FEDInsider

Innovations, Data and Security are Driving Digital Transformation in the Intelligence Community

FEATURED SPEAKERS:

- **Emily Barbero**
  Branch Chief & Deputy Chief Data Officer, CIO, Mission Operations Branch, Office of Intelligence & Analysis, U.S. Dept. of Homeland Security

- **Cameron Chehreh**
  CTO & Vice President, Pre-Sales Engineering, Dell Technologies Federal

- **Mark Krzysko**
  Principal Deputy Director, Acquisition Policy & Analytics, Enterprise Data, Department of Defense

- **John Roese**
  President & CTO, Products & Operations, Dell Technologies

- **COL Douglas P. Hayes**
  Chief Intelligence, Surveillance, Reconnaissance Information Officer, United States Air Force

The federal government has been taking a slow and steady approach toward modernization. However, recent factors, like an increased threat landscape and the need to support massive numbers of remote workers in the face of a global pandemic have pushed more rapid change in some areas. Meanwhile, the Department of Defense and intelligence agencies are embracing modernization to support mission-critical functions; driving a true digital transformation toward more efficient, secure and reliable networks.

At some level, federal agencies are always modernizing their information technology systems. The federal government has budgeted $83 billion toward information technology funding in 2020, although much of that is earmarked for maintaining existing systems. And while the missions of some agencies might make it okay for them to take a more gradual approach to infrastructure modernization, those working in the Intelligence Community (IC) don't have that luxury.

Intelligence gathering is a dangerous operation. Countries like the United States, historically among the best in the world at the task, maintain their position because of highly trained professionals armed with the best technology. Falling behind on technology innovation isn't an option for intelligence agencies. Doing so would mean putting the country at a serious disadvantage. As such, most IC and DoD agencies make continuous modernization efforts a priority.

The growth and expansion of the cyber threat landscape has been well-documented in the news. Large security breaches aren't only a source of anxiety for commercial companies. If anything, the IC and DoD are even more concerned about guarding critical information.

The very nature of the work intelligence agencies perform is also driving modernization. Most DoD and IC agencies gather massive amounts of something called unstructured data, including reams of video and audio recordings. Being able to process and analyze all of that information in a timely manner is key to producing the kind of actionable intelligence the United States needs to protect its assets and citizens.

DEALING WITH THE CHANGING NATURE OF CYBERSECURITY THREATS

The IC makes an attractive target for cyber criminals. The threat from external actors has continued to grow as the tools and tricks they use become increasingly sophisticated.

The National Counterintelligence and Security Center (NCSC) highlighted the increasingly dangerous threat landscape in its recent National Counterintelligence Strategy of the United States of America 2020-2022 report.

The NCSC report is highly detailed, and contains three key points regarding threats:

- The number of threat actors targeting the United States and its intelligence agencies are growing.
- Threat actors across the board now have increasingly sophisticated intelligence capabilities and technologies at their disposal.
- Threat actors are using these enhanced capabilities to actively attack an expanded set of targets and vulnerabilities.

Emily Barbero, Chief Information and Deputy Chief Data Officer for the U.S. Department of Homeland Security's Mission Operations Branch of the Officeof Intelligence and Analysis, outlined ways the Intelligence Community was examining and countering these new threats during a recent FedInsider webinar.

"We're looking at cybersecurity more broadly today, and we're looking at it collectively as an Intelligence Community," Barbero said. "We're always aware of what is going on with our network, but now we need to attack this problem from a more comprehensive standpoint, because everyone has really good data in the community, and we need to build the technologies and integrate that information in order for us to be proactive instead of reactive in government."

Barbero explained that the definition of cybersecurity in government is expanding, which is helping drive digital transformation efforts to deal with new threats. For example, social media channels could be considered a cybersecurity threat vector if used by adversaries to negatively impact the United States.

"So we're also considering things like social media activity as cybersecurity, and how it may be used by a foreign influence as a way to undermine our elections and things like that," Barbero said.

Defining the concept of cybersecurity is familiar territory for Colonel Douglas P. Hayes, Chief Intelligence, Surveillance and Reconnaissance Information Officer for the U.S. Air Force.

"What we've seen is that the threat isn't always a traditional one anymore like when it comes across the wire and hits the firewall," Hayes added. "We're starting to see more of what I would call covert operations with our supply chain."

Hayes explained that agencies can get used to capabilities embedded within government systems, only to later learn the company that provided the solutions has been purchased by a foreign entity. That, too, is part of the new threat landscape, Hayes said, and it's something that government must be agile enough to address.

Cameron Chehreh, Dell Technologies' Chief Technology Officer and Vice President of Pre-Sales Engineering, agrees that having a secure supply chain is paramount when supporting a digital transformation effort. Otherwise, the government can't trust the new technology it's deploying is completely safe from foreign influence or unauthorized tampering.

"I know we have invested a tremendous amount of capital from a supply chain risk management perspective," Chehreh said. "You have to take an active defense posture with regards to the supply chain because it's about risk tolerance. When you're helping warfighters or with critical missions, it's vitally important that the technologies you provide to the government are as assured as they can be."

A VIRUS INFLUENCES IC DIGITAL TRANSFORMATION EFFORTS

The arrival of the coronavirus pandemic upended many of the government's continuity of operations plans. Within a very short period of time, essentially the entire workforce started working from home. Analysts, data scientists, and support staff had to perform mission critical job functions from their homes. Shifting operations normally conducted within the confines

of a federal office to a much-less controlled home environment was a challenge for the IC, and helped to further accelerate digital transformation programs and technologies. Most agencies significantly reduced employee access to Secure Compartmented Information Facilities, commonly called SCIFs, in an effort to keep their workers safe. But most highly classified materials can only be used inside a SCIF, which created a problem with a largely telecommuting workforce.

This is a new problem for the IC, and while it's not yet been completely resolved, many people in both government and the private sector are working on solutions. In fact, this critical challenge is almost driving its own mini-digital transformation effort.

One person looking for a SCIF alternative is John Roese, Dell Technologies' president and Chief Technology Officer of Products and Operations. He believes emerging technologies like homomorphic encryption might be a solution that could help intelligence agencies move beyond their reliance on SCIFs.

"We can start to introduce new technologies like secure multi-party compute or homomorphic encryption, where the analyst never sees the data," Roese said. "The actual data is shared by multiple parties, but only exposed within the secured enclave or within the encrypted boundary. They can still run algorithms against the information without exposing the raw data. And this technology can extend the trust model even further, so this is an area not just for secure remote SCIF but also remote test taking, or any area where the idea of confidentiality and trust is profound."

Barbero also sees the potential for homomorphic encryption technology to support digital transformation within government. It could prove especially valuable because it would allow data-sharing while protecting the people and methods used to gather the information.

"We could ask mission related and key intelligence questions in a way that honors the data protections that are around it, and also protects the mission that we're trying to execute so we're not over sharing mission-sensitive information," Barbero said.

When paired with some form of artificial intelligence, it could even help hone the questions analysts might ask, helping create actionable intelligence in a way that keeps the data itself fully protected.

"It's about being able to ask a question when you don't know the question that you're asking or even the words in the question," Barbero added. "We hope to pilot something with this in the research and development space to test it out within the next year."

DATA IS THE FUEL FOR FEDERAL DIGITAL TRANSFORMATION

One of the main drivers of federal digital transformation is the need to analyze and organize mountains of data. Technology has improved to the point where agencies have the capacity to collect several petabytes (a petabyte is 1,000 terabytes) of information in multiple formats, over a very short period of time, for a single mission or operation.

"We've been historically people-and organizationally driven, but now the commodity and the lubricant is the data that is coming in as volumes of information," said Mark Krzysko, DoD Principal Deputy Director of Acquisition Policy and Analytics for Enterprise Data. "Now we must be able to exploit that, whatever our jobs are. Whether it's deep analysis in terms of intelligence, or it's a program manager who needs to address that when looking at the goods and services they buy, data must be leveraged to protect our warfighters, soldiers, sailors and airmen."

One key to successful technology innovation within the DoD and intelligence agencies is to find the right balance between what computers and humans can do, ideally with each performing in areas where they excel. The idea is to have technology augment and support the human workforce, not try and replace it.

"We're trying to learn this because our workforce is shrinking in many regards, and we have fewer people and more data," said Krzysko. "So the question is, how can we take advantage of the entire pyramid of technology going all the way up to deep learning? How can we exploit data science, data capabilities, machine learning, deep learning and artificial intelligence in whatever facet that we're trying to solve, whether it's a business practice or an intelligence problem? How can we gain insight and take a load off our analysts so they can perform better?"

The same kinds of innovative human and machine partnerships are also happening at the Department of

Homeland Security. And there, digital transformation is occurring in both big and small ways.

"It may not be exciting to technologists, but when you automate something that an analyst spent a week doing, that is very exciting for them," Barbero said.

"Yes, we go for the big wins and try to develop the coolest widget, but if I'm improving the daily life of an analyst and freeing up 90% of their time every day by automating that process, then not only are they much happier, but are freed to use the skills they went to school to learn," Barbero said. "They can take the automation and build upon that."

GETTING STARTED WITH FEDERAL DIGITAL TRANSFORMATION

"I think the government needs to get faster at adopting new technologies that our partners in the commercial sector are developing," Hayes said. "That way we can be better prepared to defend against the threats that our adversaries place against us."

Digital transformation doesn't have to happen overnight. It's perfectly acceptable to take smaller steps or to implement pilot programs while you learn what technologies work best within the agency. Roese compares government attempts at digital transformation to the early days of cloud computing. Now, cloud is a standard across the government.

"It may sound like extra effort, but the sooner you start to work in this domain, the sooner you can start to build up necessary skill sets and begin to understand the art of the possible," Roese said. "So my advice when getting started is to pick a project and begin to experiment with the new methodologies while you figure out what works for your agency and what doesn't. But the important thing is to commit to those first steps. You just have to do it."

ABOUT CARAHSOFT

Carahsoft is The Trusted Government IT Solutions Provider® and a top GSA Schedule holder, supporting an ecosystem of manufacturers, resellers, integrators and consulting partners committed to serving the public sector.

ABOUT DELL TECHNOLOGIES

Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
(202) 237-0300
Info@FedInsider.com
www.FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider/
@FedInsider

Carahsoft
1493 Sunset Hills Road
Reston, VA 20190
Contact: Mark DeMerse
(703) 871-8626
Mark.Demerse@Carahsoft.com
www.Carahsoft.com/vendors/dell/
Facebook.com/Carahsoft/
Linkedin.com/company/Carahsoft/
@Carahsoft

Dell Technologies
www.delltechnologies.com/
Linkedin.com/company/delltechnologies/
Linkedin.com/company/in/cchehreh/
Linkedin.com/company/in/johnroese/

For more information about Dell Products and Services, please contact:

Dell Solutions for Government
Toll-Free: (866)-Dell-2-Go
Main: (703)-871-8600
(866)-335-5246
Dellgroup@carahsoft.com

© 2020 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.