How AI Increases the Cyber IQ of Federal Agencies

govloop

PRESIDIO FEDERAL

Silver Business Partner

IBM

Introduction

Federal agencies are undergoing a cultural shift built on embracing artificial intelligence (AI), which can improve performance and scalability throughout their enterprises while increasing efficiencies in spending and the use of employees. Nowhere is the adoption of AI more important than in cybersecurity.

Cyber threats, both from criminal operations and nation-states, are increasing in sophistication and scale, targeting agencies and crucial infrastructure. The tools attackers use will soon include AI, if they don't already. Meanwhile, agencies' expanding cloud infrastructures have become too layered and complex for security teams to manage on their own, even with the array of individual tools at hand.

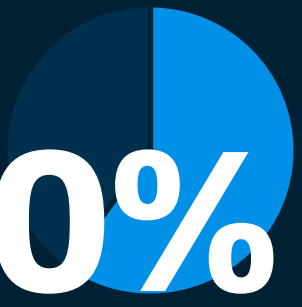
Spurred by the AI in Government Act of 2020 and the mandates of the White House Executive Order on cybersecurity, agencies are pursuing greater use of automation, AI and machine learning (ML). But they also need to improve their infrastructures to better manage the increased computing required to handle the influx and speed of data that comes with being a data-driven organization with an "AI mindset." AI can take agencies into the future — if agencies are prepared to make the most effective use of AI.

For this playbook, GovLoop partnered with Presidio Federal, which works with leading-edge providers like IBM to deliver AI solutions to government. We'll examine AI's key benefits and best practices, what agencies are doing now and how they can prepare for an automated future.

> ***"A global technology revolution is now underway.***
>
> *The world's leading powers are racing to develop and deploy new technologies like artificial intelligence and quantum computing that could shape* ***everything about our lives*** *— from where we get energy, to how we do our jobs, to how wars are fought."*
>
> **— Anthony Blinken**
> **U.S. Secretary of State**

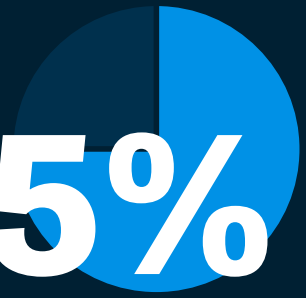
Need to Know

Agencies in the Early Stages of AI Adoption



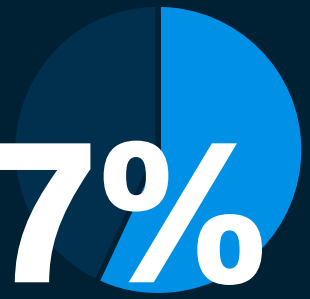
60%

of government AI and data analytics investments aim to directly impact real-time operational decisions and outcomes by 2024.



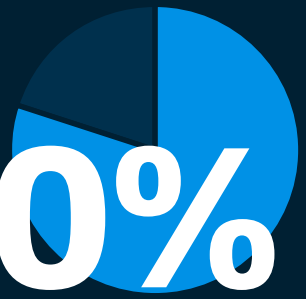
75%

of governments will have at least three enterprisewide hyper-automation initiatives launched or underway by 2024.



57%

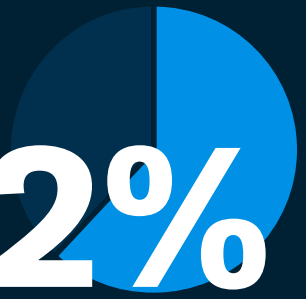
of organizations say that investing in AI, ML and automation has helped prevent cyberattacks.



80%

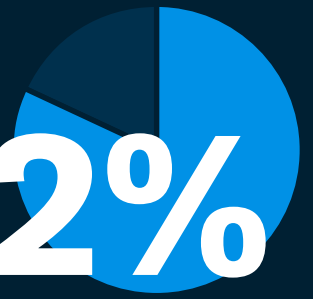
of government organizations are still at the initial or developing digital maturity stages.

Ransomware, Credential-Based Attacks on the Rise



62%

of attacks detected in the fourth quarter of 2021 were malware-free, with attackers focusing instead on credential-based attacks to avoid detection by legacy antivirus products.



82%

is how much ransomware data leaks increased in 2021 over 2020.

Federal Agencies Lead Industry in the Move to Zero Trust

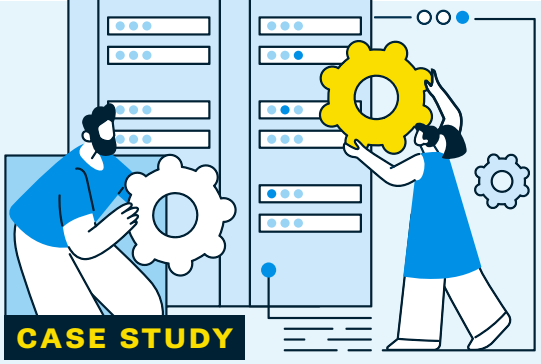
Government agencies, spurred in part by the White House Executive Order (E.O.) on cybersecurity, are outpacing industry in implementing zero-trust frameworks, according to a report by identity and access management company Okta. A 2022 survey by the company found that 72% of government organizations said they are using a zero-trust framework, compared with 56% of private sector companies.

The E.O., issued in May 2021, directed federal agencies to implement cybersecurity best practices, including zero trust, as part of a larger framework calling for greater information-sharing and cooperation between the public and private sectors. And although the order itself did not directly create funding for cybersecurity efforts, 87% of agencies responding to the survey said they had seen at least moderate budget increases for zero trust.

Government Resources

Agencies have several federal resources to turn to for guidance in implementing AI systems, including:

- **The General Services Administration**
  - AI Centers of Excellence includes guidance, examples and updates on AI initiatives.
  - Community of Practice, a community of federal employees who are either active or interested in AI policy, technology, standards and programs, currently includes 1,200 members across 60 agencies.
- **The National Institute of Standards and Technology**
  - AI research homepage links to information on AI research, standards, hardware and practices.
  - AI Risk Management Framework includes guidance for managing risks to individuals, organizations and society associated with AI.
- **The National Security Commission on Artificial Intelligence (NSCAI)**
  - NSCAI's strategy for the responsible use of AI for national security and defense aims to defend against AI threats and promote AI innovation.
- **Data.gov**
  - Provides case studies and examples of agencies implementing AI systems.



DOE Labs Using AI to Help Manage Growing Workloads

A Department of Energy (DOE) national laboratory saw the writing on the wall. Although satisfied with the performance of its Elastic Storage Server (ESS), the lab's IT leadership saw that current and future storage requirements would need the next generation of ESS in order to keep up with the lab's mission.

Organizations with large unstructured data processing and management requirements, such as those running high-performance computing systems at DOE's national labs, need the ability to deliver high performance and high reliability at scale, and must have sufficient flexibility to support different workloads in a single name space or distributed global name space.

With workloads steadily expanding and the need for virtual capabilities increasing, DOE labs need shared storage that supports complex processing requirements that can be managed holistically, easily and economically. Presidio Federal, which has supplied IBM ESS solutions throughout DOE, addresses that challenge with IBM's ESS and Spectrum Scale solutions.

4 Ways AI Is Changing the Cyber Game

AI can change the way government agencies operate by providing the visibility and advanced analytics to improve workflows, optimize cybersecurity practices and enable leaders to make better decisions. **But to get to that point, agencies need to change first, adopting an AI mindset and agencywide culture focused on automation and innovation.**

The cultural change includes understanding AI's complementary role in supporting — but not replacing — agency personnel. It will require infrastructure upgrades to manage the increased use of data. And it involves a willingness to automate processes, taking some lower-level decisions out of the hands of humans, and embracing a future where machines will play a bigger role. Since the AI in Government Act became law, several agencies, including the Department of Defense and the Department of Health and Human Services, have appointed chief AI officers.

How will AI improve agency processes and decisions? Here are several areas where AI will play an integral part — all of them relating, in one way or another, to security.

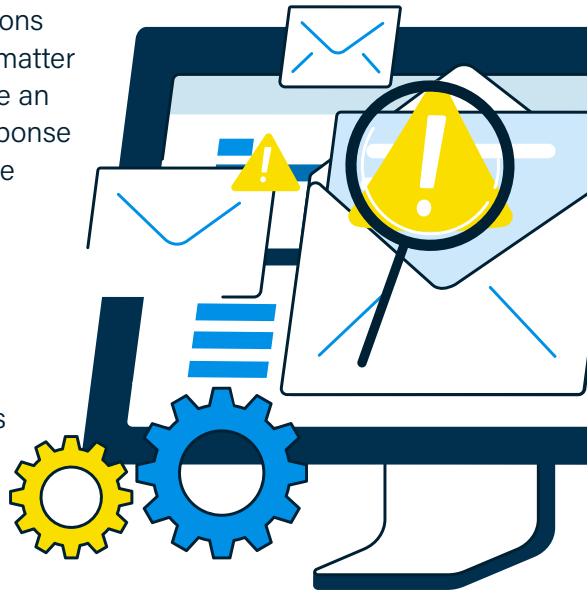
1

Detecting Known — and Unknown — Attack Patterns

The cyber world is becoming an increasingly dangerous place, with attacks against government organizations on the rise from both criminal groups and those associated with nation-states. Meanwhile, security operations centers at government agencies are being overwhelmed by alerts, false positives and the volume and speed of data coming in from growing and increasingly complex cloud infrastructures. Manual processes can't keep up, especially when teams lack full visibility into their environments.

AI and ML can make a significant difference due to their ability to work with large data sets, identify anomalies and assess the impact of threats in relation to existing security policies and risk management frameworks. Not only can AI manage the workload, dealing with cyber events in real time, but it can find patterns of behavior not tied to existing attack signatures and perform predictive analysis that can anticipate threats.

For example, AI can allow IT teams to create a model, or runbook, for responding to signs of a possible attack, such as repeated failed logins, or unusual encryption or unusual access of a file system. Typically, those actions need to be monitored by a subject matter expert. With AI, teams can configure an automated model based on the response that can detect, monitor and analyze those patterns of behavior, alerting human operators of the results.



It also can be applied to physical security such as military reconnaissance, oil and gas threat detection and even the lie detectors used at border control stations.

2

Supporting Better, Faster Decision-Making

The increased speed from automation and the clarity of AI-enabled analytics will improve agency decision-making and productivity. Its ability to quickly analyze large amounts of data, while applying the appropriate rules and frameworks, gives human analysts the insights they need to prioritize their actions and make sound decisions, whether they involve cybersecurity, procurement or constituent services.

"AI can be used anywhere," said Sridhar Satyanarayan, Data Center Architect for Presidio Federal. "It doesn't have to be limited to certain areas."

In procurement and spending, for example, AI allows decision-makers to quickly search through the text of contracts to find specific clauses and develop recommendations for cost savings. Human resources departments can use AI to identify factors contributing to employee churn.

In cybersecurity, the key is to not only provide data analytics and insights to help improve decision-making, but to do it in real time. Malicious actors are using the same types of tools to attack agency infrastructures, including legacy systems, so agencies need a platform that can integrate security tools, efficiently handle the large amounts of data being fed into it, detect anomalies and react in real time, giving operators useful, actionable information.

"AI is the only thing that can do that," Satyanarayan said.

AI not only can look back, sifting through collected data for details and patterns, but look forward via predictive analysis. "The advantage of AI is that AI can look at the history of what data has been coming in and can predict anomalies," he said. "Then it can recommend the appropriate decisions in real time, or near real time."

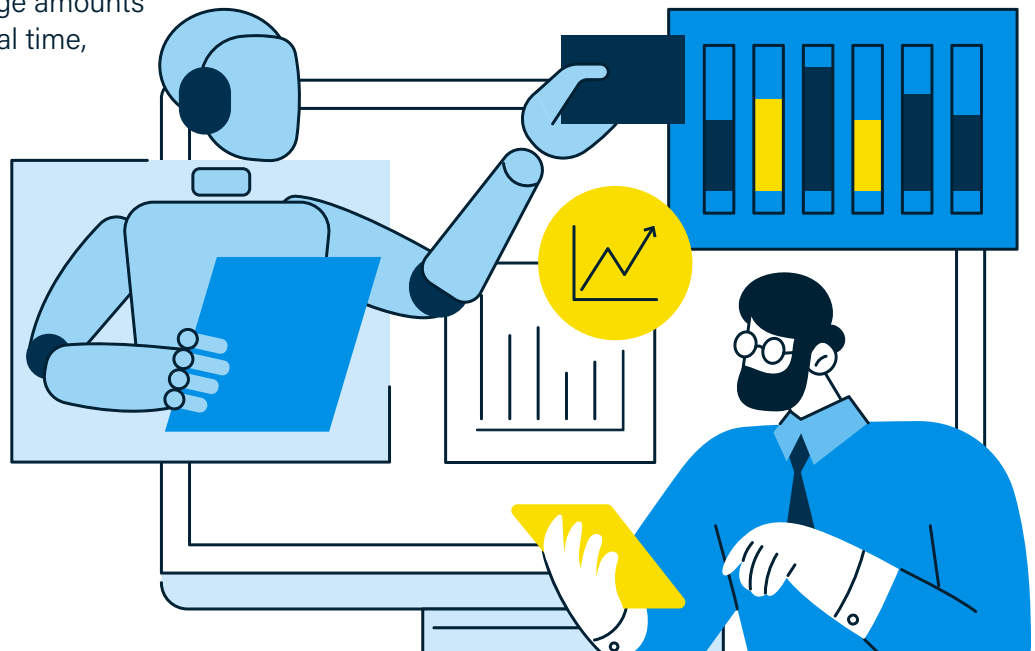
3

Adding Intelligence to Automation

AI allows agencies to make better use of their skilled employees by taking over time-consuming, routine tasks and then handling the first levels of analysis. IT staff can focus on more mission-critical projects, and make cybersecurity decisions based on data, insights and analysis provided by AI.

AI and ML go beyond the basic kinds of robotic process automation, adding an ability to learn, conduct analysis and recommend actions. For example, AI can be deployed in custom automation, such as using natural language processing, voice recognition and tone recognition to assess the state of mind of a caller — such as whether they are distressed — and transfer the call to the appropriate people. It can automate data center operations to improve cost analysis and provide the agency with a better perspective of what's happening in the infrastructure.

With recent advancements, a vendor can provide tools that enable a subject matter expert to build AI models and start using them — without necessarily having a lot of knowledge of or experience with AI, Satyanarayan said. Those tools provide another way for agencies to develop their AI mindset.

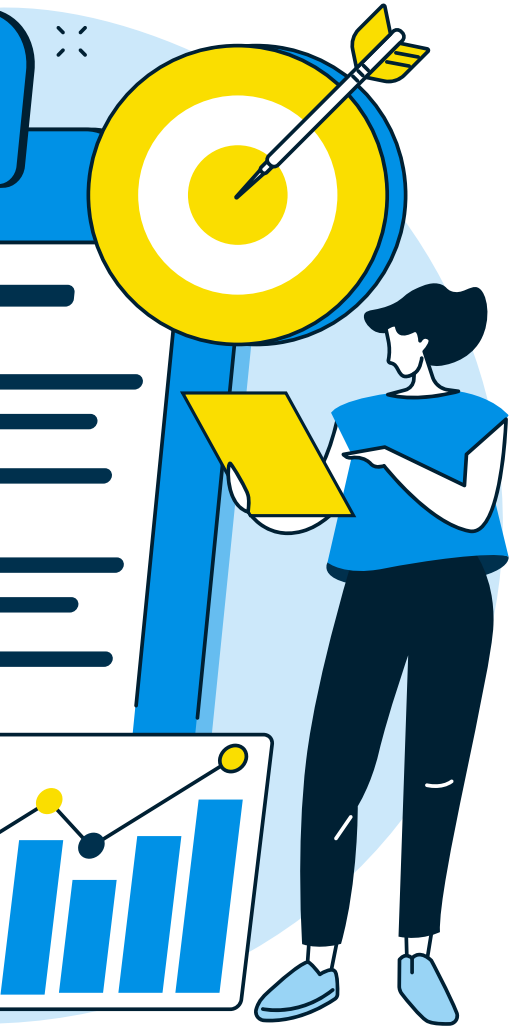


4

Preparing for What's Next

Implementing AI is part of a cultural change that affects how agencies approach operations overall, as well as cybersecurity. Adopting an "AI mindset" opens the door to what agencies can achieve with the technology and allows them to proactively identify new technologies and capabilities.

But they need to ensure their infrastructure is ready. AI is software for the most part, but to make the most use of it, agencies will need hardware with more GPUs to handle the computing load associated with AI. Networks must become more powerful.



Data storage is another area that becomes increasingly important as agencies, with the help of AI, become more data-driven. Data must be secure, discoverable, accessible and organized in order to be effective. But it often is highly distributed in hybrid cloud infrastructures, and/or stored in silos that are managed by disparate storage mechanisms. Agencies need a new approach to storing and accessing data, such as IBM's Elastic Storage System.

For cybersecurity, the speed and sophistication at which threat actors operate is only going to grow, and agencies need to grow along with them.

"The threat landscape will eventually get to the point where things are changing faster than human analysts can look at it," said Clark Anderson, Security Solutions Architect for Presidio Federal.

Threats making use of quantum computing, for instance, are on the horizon. But even before quantum threats become a reality, the cybersecurity battle will likely take place among AI systems. "In a few years — not now, but in a few years — it's going to be AI on both sides," Anderson said. "It's going be robot versus robot."

As part of their AI mindset, agencies should have long-range technology refresh plans for incorporating new technologies as they emerge.

Best Practices in Adopting AI

Before embarking on widespread AI implementation, agencies should follow several best practices to prepare for and manage AI use.

- **Evaluate their IT ecosystem**, which will allow leaders to create a comprehensive, mission-oriented strategy to protect data and assets, and improve performance while meeting compliance mandates.
- **Build out internal capacity**, including adding CPU power and flexible, accessible storage, as well as acquiring new cybersecurity tools and upskilling staff.
- **Maintain transparency throughout the process**, demonstrating how AI works within their agency in order to build trust, both among the staff and with the public at large.
- **Use AI's functionality to keep the agency within budget**, making sure to reduce the costs of core governance functions and increase productivity.

3 Ways Agencies Are Using AI for Future Defense

With the passage of the AI in Government Act of 2022, the federal government recognized that AI is going to be integral to how agencies operate. Agencies have responded with a wide array of initiatives, from procurement to improving the constituent experience.

The possibilities are endless, but IT officials know that it is an iterative process, with many looking to deploy AI in limited scenarios and build on that success.

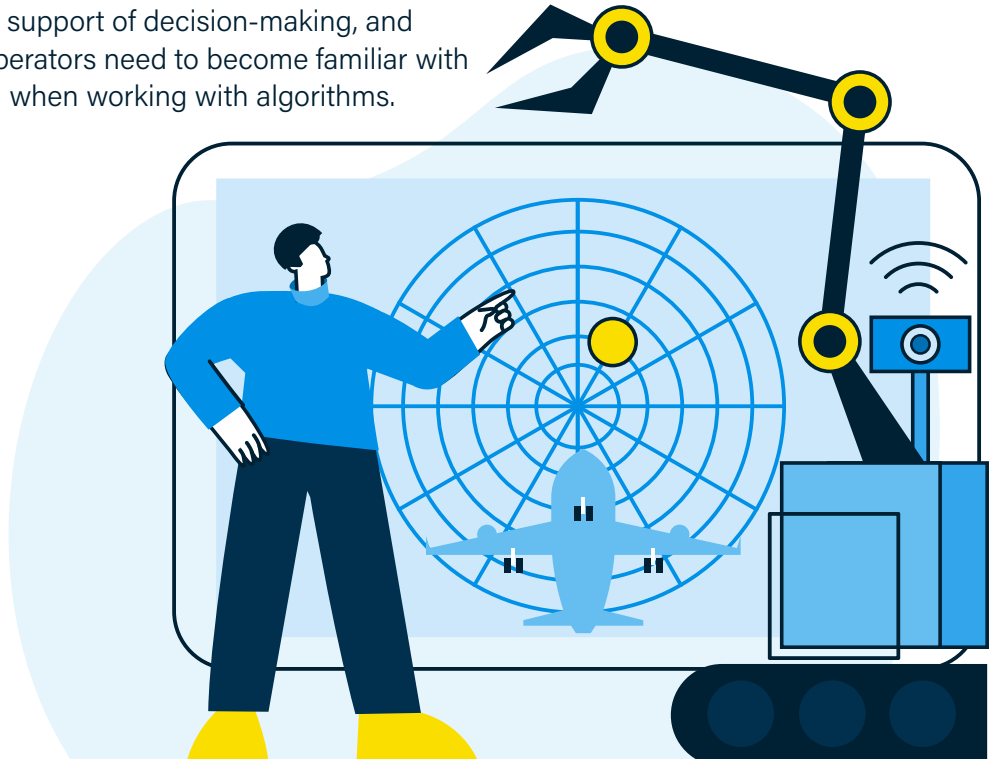
Here are a few examples of how agencies are working to use AI to improve cybersecurity.

Armed Forces Focus on Adversarial AI

The U.S. military is developing its AI programs to defend against attacks by adversaries making their own use of AI. "There's special attention being paid to AI security within the department, so a lot of work is being done on testing vulnerabilities of algorithms and keeping a lid on spoofings, interruptions and [data] poisonings," Marine Corps Lt. Gen. Michael S. Groen said at a recent event.

DOD is working with the U.S. Cyber Command and others on a number of initiatives to use AI to protect networks, Groen said. For example, AI is being used to detect threats causing anomalous activity, which is particularly important in high-speed environments like warfighting, where the pace of activity can be beyond the ability of human operators to keep up with on their own.

Like other agencies, DOD is looking for ways to compete for skilled cyber workers and develop talent within its ranks. But Groen said the department also needs to create a cultural shift to get operators and warfighters to embrace the integration of AI. Commanders need to understand what AI can and can't do in support of decision-making, and operators need to become familiar with AI when working with algorithms.

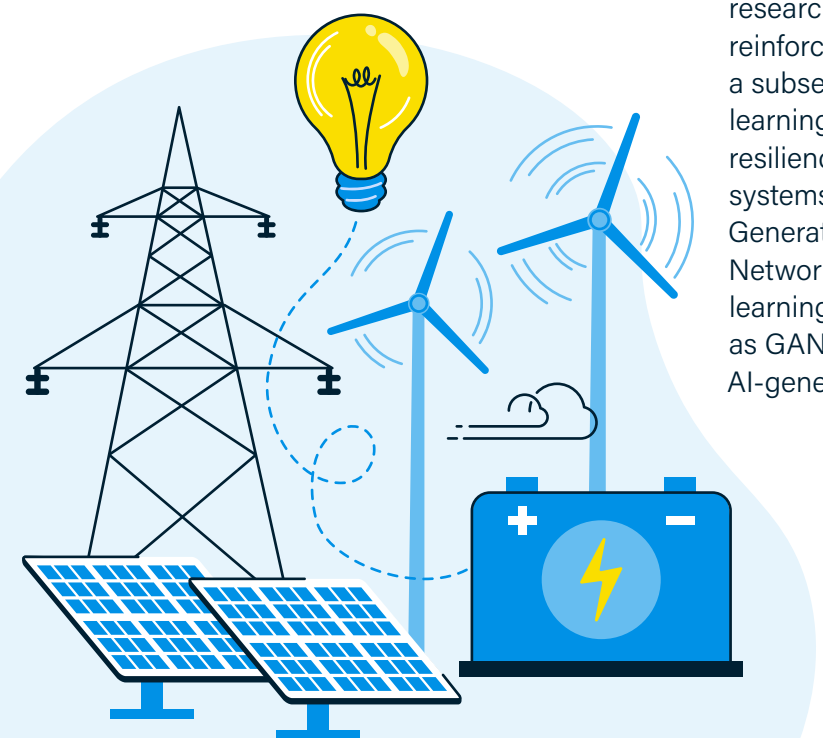


Energy Lab Employs AI to Defend the Power Grid

The Department of Energy's National Renewable Energy Laboratory (NREL) envisions a hybrid electric grid that seamlessly integrates diverse energy sources while relying on autonomous operations. But while such an "electric grid without silos" would greatly increase energy efficiency across the United States, it would also prove tempting to nation-state attackers, who have increasingly targeted critical infrastructure.

NREL's plan for protecting the grid includes implementing high-resolution, real-time simulations of energy systems at full complexity, and using AI for autonomous threat detection. NREL said it ultimately plans to perform analysis and evaluation "at unprecedented detail."

The lab, which focuses on energy efficiency, sustainable transportation, and renewable power technologies, is conducting research efforts into AI capabilities, including using AI for threat correlation across various entities and geographies, using large data sets to anticipate attacks, and characterizing device behavior to develop trust scores. It is also researching deep reinforcement learning, a subset of machine learning, to improve the resilience of distribution systems, and training Generative Adversarial Networks, a deep learning model known as GANS, to confront AI-generated attacks.



Intelligence Community Builds on Its AI Foundation

The Intelligence Community is looking to enhance the work it has done so far with AI to keep up with mounting threats around the globe.

"How do we maximize our abilities as a U.S. IC against our adversaries?" asked Jason Wang, technical director for the National Security Agency's Computer and Analytic Sciences Research Group. "I think the next frontier for us is probably in the cybersecurity space," he said during a virtual web briefing with AI experts from the CIA and National Geospatial Intelligence Agency (NGA).

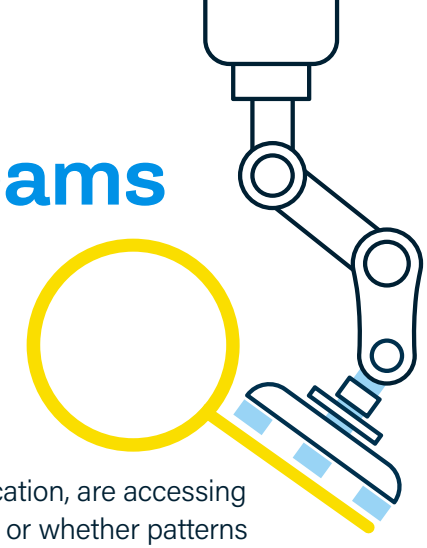
"At the NSA, with most of our industry and academic counterparts, our journey started in this area of natural language processing and computer vision — applying capabilities like machine transcription and machine translation," said Wang.

The NSA has been maturing those technologies in order to extend them to its core mission, Wang said. But the pace likely will accelerate, especially as other nations continue to invest in AI. China is of particular concern, because it might one day add an unrestrained AI program to the world's largest hacking operation, according to FBI Director Christopher Wray.

The IC is looking to employ AI's ability to quickly collect and analyze vast amounts of data, detect threats, and help inform decision-making. "There's a lot of opportunity to bring machines to this very low latency, highly dynamic problem in ways that really are not human-time kinds of responses," Wang said.

AI Will Empower, Not Replace, Cyber Teams

An interview with Sridhar Satyanarayan, Data Center Architect for Presidio Federal



AI can make extraordinary improvements to cybersecurity. It can take over time-consuming, mind-numbing tasks from overworked IT teams, and take data collection and analysis to a level beyond the capacity of human cyber warriors. But what it can't do is take over cybersecurity.

"AI systems, at this time, complement the existing cybersecurity tools," said Sridhar Satyanarayan of Presidio Federal. "I don't think it will ever take over from humans."

But what AI does bring is necessary for agencies to achieve their goals of establishing cybersecurity best practices, implementing zero-trust architectures and contributing to a unified defense.

Threat detection offers one example of AI's complementary — though critically important — nature. Attack patterns change constantly, with malware signatures changing every few seconds. Antivirus software may notice unusual activity, which occurs before every attack, Satyanarayan said, but antivirus is based on known signatures. AI has the ability to detect unknown patterns and perform analysis on them, including predictive analysis.

"AI models can predict what's going to happen next," he said. But data scientists and subject matter experts still must create inference models for AI to work with, and they also will make the decisions on response. "I would say 30% of the process still requires human intervention, and 70% can be automated," Satyanarayan said.

AI Enables Agency Cybersecurity Policies

As cloud infrastructures grow and become more complex, cybersecurity can become too big of a job for in-house IT teams. AI can take a lot of the work off their plates.

"There are certain jobs that humans have a hard time doing, such as looking for little, tiny changes over time," said Clark Anderson, Security Solutions Architect for Presidio Federal. "And that's the type a thing that a machine learning process can do. **Anything that can cut down keystrokes and consolidate information, reduce false positives — all of those factors are very important to an analyst. This is where automation is of tremendous use."**

AI also can help agencies implement zero trust, which calls for constantly reauthenti-cating users, devices and applications across hybrid networks.

It can track users, for example, noticing details such as whether they've suddenly changed location, are accessing data at unusual hours or whether patterns of use have changed over time. AI can help provide the deep visibility into the environment that allows agencies to enforce security policies, including zero trust, incident reporting requirements and mandates to share threat information.

"Zero trust is a model," Anderson said. "It isn't a tool, it's a framework for security."

Many of the tools available perform very well, but the data they deliver can overwhelm operators. AI, by working as a complement to — not a replacement for — IT staff, can give operators more control over the tools they have. For example, it can help agencies move toward a centralized, single pane of glass that provides visibility and shortens the time to response.

Ultimately, AI supports the security policies established at the top of an agency. "And policy doesn't seem like a very cool technical word, but it's really the basis of all security," Anderson said.

Serving as Dominant Partners in Your AI Journey to Ensure MISSION SUCCESS

PRESIDIO® FEDERAL

Silver Business Partner IBM

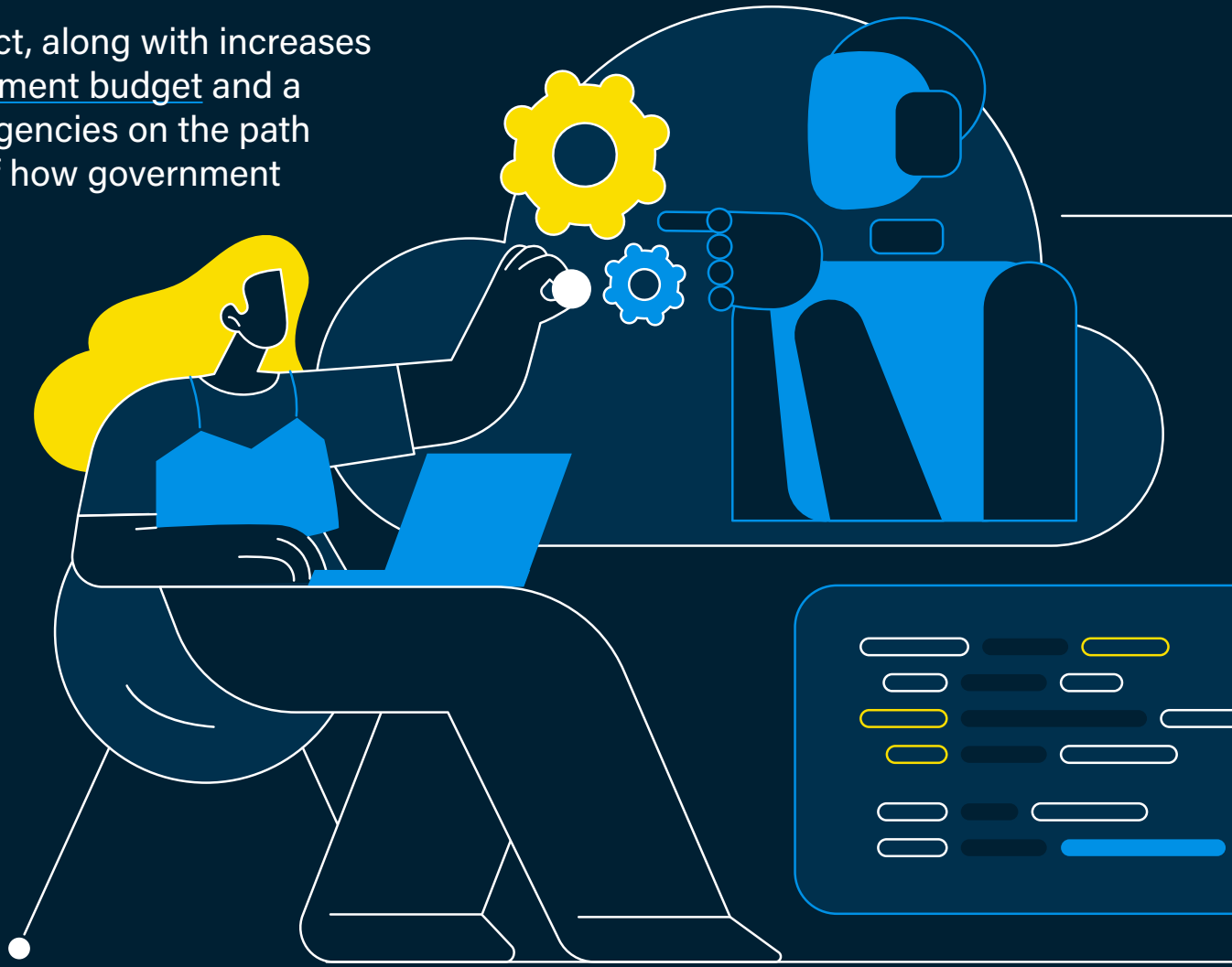
PRESIDIOFEDERAL.COM

Conclusion

The federal government is investing in AI, and with good reason. The National Security Commission on AI's report to Congress in 2021 said it feared that AI tools would soon be the "weapons of first resort" in future conflicts, while lamenting that the U.S. government was "a long way from being 'AI-ready.'"

Since then, the AI in Government Act, along with increases to the federal research and development budget and a wide range of initiatives, have put agencies on the path toward making AI a core element of how government operates. But agencies in many ways are still in the foothills of what AI can do. They need to prepare their infrastructures, bolster computing and storage capabilities, and adopt an AI mindset focused on automation and innovation.

AI can change the game for agencies, supporting better decision-making and performing predictive analysis that allow agency teams to be proactive in cyber defense. It represents the future of operations.



PRESIDIO® FEDERAL

Think Mission.

Silver Business Partner

IBM

Thank you to Presidio Federal and IBM for their support of this valuable resource for public-sector professionals.

govloop

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to **info@govloop.com**.
www.govloop.com | **@GovLoop**