Technology-enabled Governance Innovation Promises Control of Technology-enabled Threats
Use of AI and Other Disruptive Technologies Promise Protection, at Scale

In April, the Cybersecurity and Infrastructure Security Agency announced a partnership with the Office of the Director of National Intelligence, the Department of Defense, and other entities to recognize National Supply Chain Integrity Month and promote a call to action for strengthening global supply chains. This announcement and other efforts are a direct response to the damage caused by several recent cyber-attacks, including SolarWinds and Microsoft Exchange. In February, experts asserted that the collateral damage done from the SolarWinds breach was likely compounded by augmenting human intelligence with Artificial Intelligence (AI).

Artificial Intelligence and other potentially disruptive technologies have created havoc for organizations when hackers use advanced technologies to breach systems and supply chains, and expose personally identifiable information (PII). These same technologies can offer protection when applied to automation of governance that aligns resources to priorities, monitors compliance, and facilitates collaborative action across a dispersed enterprise or supply chain.

Kirsten Moncada, US Office of Management and Budget (OMB) Privacy Branch Chief, recognized the potential for this in her comments at an ACT-IAC Emerging Technology forum panel on Supply Chain a few months before the SolarWinds attack. We heard public comments such as “what does privacy have to do with supply chain issues”? She schooled participants in the importance of privacy in supply chain security and in the overall enterprise risk management discussion. Given the subsequent sophisticated operations that exposed confidential information and the PII data extracted from highly protected US systems, the injection of privacy into the supply chain discussion could not have been more timely.

Moncada noted that public trust relies on government properly handling the personally identifiable information of the public it serves, and taking into account how that information is processed by, and even fuels, emerging technologies like AI. She noted that OMB policy (Circular A-130) explicitly requires integration of privacy into the risk management framework and full integration of both information security and privacy into the system development process (as reflected in NIST 800-37 and -53). More work lies ahead in protecting all manner of government and citizen data. But Moncada spoke to the importance of agencies knowing how the external services and technology they procure operate and use personally identifiable information – that knowledge is essential to ensuring that the use of the external service or technology is in line with the agency’s risk tolerance and that the agency is able to meet privacy requirements laid out in law and policy.

Clearly, we can’t solely rely on external tools, products, systems, and services. We need a formal way to adjudicate and integrate those services that strengthens trust.

The pace of change from automation produces challenges that strain our collective response. Shared frameworks are important for orchestrating coordination, but can only go so far. FEMA CTO, Ted Okada observed that “compliance with data and privacy controls coming out of agencies like the National Institute of Standards and Technology is challenging because they haven’t kept pace with developments in cloud computing and DevSecOps”.

FEMA recognized the need for governance of real-time monitoring and analytics and is now working collaboratively across DHS IT organizations so they can automate their compliance across the organization.

The need for automated compliance, proactive detection, and data sharing will only heighten as critical missions are increasingly carried out across multiple sectors and organizations.

One example of such a large, urgent, multi-sector, multi-organization critical mission, is DoD’s Joint All-Domain Command and Control (JADC2) concept. Officials recognize the need for nearly instantaneous cross-service decisions. The JADC2 concept seeks to bring “all sensors to all shooters” as though on a single network. AI and other emerging technologies will be used to process the data to enable commanders with better situational awareness and to make better decisions.

AI-enabled automated compliance, proactive detection, and data sharing, at scale, will also be needed if JADC2 is to be successfully implemented. JADC2 needs automation of governance that aligns resources to priorities, monitors compliance, and facilitates collaborative action across a dispersed enterprise and supply chains, from the “back office” to the front lines.

In the National Security Commission on Artificial Intelligence (NSCAI) 2021 Final Report, collaboration, automation and governance is taken up a notch. It presents an integrated national strategy to reorganize the government, reorient the nation, and rally our closest allies and partners to defend and compete in the coming era of AI-accelerated competition and conflict.

The report advocates a “democratized” model of AI use for national security. “AI tools are critical for U.S. intelligence, homeland security, and law enforcement agencies.” As Moncada noted, public trust will hinge on justified assurance that government use of AI will respect privacy. The report further elaborates: “The government must earn that trust and rigorously demonstrate that its use of AI tools is effective, legitimate, and lawful. This imperative calls for developing relevant frameworks, standards, and tools to enhance oversight and auditing, increasing public transparency about AI use, and building AI systems that advance the goals of privacy preservation and fairness”. AI-enabled automation can assist in governance of such complex imperatives, while delivering increased protections.

Intelligent Automation of governance and compliance, at scale, promises orchestration of mission partners’ shared standards, data, policies, protections, and responsiveness that better defend against future large-scale attacks. A view across organizational stovepipes, enabled by intelligent automation, adjusts the perspectives beyond the immediate process and beyond checklist compliance. This view can illuminate the whole value chain and new possibilities for improvement. The government can strengthen oversight and governance mechanisms “to assess evolving concerns about AI and privacy, civil liberties, and civil rights”.

The need for automated compliance, proactive detection, and data sharing across multi-sector and multi-organization critical missions will only heighten.

For Thomas Sasala, CDO at the U.S. Department of the Navy, “the pivot from the system-centric model to a data-centric model, or an outcome-centric model,” was a “recent breakthrough” for his agency. “Because data has been wrapped up with the CIO for such a long time, they just become an IT thing for IT people, in the sense that the system owners are also the data owners ... I’ll call it our ‘pervasive cultural idiomatic,’ at least in the DoD [Defense Department] that we’re trying to plod through,” Sasala said. “It is really the data producers that are the ones that control the quality, not the people who run the systems or the applications.”

By switching to this model, Sasala said he is able to obtain data more easily from system owners because they are more willing to turn over their data once they understand “this data is going to answer this question, for this purpose, and influence this outcome” to meet “mission needs.” “We’ve coined a term: discovery then recovery,” he said. “You don’t know what you don’t know until you know it. So, we have discovered where we are [with our data] and so now we can plot a path.
Rigorous, ecosystem-wide governance can assure requisite trust in government and its mission partners, and the appropriate handling of data, especially PII.

In the end, privacy and public trust go hand in hand. With AI-based technologies moving fast, the very technology that once overwhelmed governance-by-frameworks and weaponized stolen data, now holds the keys to data-driven, real-time, automated governance that can not only thwart malevolent use of these technologies, but reinvigorates trust and reduces risk.

Authors:

John Cho, Chief Technology Officer, Peraton; Member, Forbes Technology Council

Judy Douglas, Client Industry Executive, Peraton; Executive Committee, ACT-IAC; Fellow, National Academy of Public Administration

*with Special Thanks to Kirsten Moncada, OMB Privacy Branch Chief*