Cybersecurity and Artificial Intelligence - Transforming the U.S. Government

Highlights from a Roundtable, hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Palo Alto Networks, October 2023

In recent months, Artificial Intelligence (AI) has become a prominent and vital solution to mounting cybersecurity challenges in the Federal government. AI is drastically and quickly shifting the cybersecurity landscape, which is thrusting federal agencies to the forefront of innovation like never before. Neglecting to innovate risks missed opportunities and increased cybersecurity vulnerabilities.

The Advanced Technology Academic Research Center (ATARC), in partnership with Palo Alto Networks, hosted a roundtable of federal experts to discuss the complex challenges AI brings.

Approaches to AI and Cybersecurity

Panelists noted that AI can be used as a tool to help agencies detect and intercept threats, but it can also pose a significant risk to agencies. Agencies are considering how best to evaluate and monitor threats in AI systems while balancing the sheer utility of AI in a fast-moving world.

Although AI comes with huge promises, concerns around security are vast and complex. Adversaries are constantly evolving their threat capabilities with AI. As such, agencies are striving to maintain a proactive posture with real-time network security to anticipate threats and automate responses.

> **"If we don't have a system in place to handle the threats coming from AI-derived threat actors, we're going to be in a world of hurt."**

To do this, agencies are turning to partners like Palo Alto Networks that are capable of detecting anomalous behavior and taking mitigating actions automatically. With the voracious speed and severity of cyber attacks, agencies do not have time to wait for human detection, analysis or intervention. AI cybersecurity systems will automatically identify anything outside of normal behavior based on rule sets determined by the agency.

Data Quality and Governance

> **"AI is nothing without data, and data is nothing without security."**

AI's great potential hinges on having high-quality data. Data is the throughline for effective, ethical and secure AI use in government. Agencies must take considerable care with data cleansing and tagging data to force the ethical, lawful and governable use of algorithms. If this is not carefully applied, then agencies will run into problems with biased data and inaccurate AI outputs.

Panelists noted that data quality also depends on the use case. Agencies must ensure their datasets are secure, accurate and standardized across the organization. Many agencies are working on data cleansing efforts, including standardizing nomenclature, taxonomy, acronyms, addresses and glossaries across all divisions. However, this requires a level of data literacy among the workforce.

Regarding to data quality, panelists consider the data's ontology, whether system-generated or process-generated errors exist in the data, how the data was validated and if there were any internal errors introduced. Ultimately, the success of AI comes down to the reliability, completeness and accuracy of source data.

The panel also discussed the challenges with data bias. One panelist noted that because everyone's data is biased, ethics will become a part of everyone's job. Agencies must have a conversation about the level of bias they are willing to accept in their data, and develop strategies to counteract known bias in the outputs.

Data Governance

One panelist shared the data governance strategy they use with AI models. They spend a large amount of time cleansing the data based on data requirements. They map those data elements to a conceptual data model down to a logical data model, where they again check the data against requirements. This governance metadata is then applied to the physical data model, which is where they run the actual data. The data is distributed according to governance attributes, which requires an identity management system to authenticate and authorize users for access.

Workforce Training and Culture Shifts

Multiple panelists noted the need for a shift in workforce culture for AI to be successfully implemented in government. Additionally, agencies will need to hire a mix of skill sets that are capable of developing innovative solutions to complex ethical and cybersecurity concerns surrounding AI.

Panelists suggested that in the future, agencies will be able to use AI systems to ask complex data questions that are currently being answered by technologists. While agencies are not interested in replacing people with technology, they are considering how to best train and reskill employees to utilize AI in effective, meaningful and strategic ways. Panelists believe that future agency talent will be a skilled mix of diverse, creative and analytical minds capable of harnessing AI to solve problems.

Agencies will also need to start looking at cybersecurity through a different lens, which will require a different level of collaboration and skill than is currently available. Instead of analyzing real threats, agencies must be able to imagine, anticipate and plan for future threats by following trends. Ultimately, the agency should not be operating in real time. The only way this is possible is by stepping outside the norm and operating with imperfect data, which will require a significant culture shift.

There is currently an underlying tone of excitement about AI from those willing to accept more risk, but there are also those who are entirely against the use of AI in government. Panelists agreed that a certain level of risk is inevitable, but the question remains: how can agencies achieve balance between AI usability and security?