studio 2G

Harnessing Data for National Security

5 Takeaways from the Intelligence Community

Introduction

New and emerging technologies are becoming increasingly popular: A recent report from Verizon uncovered that total global spending in the Internet of Things market is set to reach $1.3 trillion by 2026. To leverage the data generated from this exponential growth, intelligence agencies need tools that can help them effectively harness data for national security — but what can agencies do today, to better leverage data?

Panelists Tom Sasala, chief data officer for the Department of the Navy, and Cynthia Bedell, director of the Communications & Information Sciences Directorate, DEVCOM Army Research Laboratory, joined host Brandi Vincent, former defense technology correspondent for NextGov, to discuss how their agencies are addressing this challenge during the "Harnessing Data" panel discussion at Defense One's Intelligence Summit.

Afterward, David Cerjan, Managing Director for Verizon's Intelligence and National Security Community, spoke with GovExec 360's Studio 2G, to discuss how Verizon is helping support data efforts.

Continue reading to learn more about what Sasala, Bedell and Cerjan had to say.

1. Be Dynamic! Review Existing Interoperability Standards

Since the introduction of the Intelligence Communities' Information Environment Data Strategy, the amount of data agencies process has increased exponentially. In order to provide intelligence officers and analysts enough information to effectively make decisions, agencies should ensure their interoperability standards are dynamic by creating bridges versus barricades.

"One of the biggest challenges is ensuring you have all of the data released or at least captured," Cerjan said. "If you don't have access to the data, you're making decisions that are limited."

2. Data 101: Cultivate Data Skill Sets Among Existing Employees

The Office of Personnel Management's 2021 Federal Employee Viewpoint Survey found 67% of federal employees are Generation X or above. Digital natives — those who grew up using technology — make up 32% of the federal workforce. This means to leverage data, talent who are not digital natives must learn about how they can draw insights from emerging technologies.

> **"One of the biggest challenges is ensuring you have all of the data released or at least captured. . . if you don't have access to the data, you're making decisions that are limited."**
>
> —
>
> **David Cerjan**
>
> Managing Director for Verizon's Intelligence and National Security Community.

3. Friend Request Incoming: Focus on Building Collaborative Partnerships

At the Army Research Laboratory (ARL) building schematics and testing prototypes is a part of the job, but experimentation is enhanced by collaboration, which is why they partner with incubators and foundries. These collaborators empower the ARL with the skill sets and ability to run small-scale operational tests designed to mimic real-world environments.

"It helps us to have trusted partners. Whether they're academic, small business [or] commercial businesses, [they] help us drive the technology where we need it to go," said Bedell.

Sasala agreed, "we don't need to do it all ourselves." Instead, collaboration among partners, both internal and external, can help agencies tackle existing problems and improve problem-solving capabilities.

4. Keep Humans in the Loop When Using AI/ML

Artificial intelligence and automated processes could help intelligence organizations address the rise in data, relieving data scientists of manual tasks like data tagging. However, AI/ML is an emerging and growing technology, says Cerjan.

"[Having a human] work with it to make sure the algorithm is labeling it correctly before we put that data in a repository where other people can use it is critical," said Bedell. "We have lots of unlabeled data . . .but it has to be used for the right application. Not every algorithm is applicable to every piece of data and vice versa."

> **"[Having a human] work with it to make sure the algorithm is labeling it correctly before we put that data in a repository where other people can use it is critical."**
>
> —
>
> **Cynthia Bedell**
>
> Director of the Communications & Information Sciences Directorate, DEVCOM Army Research

And this is where keeping a human in the loop is crucial. Trained employees can ensure the data is accurately processed, stored and managed, says Bedell. For instance, data in the intelligence community is beholden to IC Directive 700. By keeping a human in the loop, agencies can rest assured their data is secure, and the algorithm is not breaching data standards.

5. Focus on Balancing Agility and Security

As AI/ML matures, the benefits it offers to the intelligence community are numerous. Emerging tools help national security agencies support highly episodic scenarios where circumstances change rapidly — processing and flagging information faster than ever before. However, this requires agencies to balance security and agility.

"The reality of it is that if you want to get some agility, you're going to have to address your risk profile," says Cerjan.

Addressing risk profiles is a complex endeavor. Despite this, there are steps agencies in the IC can take, says Cerjan. First, review existing workloads. What information is Top Secret? What information is Confidential or Unclassified? Second, once these existing workloads are relegated to their separate buckets, then decisions can be made. For example, moving unclassified information poses the lowest risk to an organization; therefore, the information would be a prime candidate for AI/ML modeling.

"The most important thing is the ability to take data, collect it quickly, make quick decisions, and change and make decisions in real time," said Cerjan.