Defense Matters

Positioning, Navigation, and Timing; Cybersecurity; and Spectrum Management

(Planning Mission Success in Modern Warfare)

Doug Taggart
President
Overlook Systems Technologies, Inc.
and ION Fellow
with

Jules McNeff
VP Strategy and Programs

Prologue

As I draft this column in mid-February, our country's federal workforce is experiencing significant shake-ups, impacting both federal employees and federal contractors. The ongoing cuts and workforce reductions initiated by the Department of Government Efficiency (DOGE) raise questions about what the future holds. While the full impact remains unclear, here is a collection of quotes, attributed to Peter Drucker[1], that may be apropos to the uncertainty of what lies ahead.

"The only thing we know about the future is that it will be different."

"Trying to predict the future is like trying to drive down a country road at night with no lights while looking out the back window."

"There is nothing quite so useless as doing with great efficiency, something that should not be done at all."

"Efficiency is doing the thing right. Effectiveness is doing the right thing"

"The best way to predict the future is to create it."

Now to the business at hand – Defense Matters Positioning, Navigation, and Timing, Cybersecurity, and Spectrum Management (Planning Mission Success in Modern Warfare).

Maximizing Mission Success: A Critical Approach to Integrated PNT, Cybersecurity, and Spectrum Management

As military systems grow increasingly reliant on integrated technologies, the convergence of three critical areas—positioning, navigation, and timing (PNT), cybersecurity, and spectrum management—becomes paramount for mission success. To maximize the probability of success, these interconnected domains must not be considered in isolation, but seamlessly integrated as they are foundational to operational effectiveness.

1 Peter Drucker (1909 to 2005) was regarded as the founder of modern management.

This integral relationship was graphically depicted by the Department of Defense in its *Strategy for the DoD PNT Enterprise,* released to the public in 2019. An introductory figure titled "Electronic Foundations of Joint Warfighting" shows Communications (Spectrum), Computers (Cyber), and PNT as the three foundations of the DoD Information Technology (IT) and Cyber Enterprise. Precise PNT from GPS is shown as the catalyst that, since the early 2000's, has enabled warfighters to bridge the notional Command and Control (C2) divide between Reactive Operations, where information latency hinders C2 execution, to Coincident Operations where continuous Situation Awareness with precise position and time enables real-time C2 execution.

The strategy enjoins the entire DoD to adopt a holistic view toward implementation of these foundational elements within the military forces and notes that, while GPS will remain the cornerstone PNT capability for the department, complementary PNT sources must also be employed for flexibility and resilience in integrated PNT applications.

The Imperative of NAVWAR Compliance

This foundational guidance is codified by DoD policy in DoD Instruction 4650.08 (Positioning, Navigation, and Timing (PNT) and Navigation Warfare (NAVWAR) Policy). This policy document states, ***"DoD will use NAVWAR to ensure DoD use of and prevent adversary use of PNT information through coordinated employment of space, cyberspace, and electromagnetic spectrum operations."*** It requires that all DoD systems be equipped to operate in hostile NAVWAR environments and emphasizes that NAVWAR compliance is a non-negotiable requirement in the acquisition of PNT User Equipment (UE).

It mandates that a NAVWAR Compliant PNT system ***"…continues to provide trusted***

PNT information over the time period required by a specific mission at the level of accuracy required by the mission in the expected physical, electromagnetic, and cyber environment."

NAVWAR compliance is the bedrock for ensuring operational reliability and resilience, positioning the U.S. military for success in the face of adversary threats that are designed to exploit vulnerabilities in the PNT domain.

Addressing the Interconnected Challenges

The military's ability to operate in contested environments demands more than just a functional PNT system. It requires a comprehensive approach that integrates PNT, cybersecurity, and spectrum management.

Three key principles of PNT—accuracy, availability, and integrity—are essential benchmarks for evaluating system effectiveness. However, a fully resilient PNT system extends beyond these principles. A resilient PNT system must proactively detect and mitigate interference, identify spoofing attempts, and disregard corrupted data from compromised sources. Beyond the military environment, these capabilities are also foundational to civilian applications, ensuring the safety and security of critical infrastructure, such as power grids, transportation operations, and communication networks, all of which are equally vulnerable to PNT disruptions.

Cybersecurity: The Backbone of Mission Success

In the realm of cybersecurity, a similar set of principles, the CIA Triad—Confidentiality, Integrity, and Availability—serves as a guideline. This model underpins the strategies designed to protect critical systems from both malicious attacks and accidental breaches.

In the context of PNT, which is simultaneously an enabler and a product of computer operations, cybersecurity must be integrated at every level of process monitoring, authentication, and control. Any compromise of mission data or command authority can lead directly to mission failure. Therefore, robust cybersecurity measures are not an optional enhancement but a critical element that ensures the reliability and security of PNT systems, as well as the integrity among the multiple cyber networks supporting military operations.

The Role of Spectrum Integrity

Similarly, protection of the electromagnetic spectrum is no less critical. While the terminology around spectrum management lacks the specificity of PNT or cybersecurity, the radio spectrum plays a fundamental role in supporting both communication and PNT systems.

As adversaries increasingly exploit vulnerabilities in the spectrum—through tactics like frequency jamming or spoofing—military systems become more vulnerable and susceptible to disruption.

Spectrum integrity ensures the reliability of all electronic operations, and its protection is crucial for maintaining interoperability, especially in joint or coalition environments.

To secure mission success, the spectrum must be vigilantly monitored, with mechanisms in place to detect, characterize, attribute, and neutralize interference, whether deliberate or accidental, that could degrade system performance.

> ***"DoD will use NAVWAR to ensure DoD use of and prevent adversary use of PNT information through coordinated employment of space, cyberspace, and electromagnetic spectrum operations."***
>
> It mandates that a NAVWAR Compliant PNT system ***"…continues to provide trusted PNT information over the time period required by a specific mission at the level of accuracy required by the mission in the expected physical, electromagnetic, and cyber environment."***
>
> DoD Instruction 4650.08

Conclusion: Integration is Mandatory

As military operations become ever more dependent on integrated technologies, the ability to consolidate and securely manage the PNT, cyber, and spectrum elements of Information Technology-enabled systems is paramount for mission success.

Achieving NAVWAR Compliance in the acquisition of PNT UE is critical as PNT is a vital enabler in the operations of communications (spectrum management) and computer (cybersecure) systems. Resilience, proactive interference mitigation, and seamless integration across these domains will dictate operational effectiveness and the ability to adapt in the face of evolving threats.

The future success of military operations hinges on the ability to secure these interconnected domains, ultimately providing and maintaining a decisive edge on the battlefield.

Our government leaders have pondered this situation without substantive action for far too long, and we are at the precipice of being late in fielding fully resilient PNT capabilities for both military and civil critical infrastructure applications. Our adversaries are not sitting idly by but, as press reports indicate, are increasing their investments in resilient PNT capabilities, space and terrestrial.

The time for the U.S. to act is now—our future national security and economic prosperity demand nothing less.