Defense Matters

National Cybersecurity and National PNT

Are we getting closer? Not really.

Not a day seems to pass without a new report in the news about data breaches, cyber-attacks, and what we need to do to protect ourselves from being hacked, having our identity stolen, and our privacy compromised. These endless reports highlight our constant struggle to block threats from those with bad intentions.

As we march to the drumbeat of absolute reliance on the Internet for nearly everything we do, our smartphones have become the most important item we carry. To leave home without your phone can make for a distressing, frustrating day. Phones are essential for communicating, keeping track of our e-mails, accessing our bank accounts, and knowing where we are and where we are going.

More and more applications are employing password policies that increase the password's strength, with requirements governing password length, required or prohibited character types, and how often a user must change a password (ever more often, it seems). Many applications are implementing a secondary piece of electronic security - multi-factor authentication, which makes our phones even more critical to have with us in order to gain access to our data.

National Cybersecurity Strategy

On 2 March 2023, the Biden Administration released the *2023 National Cybersecurity Strategy.* This strategy replaced the Trump era, *2018 National Cyber Strategy.*

The 2023 strategy was noted to be in development for nearly two years and involved more than 20 government agencies and consultations with a large number of private sector organizations. [Note: In that regard, its developmental duration nearly paralleled the creation of the National PNT Architecture between early 2006 and mid-2008, an effort involving over 30 agencies.]

Development of the Cybersecurity Strategy was initiated by the Biden Administration's May 2021 *Executive Order on Improving the Nation's Cybersecurity.* This Executive Order indicated that the Federal Government must lead by example for the prevention, detection, assessment, and remediation of cyber incidents to protect the nation's digital infrastructure, which is essential to national and economic security.

On page 2 of the Strategy's *Introduction,* under the heading of *Emerging Trends,* there is a discussion on the "deepening digital dependencies" of systems where next-generation interconnectivity is "collapsing the boundary between digital and physical worlds, and exposing some of our most essential systems to disruption."

This passage goes on to state, "Our factories, power grids, and water treatment facilities, among other essential infrastructure, are increasingly shedding old analog control systems and rapidly bringing online digital operational technology."

Missing the PNT Point

It is here that positioning, navigation, and timing (PNT) gets a brief nod in the form of "…space-based assets – including those enabling positioning, navigation, and timing for civilian and military uses…will accelerate this trend, moving many of our essential systems online and making cyberattacks inherently more destructive and impactful."

Unfortunately, the point being made is not that over-reliance on GPS as a source of PNT is the problem, but rather that the emergence of space-based technologies such as GPS are simply creating more digital systems that are PNT reliant.

The assumption that a shift toward such space-based technologies, rather than the explicit reliance on them alone, is making essential infrastructure systems more vulnerable to cyberattacks is the flawed reasoning that skirts the issue.

It is unfortunate that the Administration has missed an opportunity to elevate the need to invest in alternate sources of PNT to address the overreliance on GPS as the single source of PNT. Clearly the phrase PNT as used in this Strategy is just another way of saying GPS; and the bad actors that may seek to disrupt those essential infrastructure systems know that GPS is vulnerable.

Reading further, the 2023 Strategy is built around five pillars: defend critical infrastructure; disrupt and dismantle threats by malicious cyber actors; shape

Doug Taggart
President
Overlook Systems Technologies, Inc.

market forces to drive security and resilience; invest in a resilient future; and forge international partnerships to pursue shared goals.

Those five pillars line up well if the intended focus can be broadened to developing alternate sources of national PNT capability as a way to achieve the desired security and resilience.

It is asserted that for the nation to address these five pillars, two fundamental shifts in the roles, responsibilities, and resources in cyberspace must occur.

The first is that stewardship of the digital ecosystem must shift away from individuals, small businesses, and local governments, and toward organizations that are best positioned to address wider-reaching security and resilience.

The second is characterized as a rebalance of incentives and investments between building a secure and resilient foundation for the future digital ecosystem and defending ourselves against urgent threats of the day.

Again, the "fundamental shift in roles" lines up well if the intended focus of the strategy is to develop alternate sources of national PNT capability.

Looking back on the Trump era 2018 Cyber Strategy, which demonstrated a commitment to a significate agenda on space issues, there was a single reference to PNT (on page 10) where it states, "The Administration is concerned about the growing cyber-related threats to space assets and supporting infrastructure because these assets are critical to functions such as positioning, navigation, and timing (PNT)…" but that mention of GPS reliance was not made in the context of identifying alternatives, but simply recognizing that attacks on GPS were concerning from the perspective of the cyber world.

How the DoD is Proceeding

Looking to the defense side of developing a more robust and resilient PNT capability for the warfighter, a key purpose of the DoD PNT Enterprise strategy released in 2019, is to meet national objectives for improving U.S. global military effectiveness through DoD-wide implementation of not only GPS modernization, but also new integrated PNT applications to augment GPS. The strategy is specifically intended to encourage DoD PNT application designers to use modular, open-system approach techniques to integrate a diverse mix of PNT sources within individual DoD systems based on the operational environments each will be required to face.

Challenges Remain

National defense spending as a percentage of GDP has dropped from 5.8 percent in 1985, the height of the last global competition, to 3.2 percent in 2021.

In addition, in 13 of the past 14 years, the Defense Department has operated under a continuing resolution for part of the year, preventing the new starts essential for modernization. The 2024 White House Funding request for $842 billion in defense funding is noted to be 3.2 percent above the 2023 budget, which is unfortunately still beneath the rate of current inflation. Further, we are in a marketplace where fundamental good practices must compete for resources with shiny new add-ons and the latest features. Instead of using sound engineering principles to build strong, resilient systems, the majority of the money and attention has gone to adding yet another layer of patches and extensions on top of fundamentally broken technologies. Despite those realities, the DoD is paying additional attention to equipage of key Joint Force platforms with modernized GPS equipment and integrated complements using diverse sources of PNT information that ensure functionality should GPS be disrupted.

For the DoD, the PNT end state is straightforward: ensure that our warfighters have robust and resilient PNT-enabled platforms, services, and technologies to maintain operational superiority, never engaging any competitor on an even technological basis.

ION SATELLITE DIVISION

CALL FOR NOMINATIONS

The Johannes Kepler Award

Nominations Due: June 30

Presentation of the Johannes Kepler award takes place at the Satellite Division's Annual ION GNSS+ meeting in September. The purpose of the Kepler Award is to honor an individual for sustained and significant contributions to the development of satellite navigation. All members of the ION are eligible for nomination. A special nominating committee determines the winner of the award, which is presented only when deemed appropriate.

ION members are encouraged to submit nominations for deserving individuals. For complete instructions, or to submit a nomination, go to ion.org/awards, and click on "Kepler" in the left-hand menu. Nominations must be received by June 30.

To view a complete list of previous Kepler Award winners, please visit ion.org/awards/kepleraward.cfm.

Dr. Boris Pervan, 2022 Kepler Award winner. For his pioneering contributions to high-integrity GNSS-based aviation navigation and his dedication to education.