Deloitte.

Clearing roadblocks to AI-enabled cybersecurity: the President's 2021 Cybersecurity Order and AI innovation

AI, or bust – How the ever-advancing cyber threats of tomorrow are pushing the government to innovate

By Eric Dull, Joe Nehila, Catherine Yin, and Christian Lloyd

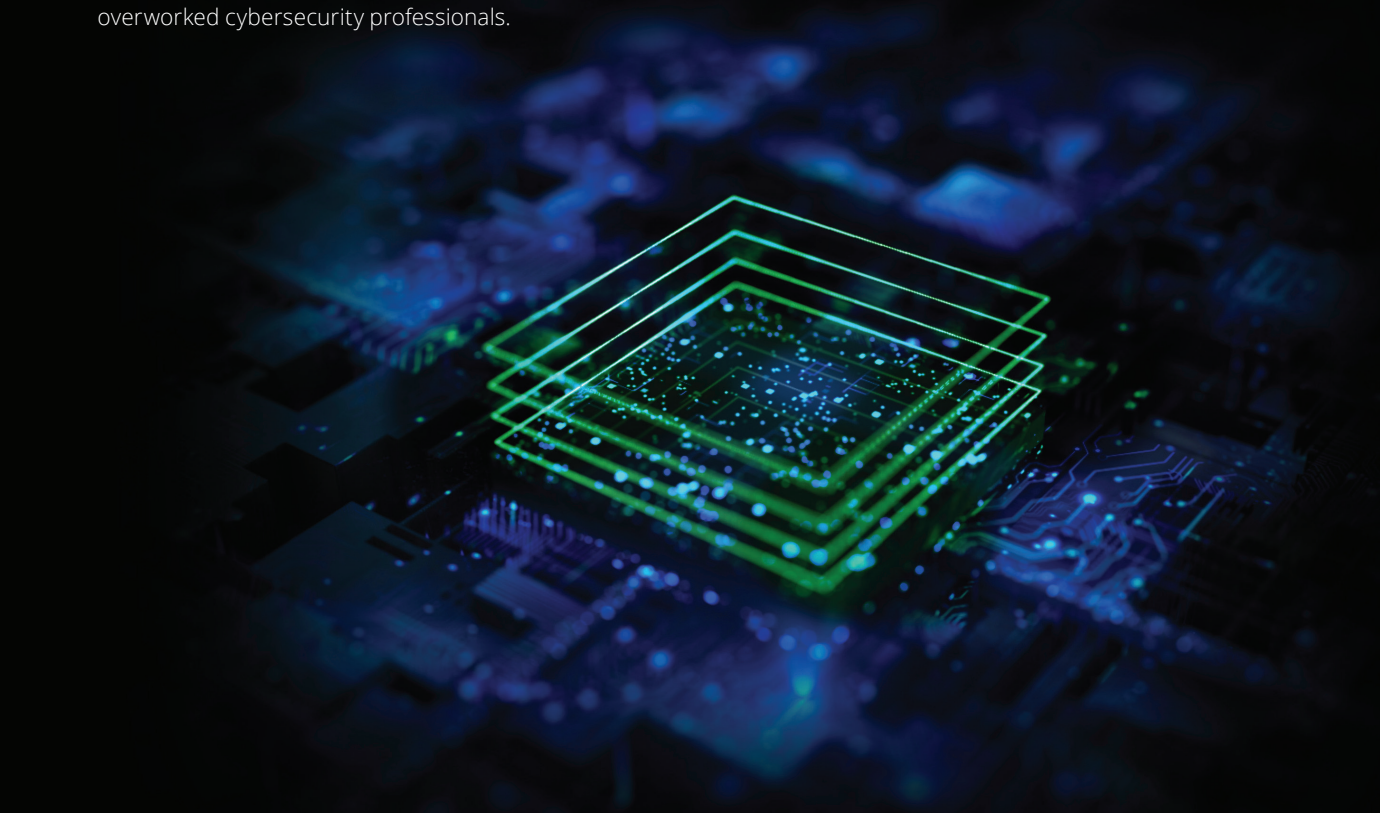
A publication from the Deloitte AI Institute for Government

June 2022

The US government faces a rapid expansion of cybersecurity threats, in terms of both scale and complexity. In fiscal year 2020, US government agencies recorded over 30,000 cyber incidents, an 8% increase from 2019.[1] Several specific cybersecurity intrusions reinforce the seriousness of this challenge. The December 2020 SolarWinds hack[2] led to network breaches at several US government agencies, and the log4j vulnerability discovered in December 2021 may already have been exploited hundreds of thousands of times.[3]

Because of this growing problem, demand for cybersecurity professionals has increased and will likely remain elevated. According to the US Bureau of Labor Statistics, the number of employed information security analysts will grow 33% over the next decade, roughly four times faster than the labor market as a whole.[4] With such high demand, US government agencies may struggle to fill positions, increasing the burden on already overworked cybersecurity professionals.

Due to ever-evolving, sophisticated cyberattacks orchestrated by nonstate and rogue state threat actors, and a widening gap between the demand for and supply of information security analysts, the need for cybersecurity innovation within the federal government is immediate and ongoing.



Artificial intelligence (AI) is critical in achieving this innovation. However, before government agencies can begin to fully leverage AI in cybersecurity, three constraints should be addressed. Until now, AI deployment for cybersecurity in the federal government has been stymied by inadequate data access, cumbrous on-premises infrastructure requirements, and limited workforce capabilities. Fortunately, the White House's May 2021 Executive Order 14028 (EO14028) on Improving the Nation's Cybersecurity may help address these constraints, enabling a new age of cybersecurity in the federal government.

Although the Cybersecurity EO does not explicitly outline or require AI's future deployment within federal agencies, its requirements do open a path forward.

Section 3, "Modernizing Federal Government Cybersecurity," paves the way for agencies to overcome current roadblocks and broaden AI's deployment in the cybersecurity domain. Specifically, Section 3(a) calls for:

- Centralizing and streamlining data access
- Accelerating movement to secure cloud services
- Investing in personnel (and technology) to meet modernization goals

Once agencies adapt to the parameters outlined in the Executive Order, their cybersecurity programs can be poised to facilitate the deployment of AI-enabled workflows.

Removing hurdles and harnessing AI can help improve the underlying infrastructure, allowing mission cybersecurity workforces to be more efficient, reduce burnout, and pivot agencies' cybersecurity postures from reactive to proactive.

Historic AI roadblocks and impacts from the EO

Data access.

In a world of data overload, the existence and inaccessibility of cyber data (e.g., cyber log and telemetry data) within the federal government has significantly impeded the advancement of AI. Data access challenges often stem from stringent policies and permissions, as well as confusion as to what data exists and where. Challenges with incentivizing participation and harmonization exist both across the inter-agency and within intra-agency data lakes.

The Cybersecurity Executive Order calls for the federal government to centralize and streamline access to cybersecurity data. By requiring centralization, obstacles such as confusion surrounding what data exists can dissipate, and a main hurdle to realizing AI's positive potential against the cybersecurity problem space can be overcome. AI, like many statistical models and analytics, requires large volumes of data to be successful. With centralized data and easier access, agency analysts will have the tools to develop, deploy, and train AI algorithms– if given the right computing infrastructure.

Infrastructure.

Most agencies today utilize on-premises (on-prem) environments to store network and cybersecurity-related data. These environments require hefty investments of time, money, and resources to maintain – costs which are potentially exacerbated by the need to access, analyze, and share data during the AI development lifecycle. The resulting limitations on computing and scaling present challenges to processing the volume, variety, and velocity of cybersecurity relevant datasets (often measured in billions of records per day); executing advanced threat detection analytics in a timely manner; and developing new analytics.

Moving to secure cloud infrastructure would enable the agile deployment, testing, and tuning required to successfully leverage AI algorithms, all while reducing costs and increasing capacity. Cloud environments can provide more computational power, at a fraction of the cost and downtime, to meet certain use case demands commonly associated with legacy on-prem environments. With this approach, agencies can ultimately gain the computational scale necessary to match dynamically growing data volumes. With added computational power, models can be run more efficiently, but the sustainability of these technical innovations relies on the workforce creating and operating them.

Workforce capabilities.

Without the right people setting strategy, AI cannot be effectively applied to address cybersecurity problems. A balanced combination of cyber subject matter experts (SME) and people with technical skillsets (e.g., data scientists and software engineers) is necessary to properly develop AI models that meet threat detection needs. Data scientists can develop models and AI capabilities, but often require guidance to understand and incorporate cyber- and agency-specific nuances.

Unfortunately, competitive salaries for technical positions in the private sector and the agile, innovative work environments they foster often lead those with technical acumen away from government work.[5] An investment in AI-enabled cybersecurity, including training and hiring elements, is therefore vital for achieving the objectives of the White House's Cybersecurity Executive Order as well as for providing future strategic and innovative protection within our federal government.

Agencies, by investing in personnel and training, can narrow the gaps to create a balanced AI and cybersecurity combination. Additionally, with proper training across the agency, everyone from analysts to leadership will be able to not only understand what it means to implement AI, but also start identifying specific cybersecurity challenges where AI may be incorporated – critically retaining humans in the loop.

The potential for AI-enabled cybersecurity

With the critical three hurdles—limited data access, infrastructure constraints, and workforce capacity—improved by the Cybersecurity Executive Order's requirements, the potential for reaping AI's significant benefits within the federal domain is unlocked. As threats to cybersecurity have increased, so has the burden on cybersecurity analysts who monitor networks to identify intrusions and malicious behavior. This contributes to "alert fatigue,"—higher numbers of false positive identifications and other errors that complicate performance. A 2021 survey of 489 cybersecurity professionals found "overwhelming workload" to be the second most-cited contributor to work stress, and 57% of respondents agreed that the market-wide cybersecurity skills shortage was impacting their organization.[6]

Incorporating AI into cybersecurity helps overworked analysts sift through the cybersecurity noise to identify anomalous behaviors, prioritize alerts, and reduce false positives.[7] Cybersecurity tends to have very high volumes of very structured data, up to a billion records or more if sourced from a live data stream. The two main algorithm types in AI are unsupervised and supervised algorithms. They require different kinds of input data and can be used to address different types of cybersecurity problems (e.g., exploratory vs. predictive).

The unsupervised method allows large sets of unlabeled data to be clustered and summarized to identify patterns and groupings, including possible cyber mischief, in a way that narrows analysts' attention and stimulates the learning process. By contrast, supervised learning methods focus on fully labeled and characterized cyber data in order to predict and analyze known threats. Models require different kinds, and may also necessitate different amounts, of input data. The potential impacts of the Cybersecurity Executive Order on AI open the doors to development of both unsupervised and supervised models, allowing for a greater variety of models to be used to tackle cyber security challenges.

Unsupervised: Large data sets containing labeled examples of adversary behaviors can be difficult to collect. Leveraging an unsupervised approach can assist in grouping and categorizing the data autonomously, while an agency builds up its set of labeled data. The unsupervised method enables large-scale pattern identification without the need for human input, which in turn allows the agencies to understand their data more quickly than before. As such, unsupervised models can "enable human intuition."

Supervised: The ultimate goal is to utilize supervised learning within the cybersecurity domain. That said, this approach requires large quantities of data and input from analysts to train and tune the models. It requires labeled data and is considered a classical AI or machine learning (ML) approach; with the input of an analyst, the supervised approach enables agencies to classify, advance, and anticipate the ever-evolving cyber threats. Building the labeled datasets and training the models requires a large upfront lift. However, when executed properly, the supervised method may help automate an analyst's initial judgment of threats, enhance the prioritization process, and increase the efficiency of cyber threat detection.

In both cases, AI models serve to "buy back" analysts' time, making them more efficient and effective. Analysts can transition away from being overwhelmed by alerts and hampered by their technology. They can move toward proactively analyzing data and behaviors on networks to contextualize potential alerts, and toward taking advantage of technology-based automation.

The cyber threat climate today has forced both the federal government and commercial industries to concentrate their efforts on cybersecurity advancements and innovation.

With the requirements outlined in the President's 2021 Cybersecurity Executive Order, deploying AI across the federal government is now possible. Pairing the technological advancements of AI with the right personnel can strategically position agencies to stay abreast of malicious threat actors. Agencies can gain the benefit of big data to better understand their network(s), analyze threat behavior, anticipate and rapidly detect malware/ransomware attacks, and customize their unique approach to cybersecurity. Following the Executive Order's imperatives regarding data access, infrastructure, and workforce capabilities can prepare agencies to deploy AI-enabled solutions.

Contact us

Eric Dull
Advisory Managing Director
Deloitte & Touche LLP
edull@deloitte.com

Joe Nehila
Advisory Manager
Deloitte & Touche LLP
jnehila@deloitte.com

Catherine Yin
Advisory Manager
Deloitte & Touche, LLP
catyin@deloitte.com

Christian Lloyd
Advisory Senior Consultant
Deloitte & Touche LLP
clloyd@deloitte.com

About Deloitte AI Institute for Government

The Deloitte AI Institute for Government is a hub of innovative perspectives, groundbreaking research, and immersive experiences focused on artificial intelligence (AI) and its related technologies for the government audience. Through publications, events, and workshops, our goal is to help government use AI ethically to deliver better services, improve operations, and facilitate economic growth.

Contact the Institute

usgpsartificialintelligence@deloitte.com

Endnotes

1 "FISMA FY2020 Annual Report to Congress" (The White House, 2020), https://www.whitehouse.gov/wp-content/uploads/2021/05/FY-2020-FISMA-Report-to-Congress.pdf.

2 Lily Hay Newman, "A Year After the SolarWinds Hack, Supply Chain Threats Still Loom," Wired, December 8, 2021, https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/.

3 Danny Palmer, "Log4j Flaw: Attackers Are Making Thousands of Attempts to Exploit This Severe Vulnerability," ZDNet, December 13, 2021, https://www.zdnet.com/article/log4j-flaw-attackers-are-making-thousands-of-attempts-to-exploit-this-severe-vulnerability/.

4 Bureau of Labor Statistics, "Information Security Analysts," Occupational Outlook Handbook (U.S. Department of Labor, January 12, 2022), https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6.

5 Meagan Metzger, "The Government's Challenge Is Not Attracting Top Tech Talent—It's Keeping It," August 12, 2019, https://www.nextgov.com/ideas/2019/08/governments-challenge-not-attracting-top-tech-talentits-keeping-it/159095/.

6 Jon Oltsik, "The Life and Times of Cybersecurity Professionals 2021, Volume V" (The Enterprise Research Group and the Information Systems Security Association, July 2021).

7 Curt Aubley et al., "Cyber AI: Real Defense," Deloitte Insights, December 7, 2021, https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html.

Deloitte.