Leveraging Emerging Tech and Innovation at the FBI

New tech has a place, but agencies should be mindful of security risks.

Connor Collins

Mon, 05/20/2019 - 15:00

Photo credit: MeggiSt/iStock

With an abundance of new and emerging technologies like blockchain, AI, machine learning, drones and genetic genealogy, FBI leadership recently discussed the importance of leveraging and combining these with innovative thinking to make America safer.

Opening with the story of how law enforcement personnel recently leveraged modern genealogical technology to solve the Golden State Killer cold case, Paul Abbate, the associate deputy director of the FBI, encouraged the use of new and emerging technologies and innovative thinking to improve law enforcement

capabilities across agencies and at all levels.

“Since that arrest of the suspected Golden State Killer, investigative genealogy has helped identify more than a dozen other major cold case offenders across the country,” Abbate said at the AFCEA Bethesda Law Enforcement and Public Safety Technology Forum (LEAPS) last week.

Abbate offered a state-of-the-FBI overview, covering topics from solving homicides like the Golden State Killer case to domestic terrorism and cybersecurity. He also emphasized the importance of innovating to counter the wide range of threats that exist today.

“If we’re going to stay ahead of the threat — whether it’s criminal, terrorism, counterintelligence, cyber — we need to evolve constantly,” Abbate said. “And we do this within the FBI by encouraging innovation, by working together, by working externally … and working hard to recruit the best and the brightest."

Innovation, emerging tech and talent will be crucial if any agency — law enforcement, civilian and military alike — expects to deal with the deluge of technologically enabled pain points, be it cybersecurity attacks or online connectivity facilitating terrorist attacks.

“When I look back over my 23-plus years in the FBI, again, there’s no doubt that the threats that are coming at us today are many many more than ever before,” Abbate said.

The FBI is still focused on preventing terrorism attacks from foreign terror organizations on U.S. soil, but the threat of homegrown violent attacks has been a growing challenge, Abbate said. Because of the isolated nature of the origin of these attacks, they are often harder to predict and prevent. Additionally, these homegrown attacks often select “softer” targets like schools, hospitals and concert venues as opposed to traditionally “harder” targets like airports, power plants and government buildings.

But there is good news.

“We’ve had more arrests and disruption with regard to homegrown violent extremists over the last two to three years than we’ve ever seen before, ever in history,” Abbate said. “We remain laser-focused on that within the FBI."

However, Abbate expressed a desire for the country — citizens, media, everyone — to remain vigilant of such homegrown threats, especially in the information-overload age of today.

In terms of cybersecurity, the FBI is facing a range of capable and dangerous actors like nation-states, criminal syndicates and terrorist organizations, Abbate said. Those actors then also utilize a range of tools like ransomware, botnets, spear phishing and other advanced and persistent cyber threats. This diverse threat landscape makes it difficult, if not impossible, to accurately predict and prevent all attacks and intrusion attempts.

“It’s really not a matter of when or how we’ll be hit. It’s going to happen. It’s a question of how severe the damage, the fallout, is going to be,” Abbate said.

In addition to these cybersecurity threats, the FBI is looking at technology supply chains and the threats that may arise there.

“Every link in the chain is a potential vulnerability, and we’re talking about not just our companies and our employees themselves, but the vendors that we do business with and the contractors and their subcontractors,” Abbate said. A weak link in the manufacturing process for defense and consumer technology components could present a huge problem, he added.

Abbate offered advice to companies and organizations that might benefit from cyber, privacy and access controls to alleviate some of these security concerns.

“The key questions are: who has access to your proprietary information? Who has information about your day-to-day operations and the decision-making processes that you employ, your long-term business plans? Who holds the company’s most valuable … business secrets?” Abbate said. He added that the next question should be: do all of those people who have access require that access? If not, limiting access to vital business and operational information would be a good step to take to tighten cybersecurity.

Even with all of the work the FBI has been doing, often in the background, to

combat the threats discussed so far, the agency must continue to explore new target areas and build-out its capabilities to do so. Abbate acknowledged that new and emerging technologies that may aid the FBI will inevitably present new challenges and threats.

“Next-generation telecommunication networks like 5G, the rise of artificial intelligence and machine learning, the use of cryptocurrencies, unmanned aerial systems, deepfake technology, new and emerging technology that may have far-reaching implications that we may not even be able to envision right now … These are the threats that are shaping and will shape our future,” Abbate said.

View printer friendly version
FBI
emerging tech
innovation
safety
cybersecurity
Standard