DIÁLOGO
DIGITAL MILITARY MAGAZINE • Forum of the Americas

United to Counter Cyber Crime

International forum among military experts and other professionals discussed strategies for information technology, information sharing, and cyber security best practices.

U.S. Army Lieutenant Colonel Jay H. Anson, chief of SOUTHCOM's Cyber Security Division* | 19 May 2017

INTERNATIONAL RELATIONS

Military and government cyber experts from Latin America, the Caribbean, and the United States came together at the Partner Nation Command, Control, Communications, Computers and Cyberspace Symposium. (Photo: SOUTHCOM)

Military forces in Latin America and the Caribbean are taking serious steps to counter cyberattacks. Repelling malicious outbreaks, protecting their networks, and stopping cyberadversaries are all part of their cyber security efforts. These strategies set the tone for the discussion of a group of military and government cyberexperts from Latin America, the Caribbean, and the United States at their annual "Partner Nation Command, Control, Communications, Computers and Cyberspace Symposium" (PNC5S).

Argentina, Barbados, Belize, Brazil, Canada, Colombia, Costa Rica, El Salvador, Grenada, Guatemala, Mexico, Nicaragua, Paraguay, Paraguay, Peru, Saint Vincent & the Grenadines, Saint Kitts & Nevis, Suriname, Trinidad and Tobago, United Kingdom, Uruguay, and the United States met in Miami, from April 18th to 20th, to talk about a variety of topics spanning information technology, information sharing, and cyber security best practices.

U.S. Southern Command (SOUTHCOM) hosted the event with the participation of the U.S. Defense

Department and industry partners. The goal of the conference was to bring a variety of perspectives together, showcase current and future capabilities, promote interoperability, and open doors for future collaboration in confronting common regional security challenges.

“The number one lesson learned from several decades of defending our networks, is it only takes one careless computer user clicking on a phishing email to defeat billions of dollars in cyber security technology,” said U.S. Army Colonel Jonathon R. Moelter, SOUTHCOM’s Chief Information Officer. “Campaigns to educate users against spear phishing and malicious websites are the best and most cost-effective defense against cyber security threats,” added Col. Moelter.

Cyber security is a challenge shared by all countries in the region. “Cyber space is being exploited by criminals, terrorists, or different groups or individuals that threaten the security or defense of the countries. They are exploiting their anonymity to be able to carry out attacks without being identified,” said Uruguayan Army Colonel Pablo E. Camps, responsible for the cyber incident response team at the Ministry of National Defense. Uruguay is working on a national cyber security network to safeguard against cybercrime.

“Cybercrime generates more economic resources for crime than drug trafficking or organized crime,” said Mexican Navy Commander Jorge Daniel Berdón Lara, head of the Infrastructure Continuity Management group at the Mexican Navy’s General Staff. “It’s important to share what the risks, threats, and vulnerabilities are in our region… We need to encourage information sharing about the threats and risks in cyber space and to know who the people are working on these issues.”

For his part, Sargent Emel Jacobs, Information and Technology officer at the Royal Saint Vincent & the Grenadines Police Force, explained the topic’s importance for his country as they too face cybercrime attacks. “Most of the cybercrime is not only happening in our region, but it’s happening worldwide,” he said. “It’s on the internet, and we need to know the problems that countries are facing and see where we can help each other.” St. Vincent & the Grenadines recently implemented cybercrime laws.

Cybersecurity threats

Cybersecurity threat networks engage in a range of destabilizing illicit activities to damage infrastructure or generate profits. Brazil’s Armed Forces are working to address this dimension of security. “We are working hard in the protection of the critical systems related to the military forces of our country,” said Brazilian Army Colonel Alan Denilson Lima Costa, chief of the Joint Staff at the Cyber Defense Command.

According to Col. Denilson, cybercrime is targeting all citizens, businesses, and governments at a rapidly growing rate. Among the cybercriminal tools being used in Brazil, he said, is the stealing of personal and financial data such as accounts and credit card scams as well as hackers capturing information demanding payment for its release. Col. Denilson added that while a lot of work is underway internally to combat the cybercriminal underground economy, Brazil is also cooperating with countries in the Western Hemisphere and Europe to defeat this threat.

Of the different types of cybercrime, ransomware is particularly on the rise. “Cybercrime is the number one threat in Mexico, but lately, statistics show that government offices are suffering attacks mainly related to the hacking of data,” said Cdr. Berdón. Mexico is working on a national cybersecurity strategy to thwart the attacks.

Improving strategies

To stay on top of its game, SOUTHCOM is developing OneNet, a multilateral information system under the U.S. Department of Defense’s Mission Partner Environment Information System program. OneNet provides the means to coordinate classified data between SOUTHCOM and partner nations.

Trinidad & Tobago Coast Guard Lieutanant Commander Tonino K. Tracey (left), and Brazilian Army Colonel Alan Denilson Lima Costa pay attention to a presentation during the symposium. (Photo: Geraldine Cook/Diálogo)

The plan is to have "trans-regional, transnational networks whereby everyone is on a level playing field collaborating between the United States, partner nations, and amongst themselves," said U.S. Navy Lieutenant Commander Matthew Johnson, program manager of the Multinational Information System, the defense information program responsible for partner nation networks.

Lt. Cmdr. Johnson affirmed that SOUTHCOM's ultimate goal is "to have a network that the partner nations can feel comfortable operating on without having to worry about threats from hackers, illegal users, or unauthorized users. It's ultimately about collaboration as a comfort factor; they have to feel confident that when they use this network, their information is secure and not at risk. It is our responsibility as technical providers to mitigate that risk as best we can."

Other topics covered at the conference included insider threats, the Dark Web (websites that hide their identity), and emerging countermeasures to those challenges such as Blockchain Technology (special secure database). However, after three days, military personnel, public security, and private industry reached the same conclusion: working together to defeat cybercrime is a must.

"Cyber security is an evolving threat, and there are things that may be applicable today that will not be applicable tomorrow," said Trinidad & Tobago Coast Guard Lieutenant Commander Tonino K. Tracey, commander of the Port Security Unit. "We must be able to learn from each other's experiences to implement the security measures that we all need," he added.

"It's very important to collaborate. These types of security threats have no boundaries," said Col. Camps. "It is very important to participate in this type of exchange in a multi- or bilateral setting as we are able to learn a great deal from lessons previously learned [from other countries]."

Col. Denilson agreed. "The key to halting cybercrime is integration amongst the armed forces. It will be very

difficult to combat it if we are isolated."

*Geraldine Cook/Diálogo contributed to this article.