DHS Partnership Fights Cyber Crime With Innovative Digital Tools

The organization is working on digital forensic technologies to support cybersecurity.

Kate Macri
Fri, 11/13/2020 - 14:04

Jim Jones made a career of “chasing the bad guys,” and now he leads a center of excellence (COE) focused on cyber crime to support the Department of Homeland Security mission.
The Criminal Investigation and Network Analysis Center (CINA), a DHS S&T COE led by George Mason University, provides R&D for various DHS components, including Customs and Border Protection, the Coast Guard and the Secret Service. CINA works most often with Homeland Security Investigations (HSI), specifically for the Cyber Crime Center.

Much of Jones’ and CINA’s work revolves around digital forensics. CINA produces a variety of tools and “knowledge products” to help DHS catch drug cartels and cybercriminals, Jones told GovernmentCIO Media & Research.

Three of CINA’s most recent projects are ready to transition to DHS next year, like the one having to do with voice forensics. With voice forensics, researchers can take a voice recording and analyze small fluctuations like echo to determine where that person is, such as in the case of a distress call to the Coast Guard, he explained.

This voice forensics tool could have a variety of other uses across the agency.

“Any time we have a voice recording in an investigation, we can help validate the authenticity of that recording,” Jones said.

Another CINA project ready to transition to DHS in 2021 is the video forensics counterpart of the voice forensics tool.

“[The tool] is given different videos of potentially the same entity, so you can tell if that's the same person in two different videos,” Jones said. “Say you have video from a crime scene, poor quality, and then at other points in the video we have very good images of a person's face that's not committing any crime. So this helps find if that person did commit the crime.”

The third project prepared for a 2021 transition to DHS' Cyber Crime Center is a digital forensics project that helps law enforcement trace and access deleted data across different devices.

“If we had a phone and laptop that we didn't know were associated with the same crime, this work would in fact link them,” Jones said.

Not all CINA projects result in specific tools for DHS use — some are more analytical in nature, providing helpful research to inform DHS missions.
“There was one project that was a study of dark web marketplaces and teased out geospatial information that goes with those dark web marketplaces,” Jones said. “To do any kind of real investigation we have to make physical contact. That turned into a knowledge product that went over to DHS. The other other one would be a study of the cartels in the northern triangle. By geolocating those posts in the social media side, they can tell where the cartels are operating, it's turning into a map that's given to DHS to show how the cartels are spreading and contracting at different times.”

Despite lockdowns due to COVID-19 across the country, Jones said CINA’s work hasn’t faltered this year. In fact, it’s almost easier to catch “the bad guys” during a pandemic.

“A couple months into the pandemic, we looked at how criminal organizations are changing due to the pandemic and the pandemic response,” he said. “The folks moving stolen goods and people across borders — their job got a lot harder all of a sudden. So we looked at the adjustments criminal organizations were making and what opportunities that created for the investigative side. It's a whole lot easier to see a ship acting suspiciously in a port when there's only two ships in the port. That's one of the biggest changes we saw with the pandemic, as a driver of change on the criminal side.”

DHS charges COEs with specific requests, even though DHS has its own research arm in its Science & Technology Directorate. COEs also fill a research gap left by S&T: instead of only addressing current DHS needs, COEs like CINA think about future problems DHS might face.

Cryptocurrency, for example, poses potential cybercrime challenges. Two of the center's projects are dealing with cryptocurrency.
“One extracts data from crypto wallets, how can we know if they're using a particular crypto and if we can get a transaction history out of that? The second looks at crypto transactions and identifies which ones are likely fraudulent. How do you know which ones you need to look at? The crypto wallet one is probably more [for] the Cyber Crime Center and the digital forensics unit. The crypto transactions project is probably [more for] HSI. It's an open source of data that helps us tie cryptocurrency data, possibly anonymized, to criminal activity. Putting the pieces together of the criminal operations to say these groups, this is how they're operating and this is where their flows are going,” he said.

For Jones, spending time in a lab inventing new ways to catch cybercriminals is practically the zenith of a 20-year cyber career that involved work at the Defense Department.

“The career chasing bad guys and girls was humbling because we caught them, to be really honest,” Jones said.

Now, Jones and CINA work behind the scenes to help cyber practitioners at DHS catch the bad guys.