CYBER DEFENSE CONFERENCE

WESTERN HEMISPHERE

14-15 May 2019
Bogota, Colombia

CONFERENCE REPORT

IADF
Inter-American Defense Foundation

Inter-American Defense Board

La Victoria es de Todos
Fuerzas Militares de Colombia

I. Executive Summary

Cyber defense represents the single greatest shared threat and opportunity for cooperation in the Western Hemisphere. The 2019 Cyber Defense Conference addressed both the threat and opportunity dimensions by assembling 170 high-level military, government, academic and private sector authorities from 25 countries with the strategic intent to enable improved cyber cooperation in the Americas.

In May 2019, the Inter-American Defense Board (IADB) and the Inter-American Defense Foundation (IADF) in partnership with the Colombian Military Forces held the first Cyber Defense Conference in Bogota, Colombia. The objectives for this conference included:

1. Providing contextual awareness of the cyber landscape to include threats and opportunities for cooperation between key stakeholders (government, academia, industry, and nation states) and thought leadership;
2. To promote analytical and technical exchanges of information by seeking consensus on common regional challenges;
3. Building strategic multi-lateral and bi-lateral partnerships between key stakeholders to promote best practices and improved multidimensional information sharing;
4. Recognizing hemispheric accomplishments in recognition of existing diverse cyber defense efforts;
5. Establishing the basis for both short and long term hemispheric cyber defense cooperation by key stakeholders; and
6. Creating one-to-one relationships among leaders from government, industry, and academia.

The agenda was organized according to the following discussion topics: policy and strategy, global cyber trends, protection of critical infrastructure, collaborative approaches to cyber defense, public-private partnerships and the role of industry, global partners, technological developments, and advancements in cyber training and education.

II. Key Observations and Conclusions

The 2019 Cyber Defense Conference outlined topics which require multi-lateral perspectives for understanding as well as the benefits of addressing the issues and threats collectively. However, it also demonstrated the challenges of doing so and the political commitments required to improve cyber defense at speed and at scale.

Officials also discussed the latest cyber defense and cybersecurity developments globally and regionally and how to improve defense cooperation in priority areas. Specifically, many agreed that countries in the Americas must ensure that networks are resilient and secure, national critical infrastructure is protected, and that strong partnerships with both academia and the

private sector are fostered. Moreover, the benefits of sharing information with international partners, domestic actors, and industry were explored during the conference and their ability to strengthen nations against common threats. Global competitors are already involved in the region and strong cyber defense postures are essential in pursuing common interests and strengthening regional security.

Participants, presenters, and panelists indicated that developing a hemispheric cyber defense framework or doctrine was of interest and topics of common interest included:

1. **Improving multi-level cyber education and training.**

   Improving cyber education and training at senior political and technical levels is at the core of efforts to strengthen a culture of cyber awareness and developing the appropriate technical skills. Both awareness and technical skills are widely accepted by cyber security professionals as essential foundational elements of a cyber defense capability and capacity.

2. **Improving unclassified information sharing both in the multilateral and state context.**

   Both government and industry cyber security experts are virtually unanimous in the assertion that a unifying framework and strategy to include establishing digital platforms to share relevant unclassified information could be highly beneficial. These recommendations could include information on:

   a. Cyber capabilities;
   b. Best practices;
   c. Lessons learned; and
   d. Threat intelligence to include but not be limited to indicators, hashes, protocols, procedures, processes, and mitigation.

   Additionally, creating a common lexicon was deemed to be of importance in addressing the topic from a multi-national perspective. Improving the ability of countries to work together in the Western Hemisphere among each other and with international partners in operations is essential to ensuring future interoperability of IT, OT, processes, and people.

   Formal information sharing mechanisms at the multilateral level were preferred over informal arrangements. Common issues should first be identified before determining what information could be shared.

3. **Sharing best practices in defining and protecting critical infrastructure.**

   Militaries are impacted when critical infrastructure is affected. Countries agreed that strengthening their institutions and their responses to cyber threats, including having a

dedicated cyber command, could better protect critical infrastructure in the short and long term. Moreover, sharing real-world experiences and best practices of cyber incident response, particularly in the case of recent cyber-attacks against critical infrastructure was deemed of interest among the countries.

Good communication and collaboration with internal agencies and the private sector, was another aspect that was identified that would improve a country's ability to respond appropriately to threats.

4. **Creating a clear and relevant cyber regulatory framework.**

A solid legal framework that governs rules and policies, definitions, and actions to protect against threats and guarantee the public interest needs to be defined, legally and politically. Developing the appropriate legislation as well as the corresponding processes and inter-agency agreements are required when combating this new type of threat.

Cybercriminals and malign actors do not necessarily fit within the traditional profiles and laws, which is why there is an urgent need to ensure that adequate regulatory frameworks be adopted or developed and implemented.

5. **Ensuring appropriate military, government and private sector collaboration.**

Strengthening global cooperation among allied partners to include the private sector is essential in meeting today's complex multidimensional cybersecurity challenges. The complexity of network, system and data ownership coupled with industry's ability to rapidly innovate makes a close partnership between the military, civilian government and private industry a necessary component to increasing cyber defense capabilities at every level.

However, it is crucial to select the right kind of partners, who will be beneficial to advancing the Hemisphere's interests in the short and long term. Countering malign influence both in terms of the private sector and state actors should be a priority.

6. **IADB and IADF to assume a more prominent role in cyber defense.**

Several countries requested that the IADB and IADF assume a larger role in cyber defense, including but not limited to:

a. Continuing to organize high-level conferences annually;
b. Organizing exercises/tabletop exercises;
c. Requesting support from NATO as a model for the Western Hemisphere to follow concerning a cyber framework/doctrine, and the corresponding manuals; and

d. Assisting in capacity-building and developing common definitions and understanding surrounding: critical infrastructure, threats, vulnerabilities, protection, tactics-techniques-procedures, and coordination with existing mechanisms.

III. Participating Entities

The conference attracted one hundred and seventy (170) high-level military, government, academic and private sector authorities from the following twenty-five (25) countries:

1. Argentina;
2. Barbados;
3. Belize;
4. Brazil
5. Canada;
6. Chile;
7. Colombia;
8. Costa Rica;
9. Dominican Republic;
10. Ecuador;
11. El Salvador;
12. France;
13. Guatemala;
14. Guyana;
15. Honduras;
16. Italy;
17. Jamaica;
18. Mexico;
19. Panama;
20. Paraguay;
21. Peru;
22. Spain;
23. Suriname;
24. United Kingdom; and
25. United States.

Additionally, eight (8) other entities participated:

1. North Atlantic Treaty Organization (NATO);
2. United Nations (UN);
3. Inter-American Defense Board (IADB);
4. Inter-American Defense College (IADC);
5. Inter-American Defense Foundation (IADF);
6. Florida International University (FIU); and
7. National Defense University (NDU); and
8. Escuela Superior de Guerra (ESDEGUE).

Finally, five (5) private sector companies were in attendance:

1. Fortinet;
2. Scitum-TELMEX;
3. McAfee;
4. Q-Mission; and
5. XtremeLabs.

IV. Next Steps

Participants unanimously agreed that the Bogota Cyber Defense Conference provided significant insights. Participants spoke highly of the technical and strategic discussions as well as the one-to-one personal connections made with other military, civilian, and industry leaders. It is hoped that this conference will continue further multilateral, bilateral and national cyber defense discussions and serve to inform strategy and decision-making. It is also hoped that the Bogota Conference, with the continued support of the IADB and IADF, will act as a catalyst to strengthen relationships, advance multilateral interests, share best practices, and learn from allies and partners.

There was genuine excitement to continue building a hemispheric approach to cyber defense and the Inter-American Defense Board and its Foundation are laying the groundwork for the next conference. The venue for the Second Cyber Defense Conference will be announced shortly.

V. Annexes

1. Final agenda
2. Photo Gallery

Annex 1: Final Agenda

CYBER DEFENSE CONFERENCE: WESTERN HEMISPHERE DAY 1: MAY 14, 2019	
07:45	**REGISTRATION & COFFEE**
08:30	**Opening Ceremony and National Anthem**
	POLICY & STRATEGY: NATIONAL APPROACHES TO CYBER DEFENSE
08:45	**Opening Keynotes** • Major General Nicacio de Jesús Martínez Espinel, Commander of the Colombian Army • Doctor Diana Catherine Abaunza Millares, Deputy Minister of Defense of Colombia • Brigadier General Stephen Lacroix, Director General, Inter-American Defense Board
09:15	**Colombia's Cyber Defense Policy and Strategy** Guillermo Botero Nieto, Minister of Defense, Colombia
09:35	**Cooperating to Strengthen Defenses Against Cyber Attacks in the Western Hemisphere** Sergio de la Peña, Deputy Assistant Secretary of Defense for Western Hemisphere Affairs, Office of the Secretary of Defense, USA B. Edwin "Ed" Wilson, Deputy Assistant Secretary of Defense for Cyber Policy, Office of the Secretary of Defense, USA
10:00	**COFFEE AND NETWORKING BREAK**
10:15	**Chile's Cyber Defense Strategy** Cristian de la Maza Riquelme, Deputy Minister of Defense, Chile
10:45	**Defending Defence in Canada; a Cyber Strategy** Len Bastien, Defence Chief Information Officer and Assistant Deputy Minister of Information Management, Department of National Defence and the Canadian Armed Forces, Canada
11:15	**Brazil's Cyber Defense Command and its role within the National Defense Strategy** Brigadier General Alan Denilson Lima Costa, Director, Cyber Defense Center, Cyber Defense Command, Brazil
11:45	**Cybersecurity Strategies: From Concept to Implementation** Philip Quade, Chief Information Security Officer, Fortinet
12:15	**NETWORKING LUNCH**
	COLLABORATIVE APPROACHES TO CYBER DEFENSE
13:30	**Global Cyber Defense and Cybersecurity Trends** Dr. G. Alexander Crowther, Senior Research Associate, Jack D. Gordon Institute for Public Policy, Florida International University (FIU)

13:50	**PANEL DISCUSSION: Protecting Critical Infrastructure: Civilian-Military Cooperation** • How to deliver network and information security across a variety of sectors and protect the infrastructure that is vulnerable to attacks in the digital realm? • Ensuring that these infrastructures are protected and robust enough to meet varied cyber threats, and establishing best practices Panelists: • Major General Ricardo Jimenez Mejía, Joint Chief of Staff of the Colombian Military Forces, Colombia • Philip Quade, Chief Information Security Officer, Fortinet • Richard Driggers, Deputy Assistant Director for Cybersecurity for the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), USA Moderator: Marco Emilio Sánchez Acevedo, Lawyer, Director of IUSATIC Abogados & Consultores
14:40	Q&A
14:50	**PANEL DISCUSSION: Hemispheric Framework for Cyber Defense Cooperation** • How could the Western Hemisphere benefit from improved cyber defense collaboration? • Could improved intelligence sharing assist with developing a collaborative, multi-national cyber defense strategy? Panelists: • Dr. Diana Abaunza Millares, Vice-Minister of Defense, Colombia • Brigadier General Stephen Lacroix, Director General, Inter-American Defense Board • Brigadier General Alan Denilson Lima Costa, Director, Cyber Defense Center, Cyber Defense Command, Brazil Moderator: B. Edwin "Ed" Wilson, Deputy Assistant Secretary of Defense for Cyber Policy, Office of the Secretary of Defense, USA
15:40	Q&A
15:50	**COFFEE AND NETWORKING BREAK**
16:00	**PANEL DISCUSSION: Public-Private Partnerships in Cyber Defense: The Way Forward and the Challenges** • How can the public and private sectors more efficiently collaborate to ensure that the armed forces in the Americas have cutting-edge technologies at their fingertips • Public and private sectors will outline the challenges of working together Panelists: • Major-General François Chagnon, Cyber Force Commander, Canadian Armed Forces J6, and Chief of Staff (Information Management), Canada • Richard Driggers, Deputy Assistant Director for Cybersecurity for the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), USA • Chelsey Slack, Deputy Head, Cyber Defence Section, North Atlantic Treaty Organization (NATO) Moderator: Dr. Cristina Rodriguez-Acosta, Assistant Director for Institutional Relations at the Jack D. Gordon Institute for Public Policy, Florida International University (FIU)
16:50	Q&A
17:00	**Defending the Networks: NATO, Cyber Defense, and Partnerships** Chelsey Slack, Deputy Head, Cyber Defence Section, North Atlantic Treaty Organization (NATO)

17:30	CLOSING REMARKS AND END OF MAIN CONFERENCE DAY ONE
17:45-19:45	**Cocktail** **Venue: "Sky 15 Rooftop" at the Hilton**

CYBER DEFENSE CONFERENCE: WESTERN HEMISPHERE DAY 2: MAY 15, 2019	
08:30	**REGISTRATION & COFFEE**
	GLOBAL PARTNERS
08:50	**Opening Remarks**
09:00	**USSOUTHCOM and USNORTHCOM** Colonel Miguel Colón, Chief of Cyber Operations J3, USSOUTHCOM Colonel John Roper, Vice Chief Joint Cyber Center J6, NORAD-USNORTHCOM
10:00	**Spain's Joint Cyber Defense Command** Colonel Francisco Palomo Pérez, Chief of Operations, Joint Cyber-Defense Command, Spain
10:30	**COFFEE AND NETWORKING BREAK**
10:45	**The Role of the Inter-American Defense Board (IADB)** • IADB's Cyber Defense and Cybersecurity initiatives • How can we improve cyber information-sharing at the hemispheric level? Brigadier General Stephen Lacroix, Director General, IADB
11:00	**Cybersecurity in México: Operating the Cyber Intelligence and Cybersecurity Center** Marcos Polanco, Director of Solutions Design and Strategic Consulting, Scitum-Telmex
11:30	**Ibero-American Cyber Defense Forum** Brigadier General Tomás Ramón Moyano, Commander, Joint Cyber Defense Command, Argentina
	TECHNOLOGICAL DEVELOPMENTS
12:00	**Cybersecurity – The Fifth Domain to Protect** Luis Ortiz**,** Field Engineering Senior Director for Latin America, McAfee
12:30	**NETWORKING LUNCH**
	INDUSTRY SUPPORTING THE ARMED FORCES
13:30	**PANEL DISCUSSION: Role of Industry** • How can the public and private sectors improve collaboration to better achieve common goals and outcomes? • All sectors and actors have a vested interest in ensuring cyber safety

	Panelists: • Dr. Victor Muñoz Rodríguez, Presidential Adviser for Innovation and Digital Transformation, Colombia • Pedro Paixao, Vice President and General Manager, Fortinet Latin America • Marcos Polanco, Director of Solutions Design and Strategic Consulting, Scitum-Telmex Moderator: Dr. Jeimy Cano, Academic and International Consultant, Universidad de los Andes
14:20	Q&A
	CYBER TRAINING AND EDUCATION INITIATIVES
14:30	**Military Power in Cyberspace: Cyber Defense Political and Strategic Analysis** • Understanding the implications of cyber defense policy and strategy in the mission and functions of military power in cyberspace Dr. Boris Saavedra, Associate Professor, William J. Perry Center for Hemispheric Defense Studies, National Defense University
15:00	**COFFEE AND NETWORKING BREAK**
15:15	**PANEL DISCUSSION: Advancements in Cyber Defense Training and Education** • Strengthening cyber training and knowledge to better address security risks • Establishing multilateral cooperation agreements to train armed forces personnel on cyber defense through simulations and exercises Panelists: • Major General James Taylor, Director, Inter-American Defense College • Rear Admiral Orlando Grisales Franceschi, Deputy Director, Escuela Superior de Guerra, Colombia • Randy Pestana, Assistant Director of Research and Strategic Initiatives at the Gordon Institute for Public Policy Florida International University (FIU) Moderator: Dr. Yezid Enrique Donoso Meisel, Director, Department of Systems Engineering and Computing, Professor, Universidad de los Andes
16:05	Q&A
16:15	**UNODC Global Program on Cybercrime: Challenges and Opportunities in the Northern Triangle of Central America** Luisa Fernández, National Coordinator Guatemala, Cybercrime Program, United Nations
16:45	**Closing Remarks** Major General Ricardo Jimenez Mejía, Joint Chief of Staff of the Colombian Military Forces, Colombia
17:00	**END OF MAIN CONFERENCE DAY TWO**

Annex 2: Photo Gallery

All of the conference photos can be accessed at the following link:

https://www.iadfoundation.org/photo-gallery/