

Safeguarding Military Infrastructure and Frameworks: Opportunities and Challenges for Government | West Coast

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Palo Alto, November, 2024

In a recent roundtable, experts from the DoD and industry discussed the various challenges facing cybersecurity frameworks and infrastructure posed by rapid technological advancements. Discussion centered around strategies to secure legacy systems in advance of quantum computing, including improving visibility into assets, consolidating disparate tools, and increasing collaboration between government and industry.

Safeguarding Challenges

The Pace of Technology & Legacy Systems

“Legacy systems were not designed to take the scope, scale, and sophistication of threats that are coming our way.”

Panelists discussed the challenges of securing legacy systems amidst rapid technological change. One participant noted that a single network faces over a million zero-day attacks daily, and emphasized the only way to combat this is with AI and machine learning technologies.

While some panelists note that it's often easier to implement new technology than to augment legacy systems to make them perform in ways they were not designed to, others have found ways to leverage existing capabilities. Ultimately, agencies need to automate repeatable tasks, which will allow analysts to address more complex threats.

Visibility

“We can't secure something we don't know is there.”

Because legacy systems were not designed to withstand the scale and scope of today's threats, vulnerabilities can easily be missed. The innumerable disparate tools and systems that make up cybersecurity ecosystems make it increasingly hard to gain visibility into the network vulnerabilities.

Ensuring data interoperability among disparate tools is also a challenge. Integrating disparate tools to work together so that data and intelligence are accessible is not always possible, and certainly not at the speed needed to match the current pace of technology.

Quantum Computing

“When you put it all together, it’s a huge risk for us. We can’t wait. We have to start getting that encryption put in place.”

Roundtable participants also discussed the threat of quantum computing on existing infrastructure, and the need to fortify existing systems with post-quantum cryptography. Panelists note that although quantum computing is new, agencies cannot wait for official guidance to start safeguarding data.

Some panelists questioned the feasibility of altering existing systems with quantum cryptography, arguing it would require complete redesigns of the physical infrastructure. Others have been able to develop quantum resistant encryption as a feature in existing firewalls, which allows for the flexibility to use different cryptography in the future if necessary.

When approaching quantum cryptography, agencies should follow a strategy to implement changes incrementally. As technology, standards, and policies continue to evolve, agencies need the ability to adapt existing systems. Panelists agree that industry and government must work together to develop quantum solutions and mitigate the inevitable risks ahead.

Safeguarding Strategies

Panelists discussed several strategies agencies can begin taking to safeguard critical infrastructure and cybersecurity frameworks on the heels of quantum computing.


Collaboration

Panelists underscored the importance of collaboration across government and industry to identify and implement solutions to keep pace with technology. Some participants posit that as quantum continues to evolve, partnerships with vendors will become more important as the onus is put on vendors to identify vulnerabilities and ensure solutions meet standards.

Collaboration between government and industry is also critical to develop effective policy around quantum. Clear communication between the two can help develop more effective solutions, educate agencies on new capabilities, and ensure policies are properly aligned.

Participants shared successes with innovation labs to leverage data and AI to streamline processes and enhance efficiency. Another successful model includes a government only group with an industry liaison. These collaborative environments allow agencies to discuss ubiquitous problems and to develop creative solutions. They have already helped foster better collaboration with industry, facilitate policy development for some agencies, and accelerate development of defense strategies.

Although collaboration occurs on many levels, some participants noted that the practicalities of implementing standards, especially in hardware, is often overlooked by those designing solutions or products. The panelist called for a feedback mechanism to ensure the realities of implementation are considered in the design process.



Panelists also shared unique challenges and use cases that industry had not yet encountered, but pointed to the effectiveness of forums, like this roundtable, to connect the right people to address the issue. Vendors, like Palo Alto, collaborate closely with agencies on unique, complex use cases. In some instances, the solutions are then scaled commercially and move the industry forward.

Platform Consolidation

Panelists underscored the importance of a unified platform to improve visibility and better manage and monitor the myriad tools and legacy systems that make up an agency's security network. Panelists shared numerous benefits of operating on a platform including using AI to inspect traffic and identify vulnerabilities across the network, and using ML to conduct future anomaly detection. A platform can also serve as a single source for actionable intelligence to help set policy. Additionally, agencies can more easily add capabilities to a platform instead of developing new products.

Final Thoughts

Participants concluded the discussion by emphasizing the importance of network visibility and integrating systems and tools to prepare for the changes ahead. Panelists also highlighted the importance of training more of the workforce in cybersecurity, and ensuring that tools are intuitive for the end user.

Panelists also note that no matter what technology agencies want to implement within a department, cybersecurity leaders can no longer rely on departments to simply follow best practices to inform development efforts. There must be defined cybersecurity and cyber resilience performance requirements within contracts to help allocate costs and ensure cybersecurity is balanced with all other system requirements.

The Power of Collaboration

Protecting military infrastructure demands seamless collaboration between government and industry. By joining forces, we can develop cutting-edge solutions, craft practical policies, and harness emerging technologies. Innovation labs drive experimentation, while feedback ensures real-world implementation shapes impactful standards. Unified platforms enhance visibility and security, and advanced tools like AI, ML, and automation deliver rapid threat detection and response. Palo Alto Networks empowers this mission by providing integrated cybersecurity platforms and advanced technologies to strengthen defenses and enable rapid, effective responses to evolving threats. Together, we can build resilient, adaptive, and secure systems ready to meet the challenges of today and tomorrow.



LEARN MORE AT: WWW.PALOALTONETWORKS.COM/