Powered by GovExec

Safeguarding Military Infrastructure and Frameworks: Opportunities and Challenges for Government | Southwest

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

A group of Federal experts recently came together to discuss the opportunities and challenges of safeguarding DoD infrastructure against rapidly evolving threats. Discussion centered around the need for increased collaboration between the DoD and industry, as well as the need for significant cultural change within the DoD to effectively safeguard military infrastructure in the future.

Key Challenges with Safeguarding Military Infrastructure

> **“This is a culture and attitude problem. This is not IT management. This is mission management.”**

Cybersecurity Culture

Panelists kicked off the discussion by sharing cultural challenges they’ve encountered with managing cybersecurity risk in the DoD. They also discussed the impact culture has on implementing critical next gen technology that will help safeguard the nation.

Ultimately, panelists argue that cybersecurity must be viewed differently now than it did even a year ago. Threats have accelerated, and therefore cybersecurity risks are now mission-related risks and should be prioritized as such. However, due to the lack of digital and cyber literacy among senior leaders, existing cybersecurity resources and processes remain inadequate to effectively safeguard the nation’s infrastructure.

Panelists underscore the need for a paradigm change on how cybersecurity is prioritized and operationalized throughout government, not only the DoD. Currently, a top-down approach is used where edicts are issued from the top without providing the necessary resources to effectively implement, which forces agencies to reprioritize initiatives to remain in compliance.

Some panelists proposed an alternative approach where resources and reference implementation are provided upfront to empower IT leaders to make decisions based on their specific mission and risk profile. This reframe could lead to more effective cybersecurity implementation and more effective protection.

Cybersecurity Tradecraft

> **“The cybersecurity field lacks the level of sophisticated tradecraft seen in other areas of national security.”**

Roundtable participants discussed the need for skilled cybersecurity professionals in government. One panelist noted that the bar to enter the cybersecurity profession is low, which makes it difficult to determine if the capabilities of a new hire will be a threat to the organization.

Panelists underscore the need for personnel to know the network well enough to identify and trace anomalies in the network – a skill that is currently lacking. Panelists are also investing more in cybersecurity training for software developers to ensure better integration of cybersecurity in the development stage. Participants note a general shortage of frontline cyber defenders in agencies.

Additionally, panelists discussed the critical need for AI to assist with threat detection and protection. Massive amounts of data are flooding networks, making it impossible for human analysts to identify and respond to every threat. Panelists note that the emergence of quantum computing will further exacerbate this issue.

Implementing AI

> **“Being proactive with cybersecurity is critical. Otherwise, we sit and wait to be told that something bad is happening – and that's a choice. When you’re competing with a peer nation, you have to run with risk.”**

Participants discussed the need to balance the level of security with user experience. Security protocols should not be so cumbersome that they hinder users from doing their jobs effectively. However, training and improved user awareness is a key component of better user behavior and acceptance of security culture.

As technology evolves and AI proliferates cybersecurity, panelists underscore the importance of training personnel to assess the accuracy of AI-generated data to distinguish between real and false information. This additional cultural shift is necessary to ensure AI is used responsibly and infrastructure remains secure.

Panelists also discussed the need to better educate leaders on AI, noting that what is often requested as “AI” is actually process automation. This disconnect in understanding and expectations makes it challenging to prove the value of and move forward with critical new innovations.

The discussion continued with panelists raising questions about the decision-makers of AI implementation within the complex hierarchy of government. Some on the panel believe AI implementation requires a combined top-down and bottom-up approach involving top-down directives and the input from those directly involved in the work. The current inconsistency in decision-making across government creates challenges for industry partners to navigate.

Information Sharing

> **There are a lot of cultural touchstones we have to move past. Culturally, we over classify way too much information, and the information isn't even classified.**

Panelists continued by discussing how overclassification and a reluctance to share information is limiting the effectiveness of cybersecurity efforts. To fast-track AI adoption, one panelist suggested utilizing existing tools to share machine data and meta data in the cloud to accelerate computing and AI. The metadata would, in theory, not contain sensitive information and would be relatively low risk. Another panelist raised concerns with this approach, noting that some critical infrastructure strictly uses meta data to operate.

Ultimately, panelists underscore the importance of proper oversight of AI as systems are being built and recommend using test networks to prove out AI solutions with real data before going live to mitigate risk.

Key Opportunities to Safeguard Cybersecurity

> **“We have to use the same systems our adversaries are using.”**

AI and Automation

Panelists described recent cyberattacks moving faster than ever before. For instance, panelists are witnessing lateral movements within compromised systems happening in hours compared to days. This change has occurred only in the past year, which further illustrates the impact of AI-generated threats. The need for AI-powered active protection is urgent, as traditional detection approaches are no longer sufficient.

> **“Detection is no longer good enough. You have to have active prevention methods throughout your entire cybersecurity portfolio.”**

Because threats are rapidly increasing, panelists question if it’s more of a risk not to leverage AI systems than it is to wait for fully vetted systems. In response, panelists emphasized the need for assurances on mission outcomes before leadership will buy into AI. Leaders need assurance that data is accurate, and that LLMs have not been breached. There is still a concern with the validity of data provided by AI, and whether it can be trusted to make decisions.

Collaboration

> **“If this country is going to win the next conflict, it will be because of industry-military partnership.”**

Panelists concluded the roundtable discussion by emphasizing the importance of industry partnerships for the DoD to stay ahead of evolving cyber threats. As technology continues to evolve, panelists believe that tech innovation will shift further away from the military and into industry, simply because the military is too slow to innovate. Panelists discussed the importance of incentivizing industry partners, and especially small businesses, to solve government problems through funding and tax breaks.

Panelists also discussed the need for improved training programs, including vendor-provided training and collective sessions involving multiple vendors, to ensure personnel can effectively use and integrate different security tools and platforms.

Final Thoughts

In closing, the panel discussion highlighted the importance of a proactive, integrated approach to cybersecurity that aligns with Palo Alto Networks' mission of fostering collaboration with the government to strengthen national security. By shifting security left in the development lifecycle, leveraging existing infrastructure, and improving user experience, we can enhance resilience without adding unnecessary complexity. Conditional access controls, browser-based security innovations, and automation powered by AI are critical tools for building a robust defense against modern threats. Additionally, consolidating the cyber footprint into unified policy enforcement points not only enhances visibility but also empowers rapid, intelligent responses to evolving threats. Together, through collaboration and innovation, we can advance a safer, more secure digital ecosystem for all.

LEARN MORE AT: WWW.PALOALTONETWORKS.COM/