FBI, DHS Heads Discuss Plans for Emerging Technologies

Major initiatives include cloud migration, integrity of communications and augmented reality.

James Mersol

Thu, 04/25/2019 - 11:51

metamorworks/iStock

Emerging technologies can act as a force multiplier, simplifying the work of human security analysts, increasing their flexibility in accessing data and eliminating the lag between analysts in the field and their counterparts in the cyber operations center. As federal agencies consider the benefits of these technologies, they also examine the potential risks of adopting emergency technologies and the ways to ensure their applications remain closely tied to mission.

One emerging technology that federal agencies are exploring is cloud migration, which will increase the flexibility and accessibility of federal systems and their data for its employees. For agencies that control sensitive but unclassified data, cloud migration creates new challenges.

“From an evidentiary perspective, how do we know we’re actually controlling that data from cradle to grave?” said Jeremy Wiltz, assistant director of the FBI’s enterprise services division, at the AFCEA Homeland Security Conference Tuesday. He cited legal specifications for how federal law enforcement manages evidence and other documents and emphasized that data integrity is another chief concern, as any uncertainty about whether digital evidence was manipulated in one case could have wide-reaching ramifications for other federal cases.

The FBI’s concerns over maintaining evidentiary integrity, privacy and control have not stopped it from exploring other ways to use emerging technologies to further federal law enforcement’s mission. Recently, the FBI’s Criminal Justice Information Services (CJIS) Division migrated its Integrated Automated Fingerprint Identification Service (IAFIS) from the central server at CJIS’s headquarters in West Virginia to an Amazon-hosted cloud server. It was a heavy lift, said Wiltz, and the FBI is still focused on ensuring that the long-term benefits outweigh the initial costs associated with cloud migration.

In the next three to five years, agencies should also look to invest in the integrity of communications networks and IT networks, said Vincent Sritapan, the portfolio manager for physical and cybersecurity at the DHS Science and Technology Directorate.

“When we talk about 5G, there’s a lot of hype there,” he said. “But at the same time, [the older mobile data technologies] aren’t going away.” 4G and LTE will provide a roadmap for how to ensure the integrity of communications over 5G, but it will be important to ensure those older technologies have integrity themselves.

Looking farther ahead, technology in the field of augmented reality will allow agencies to blend their IT capabilities with their physical security capabilities, said Brian Gattoni, chief technical officer for the Cybersecurity and Infrastructure Security Agency (CISA).

“Where [physical and cyber security] converge, it’s important to understand how a cyber event can cause a kinetic effect,” he said. “[It works] when I have a physical security adviser on the ground, at an asset … and we make all of our data accessible through a QR code on that asset [that they can read on their tablet], in real-time, [they’re] staring at it, and [they’re] saying it’s fine, but all the data on that apparatus is telling us something different. How do we now advise that national-level event or that national critical function of our view of risk because I have a human on the ground and the entire power of big data in [their] hands to do real-time risk analysis?”

Gattoni predicted this kind of AR functionality could be used everywhere from critical infrastructure in the national security sector to managing cyber risk around the Super Bowl.

The U.S. Army already has employed a similar use case for AR in counter-improvised-explosive-device (IED) monitoring, Gattoni added. Soldiers can send a robot equipped with a camera into IED-risk areas on a regular basis to take pictures and compare them against earlier photos of the same area to see what, if anything has changed. DHS could use that same technology with AR to examine changes in a server room or other sensitive facility over time to see if any equipment has been added, taken away or altered, said Gattoni. “I want to walk into a room full of QR codes,” he said, mentioning that the technology could be further used to monitor changes to data on these assets.

Agency leads also discussed ways that emerging technologies can provide immersive training opportunities that will keep cybersecurity professionals prepared to respond to threats in ways current best practices do not allow.

“We need to actually practice,” said Wiltz. “What happens on that D-Day? Do we know who does what, how the chain of command works? And can we adapt that in augmented reality so it’s not just a paper exercise? I don’t think we practice enough.” AR games, rather than training presentations or guidance documents, could provide “sensory-engaging” simulations to instill “muscle memory” for cybersecurity professionals, much like physical training exercises for the U.S. military and law enforcement, he said.

View printer friendly version
augmented reality

cloud migration
5G
FBI
DHS
emerging tech
Standard