AI & The Modern SOC: Winning Tomorrow’s Cyber Mission Through Advanced Capabilities

Highlights from a private government roundtable, hosted by the Advanced Technology Academic Research Center (ATARC), in partnership with Palo Alto Networks, July 2023

Agencies and industry partners in the federal cyber mission are facing more challenges than ever. From staffing and talent shortages to an continually-expanding attack surface, securing systems while achieving the cyber mission is increasingly more complicated as AI technology enters the mainstream.

IT and security leaders must support the changing business demands of their agency while modernizing foundational technology. Given the speed and urgency of the government’s cyber mission, modern Security Operations Centers (SOCs) are being designed and deployed to address this head-on.

Advanced AI will radically change the nature of government operations, policy and security, including changing the capabilities of human teams. In a recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Palo Alto Networks, federal experts discussed what it will take to win tomorrow’s cyber mission.

The Need for AI Governance

Roundtable participants are eagerly anticipating guidance to standardize AI governance. Despite the current lack of formal governance, all agencies on the panel are addressing AI in one way or another. Some agencies already have AI ethics committees in place which review all use cases prior to the deployment or utilization of AI within the agency. Others are simply prohibiting the use of generative AI on government devices.

The urgent need for AI governance is evidenced by the numerous anticipated challenges already plaguing agency leaders. The prevalence of synthetic content is particularly concerning due to the evidentiary challenges this will pose to law enforcement agencies and court systems.

Another challenge is the inadvertent collection of personal or protected data by the government and the interoperability of this data among other federal agencies. Participants agree there must be guardrails in place to ensure AI is used in a way that protects privacy and civil liberties without stifling innovation. Doing so requires a concerted effort to educate the workforce on AI technology, and the ethical considerations involved with its use.

One participant liken the AI challenges facing government today with the issues that arose with the emergence of social media: “Everybody was using their personal devices. Work was bleeding into their personal life. All manner of vulnerability and violation was taking place.” Participants agree the government must embrace AI technology in a more ethical manner than they did with social media.

> “Artificial intelligence should create efficiency. It’s not a replacement.”

The Importance of Workforce Training

Approaching AI integration within the workforce starts with determining what aspects of work can be automated. Whether that’s through help desk automation, reduction in training time or freeing up workers to focus on more complex and interesting work, AI should be used to augment human capabilities, not to replace them.

At this point in time, workforce training is critically important not only to innovate and adopt new technology, but also to ensure agencies remain guarded from advancing threats. One participant notes that the nature of cyber warfare is changing as threat capabilities rapidly advance alongside AI technology.

Unfortunately, many roundtable participants are struggling to shift the narrative of AI within the federal workforce. Either leadership has a fantastical understanding of the true nature of AI or there is utter resistance to introducing and utilizing AI. In either case, workforce training is needed so AI can be used effectively and ethically within government organizations.

AI and Data Sharing

AI is designed to identify data patterns and trends that may not be visible to human analysis, especially in cybersecurity. While this could lead to new insights and discoveries, it also raises the risk of sensitive information being leaked. There is an obvious tension between the need to share government data and the need to protect sensitive information. It’s unclear how agencies should approach data governance with AI. Panelists emphasize the need for clear sharing guidelines while protecting sensitive data in a new era where so much data is being used to train AI models.

It’s unclear how agencies are to harness the power of their data to train AI models- what data to use, but also how to use it. Should each agency train a unique AI model using its own data? Is there a larger government model all agencies use? How will sensitive, proprietary or classified information be used? Roundtable participants urge industry partners to share guidance in addressing these realities.

> "Does all of that data need to get synthesized together? Probably not.”

Policy Keeping Up with Innovation

Roundtable participants are concerned that the government’s policies and procedures may not be able to keep up with the pace of AI innovation. AI is quickly being woven into the fabric of society, much like social media has over the past decade. In order to take advantage of the AI's benefits, policymakers must act quickly.

> **“It's going to be a machine-versus-machine war coming up in cyber.”**

Another important reason the government must act on AI legislation is the simple fact that adversaries are not slowing down. They are continually looking at ways to leverage AI to attack government networks. AI has enormous potential to improve cybersecurity by identifying and blocking malicious activity much more effectively than humans.

Despite the clear need to adopt AI technology, agencies are challenged by slow and ineffective acquisition processes. Panelists note that it’s difficult to communicate their specific need for AI to acquisition teams, as they may not be familiar with AI or understand the benefit of such technology. Panelists question the AI acquisition process in general, wondering whether every agency must purchase their own solution, wait for government-wide guidance, or engage with a Center for Excellence. This is another area where vendors and industry partners could assist agencies with writing requirements and proposals.

AI and the Mission

> **"There is a humongous appetite for AI without an understanding of what AI actually is."**

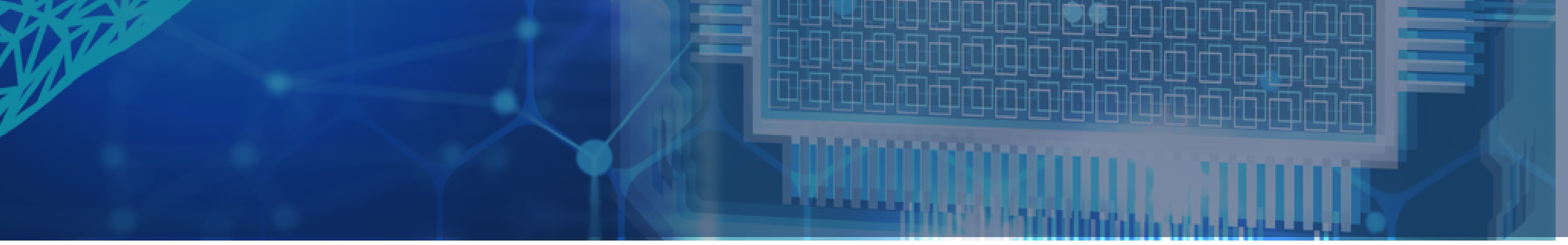
Bridging the gap between the executive leadership's appetite for AI and the reality of the government's current data situation is a challenge all panelists are facing. Many people, including agency leadership, do not understand AI’s full capabilities, and often conflate AI with a fix-all solution. One panelist cautions that while AI is a powerful tool, it’s not a silver bullet. Agencies must not only continue to modernize legacy systems, but also build platforms and infrastructure to accommodate AI technology across the government.

> **“How do I build a platform that can leverage the capabilities of AI and integrate it to make it sustainable and maintainable, while also keeping in mind the mission?”**

This is a complex task that requires the integration of different data sources and AI algorithms. But panelists remain optimistic that as they continue to clean data and build out their foundations for modernization, AI integration will be possible and operations will improve over time.

Ways to Improve SOC Operations

Panelists discussed a number of ways to improve SOC operations, including automation, inventory management, metric tracking and access identity access management. AI can be used to augment some of the tasks that are currently performed by SOC analysts, which would allow analysts to focus on more complex and critical tasks that require human judgment.



Because agencies are operating in a cloud environment with countless connections, SOCs are very complicated. Panelists recommend that agencies conduct a thorough inventory of all devices and software and turn off access based on utilization rates. This level of visibility can also help leaders determine where AI can be used in their particular agency.

One panelist raised a concern with putting trust in an AI solution created by a vendor, and whether the AI model would work optimally in a different environment from where it was trained. This results in agencies putting blind faith in a vendor's ability to train an AI model to act correctly within a specific context. This could lead to significant cybersecurity issues.

Because AI models learn and adapt over time, agencies may need to continually test, evaluate and possibly retrain AI to stay within the guardrails initially established. Similarly, agencies will also need to explain why an AI model made a particular decision, like blocking a transaction or denying access. This is not only important for regulatory purposes, but also to fully understand and trust the AI system.

Final Thoughts

- Agencies must take a holistic approach to managing AI. AI is not a single solution, but rather a collection of technologies that need to be integrated and managed together in a new and different way than traditional IT.
- AI is still in the early stages of development. There is still a lot of work to be done to improve the accuracy and reliability of AI models.
- It's critically important to train and educate human operators on what AI truly is, the implications of AI, and how to use AI effectively and ethically. The workforce must practice using AI in order for the technology to be effective.
- Agencies must have a clear understanding of the data that's being used in AI models.
- Agencies need governance structures, guardrails, oversight committees, and other policies to ensure AI technology is used in a responsible and ethical manner.

LEARN MORE ABOUT MARKET-LEADING SOLUTIONS FROM PALO ALTO NETWORKS

HTTPS://WWW.PALOALTONETWORKS.COM/