



United States Navy

Space and Naval Warfare Systems Command
Office of Public Affairs and Corporate Communications
Contact: Steven A. Davis / steven.a.davis@navy.mil
Desk: 619.524.3432

March 25, 2010

Cybersecurity Specialists Represent SPAWAR at Media Roundtable

SAN DIEGO – SPAWAR employees Sandi Lehan and Dan Green were two of 13 San Diego specialists across private, government and academic communities who participated in a San Diego Daily Transcript roundtable on cybersecurity issues March 25.

The roundtable's key objectives were two-fold: 1) how can disparate communities of interest collaborate and share cybersecurity best practices, and 2) how can San Diego combine these efforts to be recognized as a cybersecurity "model city."

"SPAWAR is pushing the envelope on information sharing to support mission success. It's important to routinely step back re-evaluate our vulnerabilities and ensure we understand the dynamic nature of the threat," explained Dan Green, a data chief systems engineer. "It was great to be included as part of a dialog with industry and local government. It strengthens SPAWAR's role as a local representative of the federal government and reminds us that, as good cyber citizens, we have to remain personally diligent to maintain our collective safety and security."

SPAWAR has joined an effort known as Securing Our eCity, and Green and Lehan were command representatives at the roundtable. According to the organization's Web site, Securing Our eCity "is a coalition of public and private stakeholders focused on combating cybercrime through educational programs, tools and technologies, and coordination with legislative and law enforcement agencies."

Representatives included authoritative figures from San Diego State University, the University of San Diego, the City of San Diego, Wells Fargo and the defense industry. Key discussion points included:

- Cybersecurity training and education – academic and informal – is important for the workforce but is only a frontline level of defense.
- Identifying the nature of cyber adversaries – online predators, identity thieves and developers of malicious codes – is essential to understanding network and personal cyberdefense.
- Even in domestic instances, prosecution of cyber crimes is extremely difficult, and more stringent penalties for cyber crimes would probably help deter such incidents.
- Irresponsible use of social media outlets – in or away from the office – can significantly impact an organization.

- Cybersecurity is important for all organizations but there are common threats and concerns shared between defense, banking and critical infrastructure communities.

“Cybersecurity is a challenge we face both as citizens and Sailors,” said Green. “SPAWAR is playing a growing national role in this mission area and it’s important for us to work with our fellow citizens, state and local governments to improve our region’s safety and cyber readiness.”

The Defense Department detected more than 360 million attempts to penetrate its networks in 2009, which resulted in millions of dollars expended to repair damages. The recent realignment of the Chief of Naval Operation’s N2 / N6 staff and establishment of Fleet Cyber Command reinforced the Navy’s commitment to ensuring effective, efficient and secure decision capabilities for its forces. Additionally, the Navy is establishing an Information Dominance Corps to more effectively and collaboratively manage a cadre of officers, enlisted and civilian professionals who possess extensive skills in information-intensive fields. This corps of more than 44,000 professionals will receive extensive training, education and work on experiences in information, intelligence, networks, space and oceanographic disciplines.

An apt analogy was raised during the roundtable. During the Cold War, the United States experienced a countrywide unity of purpose to counter the Soviet Union threat. Today, the United States needs the same level of unified dedication to deter and defeat cyber criminals and state-sponsored cyber threats.

While participants came to the table with many differing opinions and perspectives, they left with a common understanding: emphasis on strengthening cybersecurity across the spectrum in the United States will continue to increase.

###

[About SPAWAR / www.spawar.navy.mil](http://www.spawar.navy.mil)
www.facebook.com/spaceandnavalwarfaresystemscommand

The Space and Naval Warfare Systems Command (SPAWAR) designs, develops and deploys advanced communications and information capabilities. SPAWAR delivers solutions that give Navy, joint and coalition forces the winning edge, from strategic-level decision makers to tactical-level operators. With more than 12,000 professionals located around the world and close to the fleet, Team SPAWAR is at the forefront of research, engineering, acquisition and support services that provide vital decision superiority to our forces at the right time and for the right cost.