

Safeguarding Military Infrastructure and Frameworks: Opportunities and Challenges | Northeast

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

In a recent roundtable discussion, Federal experts discuss the challenges of securing the ever-changing digital battlefield and the opportunities new technology grants agencies to safeguard infrastructure and frameworks.

Safeguarding Challenges

A Changing Digital Battlefield

“It's just totally different now. The security perimeter is just completely different. There are no perimeters. Perimeters are every place a decision needs to be made.”

Throughout the discussion, participants referenced the ever-changing, dynamic nature of today's digital battlefield. Attack surfaces are expanding exponentially into IoT and devices, and there are increasingly more ways for adversaries to gain access to a network. Not only is the attack surface expanding, the volume and speed of attacks are accelerating at rates humans cannot keep pace with.

Panelists remark on the different tactics adversaries are now deploying on the digital battlefield. For instance, adversaries may target data center chillers just as easily as a network. Agencies must also consider these second or third order cyber threats.

“We see the cyber landscape and the information sharing landscape literally change on a daily basis depending on where we're operating around the globe.”

Panelists also comment on the prevalence of hidden domains and the potential threats they pose to networks. Analysts are finding that behind some commonly used sites are connections to 40 to 60 other domains, all with trackers.

One panelist noted the ease at which adversaries are able to gain insight into day-to-day processes and patterns of life simply by monitoring IoT. Several panelists question whether the traditional separation across network boundaries is an effective form of security as end users increasingly rely on mobile devices and IoT. Protecting this expanding, complicated surface and responding to thousands of alerts daily requires automation.

“What we're facing now is machine speed. It's moving so fast that a human could never hope to keep up.”

Panelists note the amount of data that agencies need to consume, use, and move at the tactical edge has increased exponentially in recent years. Drones, cameras, and other surveillance technology are capable of capturing vast amounts of data and potential intelligence. Data is freely passing through devices, WiFi and wired connections, reflecting innumerable access points that must be secured.

Ultimately, the DoD must be able to operate smoothly in a potential conflict or crises, which requires all levels of classified data to move in any direction, yet remain secure while doing so. To achieve this balancing act, agencies must have full visibility into their cyber environment.

The Human Factor

“It's the end user. It's one person that can screw up every single security thing we're talking about. We can make machines faster. We can make them more secure. But it's common human behavior that we have to adapt to.”

Alongside changing technology is changing human behavior. Panelists remark on the cultural differences of the new generation of warfighters compared to twenty years ago. The new generation is always connected to the internet, which brings another set of challenges to securing the digital battlefield. While younger warfighters may be more tech savvy, panelists note that they're also more naive to the threats brought by constant connection.

One panelist recommends embracing the cultural traits of an always-on generation and adapting security strategies rather than forcing non-digital behavior change on an entire generation. Panelists contend that many younger warfighters do not appreciate the impact of their digital footprint, and the vast amounts of intelligence that can be gleaned from adversaries from the simple act of turning on a cell phone.

“Digital footprints are everywhere. Everything we're doing has a digital footprint.”

The challenge is building these secure capabilities on top of technology that was never designed to be secure from the beginning, and to create a security foundation that is hyper resilient. Ultimately, the focus should be on user outcomes and ensuring security does not interfere with achieving the mission.

Policy and Legal Barriers

Panelists describe instances where modernization efforts stall because of contractual obligations with vendors. Additionally, policies often do not keep pace with the rate of technology change.

“The initiative sort of died on the unwanted efforts of the legal teams, despite the fact that the engineers and industry wanted to work the problem.”

Safeguarding Solutions

Dynamic Networking

“Anything from the physical layer all the way up to the cyber security or data layer has to consistently keep changing to respond to any threat environment.”

Panelists discuss the need for dynamic and adaptable networks that can self-heal to maintain security and prevent single points of failure. Continuously changing and adapting networks can keep the adversaries off their guard. Panelists mentioned using decoy networks to detract adversaries from the main network, and utilizing a diversity of applications. However, these strategies do come with the risk of maintaining multiple systems, networks, and applications.

Panelists also raised the concept of chaos engineering to test how networks and systems respond to failures or disruptions. Although this process is resource intensive, panelists would rather experience failure in a controlled environment. Panelists acknowledge that most have been approaching cybersecurity one zero trust pillar at a time, and not focusing on how to make the pillars interoperable.

Data-Centric Approach

The panelists agree that the traditional approach to security, which relies on network boundaries, is no longer effective due to the vast amounts of data that needs protecting across an endless perimeter.

“You need visibility. Whether it's network, code, IT or OT devices. Visibility is critical data.”

They suggest that a data-centric approach to security is needed, which focuses on protecting data at all stages of the life cycle regardless of where it is located and grants agencies more visibility into their security.

Panelists note that how technology processes data inherently exposes it, and acknowledge that agencies need to work to make data harder to get to. However, panelists caution isolating too much data for the sake of security. The more complex a network, the higher the propensity for users to subvert controls. Current data centric security strategies are not yet effective because the right technology is not in place, and existing physical infrastructure and data constructs are not adequate.

Panelists underscore the importance of moving to a machine state. One panelist stated that “the good news is that with more data, the better technology can detect anomalies that subvert isolation challenges”.



Industry Collaboration

“We never go into conflict alone. As those partners come and go, how do we make the flow of information faster?”

Participants highlighted the critical role of collaboration between industry and government in addressing these challenges. Certain initiatives have already demonstrated significant value in helping agencies achieve broader visibility into cybersecurity as a whole.

However, industry collaboration must also extend beyond companies with complementary services and products. Panelists agree that industry competitors must work collaboratively to ensure solutions are effectively integrated. Panelists shared experiences where vendors are hesitant or unwilling to move forward with a solution due to perceived competition.

Workforce Development


“The most powerful thing to do is sit somebody down and show them how fast this happens. Show them what the stakes are when cyber hygiene is not there.”

The panelists also discuss the importance of educating the next generation of cybersecurity leaders. They agree that the younger generation is more digitally savvy than previous generations, but they may also be more vulnerable to cyberattacks. Panelists note that senior leaders are just as susceptible. Participants shared that useful fiction and scenario planning has been especially effective in educating the workforce on threats and what it takes to remediate actions.

Another panelist shared that they've had success training staff who are relatively inexperienced in cybersecurity to use advanced technology to go after targeted “low-hanging fruit” vulnerabilities. They gave an example of using a tool to patch all cameras on a network and automatically apply policies to any new cameras added to the network, demonstrating how certain tools and newly trained staff can make a significant impact on security.

AI, ML, and Automation for Threat Detection

“Every day the SOC has to be smarter than it was the day before, because every attack you saw today I guarantee you're going to see it tomorrow.”



Panelists continued the discussion by sharing the many current and future opportunities agencies have to safeguard systems with automation. Agencies need an AI application that can analyze a network and understand what behaviors are normal to automatically detect anomalies in places that appear to be trusted.

Moreover, there are dozens of alerts correlated to a single attack that no human can analyze effectively or quickly enough. As a panelist stated, “automation is the only way to do it.” If SOCs aren’t equipped with tools that enable this type of correlation, agencies will not be able to keep up with the pace of threats. Some panelists question how agencies can use AI to come up with more creative solutions, just as a junior analyst might do.

“The static nature of our networks is a fundamental flaw. Until we can figure out how to build them up and tear them down at the speed of seconds, we're going to be on the back foot. Artificial intelligence is just as capable on the offensive side as it is on the defense side.”

Conclusion

In conclusion, the collaboration between industry leaders, such as those in Palo Alto, and government agencies is pivotal to successfully integrating AI into enterprise systems. While the risks of adopting this transformative technology are real, the expertise and innovation provided by industry partners can help automate security and address emerging threats effectively. As one panelist aptly stated, “just the act of doing things differently is worth something for the mission.” By embracing new approaches and fostering strong public-private partnerships, agencies can ensure they stay ahead in an ever-evolving landscape.



LEARN MORE AT: WWW.PALOALTONETWORKS.COM/