT resiliency.

- **Direct Funding**. DoD is not exclusively focused on GPS enhancements, as the Army is currently funding alternative PNT technologies at about $40 million a year, and about twice that on applying the technologies.[12]
  - Most recently, the Senate's FY 2021 defense authorization bill (Section 1601) directs DoD to increase attention to alternative PNT.[13] This includes developing alternative PNT capability and deploying it on DoD's highest priority platforms and weapons.
  - Additionally, the recently created Space Development Agency is exploring a proliferated low-Earth orbit (LEO) satellite constellation for alternative PNT.[14] Geostationary (GEO) orbits are also in consideration.[15]
- **Public-Private Partnership for a single GPS backup solution.** In NTRSA, Congress authorized the Secretary of Transportation to pursue a public-private partnership (P3) to develop a resilient, land-based government back-up to GPS for timing. The Act, however, is subject to appropriations, which have not been provided.
  - The P3 would allow a private entity to build E-Loran for the government, operate it,[16] and share revenue with the government for the first ten years.
  - NTRSA stipulates that the private entity would assume all financial risk. However, CBO's scoring of this approach does not agree that the P3 would be devoid of risk, and considers it to be the equivalent of a federal acquisition, effectively requiring up front government funding.[17]
- **Diverse commercial systems for diverse resiliency needs.** E.O. 13905 and a subsequent DHS report envision a diversity of commercial alternative PNT services tailored to specific needs of various National Critical Infrastructure (NCI) sectors.
  - DHS has stated that PNT needs for various critical infrastructure functions are so diverse that no single PNT system, including GPS, can fulfill all user requirements and applications. Backups must be application-specific and developed in coordination with sector owners and operators.[18]
  - Accordingly, under E.O. 13905, each NCI sector will determine its unique requirements and rely on the commercial PNT market to meet them. The E.O. envisions no government funding to help infrastructure owners and operators pay for the new services; however, it directs use of federal contracting policy to incentivize adoption.[19]

KEY ITEMS TO WATCH

PNT AND NATIONAL SECURITY

- Whether DoD's substantial efforts to reduce GPS vulnerabilities and deliver GPS alternatives will be successful.
- Whether and how DoD will orient its resilience efforts more in the direction of alternative PNT for national security.
- Whether there are synergies between resilient PNT solutions for national security and critical infrastructure applications, including those used in emergency services and first responder applications, which are operated by both governments and the private sector.

PNT POLICY

- Whether E.O. 13905's market-based approach will be sufficient to induce critical infrastructure operators to procure resilient PNT services, or whether additional regulatory or funding inducements will be necessary.
- How the Executive Branch and Congress will resolve the contrasting approaches to strengthening PNT resiliency.
- Whether, in the future, the Government will perceive a need to provide primary funding to develop, produce, operate, and maintain new PNT systems.

ENDNOTES

1 *See Space Segment*, Nat'l Coordination Office for Space-Based Positioning, Navigation, and Timing, https://www.gps.gov/systems/gps/space/#generations (last modified Nov. 2, 2020). The U.S. GPS is a Global Navigation Satellite System (GNSS), as is the Russian GLONASS, the European Union's Galileo system, and China's BeiDou Navigation Satellite System, India, France, and Japan are also developing regional navigation and augmentation systems. *See* U.N. Office for Outer Space Affairs, *Current and Planned Global and Regional Navigation Satellite Systems and Satellite-based Augmentation Systems,* 13, 19, 30, 41, 51, U.N.. Doc. ST/SPACE/50 (2010), http://www.unoosa.org/pdf/publications/icg_ebook.pdf.
2 Alan C. O'Connor et al., Economic Benefits of the Global Positioning System (GPS) Final Report ES-1, RTI Int'l (June 2019), https://www.rti.org/sites/default/files/gps_finalreport.pdf.
3 *See* Cybersecurity & Infrastructure Sec. Agency, National Security Critical Functions, https://www.cisa.gov/sites/default/files/publications/factsheet_national-critical-functions_508.pdf.
4 GPS is almost a million times weaker than other navigation signals. *See* Jeff Shepard, *eLORAN a Terrestrial Alternative to GPS,* Microcontroller tips (Oct. 26, 2020), https://www.microcontrollertips.com/eloran-a-terrestrial-alternative-to-gps/.
5 U.S. Dep't of Commerce, Draft NISTIR 8323, Cybersecurity Profile for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services, 26 (Oct. 2020), https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8323-draft.pdf.
6 Deborah Lawrence, Fed. Aviation Adm', Presentation to Stanford PNT Symposium (Oct. 2014), http://web.stanford.edu/group/scpnt/pnt/PNT14/2014_Presentation_Files/3.FAA_Navigation_Update-PNT_Symposium.pdf.
7 C4ADS, *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria* 3 (2019), https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf.
8 Cybersecurity and Infrastructure Sec. Agency, Report on Position, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System v (April 8, 2020), https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508.pdf.
9 *Id.* at 5.
10 2 A.F., PE1203164F, Research, Development, Test & Evaluation 391-402 (Feb. 2019), https://www.dacis.com/budget/budget_pdf/FY20/RDTE/F/1203614F_303.pdf.
11 *See* Paul Tullis, *GPS is Easy To Hack, and the U.S. Has No Backup,* Sci. Am. (Dec. 1, 2019), https://www.scientificamerican.com/article/gps-is-easy-to-hack-and-the-u-s-has-no-backup/.
12 1 Army, PE1206120A, Assured Positioning, Navigation and Timing (PNT) 655 (Mar. 2019), https://www.dacis.com/budget/budget_pdf/FY20/RDTE/A/1206120A_107.pdf.
13 Theresa Hitchens, *SASC Wants Alternative GPS By 2023*, Breaking Def. (Jun. 29, 2020), https://breakingdefense.com/2020/06/sasc-wants-alternative-gps-by-2023/.
14 Nathan Strout, *Can hundreds of unrelated satellites create a GPS backup?*, C4ISRNET (Nov. 29, 2019), https://www.c4isrnet.com/battlefield-tech/c2-comms/2019/11/29/can-hundreds-of-unrelated-satellites-create-a-gps-backup/.
15 *Navigation Technology Satellite – 3 (NTS-3),* AFRL, https://afresearchlab.com/technology/space-vehicles/successstories/nts-3 (last visited December 1, 2020).
16 In theory, the private entity would assume financial risk, although this does not always happen in practice.
17 Congressional Budget Office, *Cost Estimate: H.R. 2518* 4-5 (Jun. 23, 2017), https://www.cbo.gov/system/files/115th-congress-2017-2018/costestimate/hr2518.pdf.
18 U.S. Dep't. of Homeland Sec., Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS) V-VI (Apr. 8, 2020), https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508.pdf.
19 Of note, some NCI is government funded, such as Emergency Services.