2014-01

CHDS Grad Steers L.A.'s Unique Cyber-intrusion center

Center for Homeland Defense and Security
Naval Postgraduate School, Monterey, California

http://hdl.handle.net/10945/51306
Los Angeles Police Department Detective John Zambri is the first to admit he is not a techie.

But the 2012 Naval Postgraduate School Center for Homeland Defense and Security graduate has spearheaded establishment of a first-of-its-kind Cyber Intrusion Command Center (CCIC) in the nation’s second most populous city.

“The CHDS education and embracing the importance, the critical nature, of the homeland security enterprise and my part in it gave me a keener understanding of how I can affect my little area in a positive way,” Zambri said in a recent interview. “Without the education at CHDS and getting that unique mindset I would not have been able to get this accomplished.”

Mayor Eric Garcetti signed an executive directive in late 2013 creating the Cyber Intrusion Command Center that would partner with the FBI and the U.S. Secret Service to mitigate cyber intrusions. The order capped off eight months research, collaboration and footwork on Zambri’s part and a team he assembled examined such a facility’s feasibility and potential.

Last spring, Director of National Intelligence James Clapper testified before a House Intelligence Committee that cyber threats were the top danger to U.S. security.

As more and more state and non-state actors gain cyber expertise, its importance and reach as a global threat cannot be overstated,” Clapper said.

Los Angeles took note.

Deputy Chief Michael Downing, a CHDS Executive Leaders Program alumnus, assigned Zambri the mission. The idea stemmed from a Secret Service practice of reviewing municipalities' cyber-related operations in advance of a presidential visit and providing a loose model on how to monitor and combat intrusions. Zambri subsequently assemble a three-person team with Secret Service Agent Jack Furlay and LAPD Senior Systems Analyst Sanjoy Dutta.

The team began the laborious process of researching and writing a white paper outlining how to monitor and mitigate intrusion into the city’s vast, and disparate, networks. In addition to researching technology Zambri sought to enlist the executives of the city’s various departments.

Disparities of the systems used by the city’s 42 departments was a major challenge, particularly those using Supervisory Control and Data Acquisition (SCADA) systems, which are highly restrictive and used to monitor control a plant or equipment.

“They didn’t want to put out information about attacks, or their tactics to mitigate them, because that is sensitive information,” Zambri said. “We had to build into this whole system a way of protecting that information.”
As envisioned, individual departments would retain the responsibility of mitigating cyber intrusions. The CICC’s role would be serving as a clearing house for sharing what types of threats are attacking a certain department so that others may heighten their vigilance. It would also be a central hub for information on strategies to counter a newly incoming intrusion.

“So if the Department of Water and Power has an attack they would deal with it, but would push information to the CICC, which would filter it to the remaining departments,” Zambri noted. “This way everybody is on board. They are not waiting until they get attacked they can put in place safeguards.”

With the operations sketched out, Zambri also scoured potential locations to house a facility, eventually choosing the city’s Emergency Operations Center. The EOC had the infrastructure and the space. The CCIC would be staffed with 12 representatives from what are classified as Tier 1 Departments, such as the Department of Water and Power or Los Angeles International Airport, where a cyber-disruption could cause loss of life or some kind of economic loss.

Realizing the Center is now in the hands of the Mayor’s office, the city is in the process of securing vendors to install the needed hardware in the EOC. Zambri continues to participate in a working group guiding the center’s development.

“It makes the city safer in that now we do not have the gaps, or are working toward closing them, that can be exploited by our cyber enemies,” Zambri said. “Because of the disparate nature of the structure that existed nobody was talking to each other, departments weren’t sharing information. It hardens the city’s cyber infrastructure for all departments and unifies them under one security umbrella.”