REPORT

II CYBER DEFENSE CONFERENCE

28-29 SEPTEMBER 2020

INTER-AMERICAN DEFENSE BOARD

IADF
INTER-AMERICAN DEFENSE FOUNDATION

Canada

TABLE OF CONTENTS

I. MESSAGE FROM THE ORGANIZERS

Cyberspace is not an "emerging" domain anymore, but a potential collaborative scenario where it is possible for all sovereign nations to participate actively and daily. All over the world, governmental and non-governmental actors have developed cyber capabilities, which have triggered a reexamination of traditional notions of global power, as well as, priorities within nations.

The II Cyber Defense Conference, Western Hemisphere, held on the 28th and 29th of September 2020, and organized by the Inter-American Defense Board (IADB) and the Inter-American Defense Foundation (IADF), brought together more than 800 leaders and military authorities with the purpose of creating opportunities for cooperation between the main actors in cyber defense. Important to highlight is the participation of several sectors in the Conference, such as: military, government, academic, the private sector, and international organizations, among others in order to lay the groundwork for cooperation in cyber defense across the region in the short and long term.

Cyber defense is fundamental for conducting modern military operations. Considering that cyberspace is not limited to a single country, protecting our interests in cyberspace is a team sport. Developing a strong defense against malicious cyber activity requires a collective will to coordinate and collaborate in the development of cyber forces and the execution of cyber operations. Cyber threats to the security of the Western Hemisphere are becoming more frequent, complex, destructive, and coercive. We have to adapt to the constantly evolving cyber threat landscape.

The IADB supports its 29 member countries with activities and exercises focused on the generation and development of individual and collective cyber defense capacities, in order to strengthen the Hemisphere's policies and capacities. The IADB Cyber Defense Program, made possible by the generous contribution of the Government of Canada, works with regional and global partners to supplement and enhance existing initiatives.

Cyber defense represents the greatest threat and shared opportunity for cooperation in the Western Hemisphere, and the IADB and IDF will continue to act as a catalyst to strengthen relationships, foster multilateral interests, share best practices, and learn from allies and partners.

Cooperation in cyberspace will certainly lead to a more secure and prosperous future.

Sincerely,

Lieutenant General Luciano Penna
President of the Council of Delegates
Inter-American Defense Board

Isabel Niewola
Executive Director
Inter-American Defense Foundation

Organizers

Inter-American Defense Board

The Inter-American Defense Board (IADB), formally constituted in 1942, is the oldest regional defense organization in the world and is an entity of the Organization of American States (OAS). Its purpose is to provide services to the OAS and member states with advisory and educational assistance on military and defense matters in the Western Hemisphere.

Inter-American Defense Foundation

The Inter-American Defense Foundation (IDF) is dedicated to strengthening the Armed Forces of the Western Hemisphere by enhancing cooperation, establishing a productive dialogue, providing educational support, and developing capabilities on defense issues in the region. It supports the IADB in addressing systemic multilateral security and defense issues while working for a more secure future.

Partners

Government of Canada

The Government of Canada's Anti-Crime Capacity Building Program (ACCBP), administered by Global Affairs Canada, is supporting the Cyber Defense Program of the Inter-American Defense Board. It is designed to enhance cooperation and build capacity on cyber defense issues in the Western Hemisphere. It also supports Canada's longstanding commitment to cyber security in the Americas. Thanks to the support of the Government of Canada, this program is possible.

Fortinet

Fortinet offers businesses, service providers, and government organizations intelligent and uninterrupted protection across the expanding attack surface. Only the Fortinet Security Fabric architecture can deliver more critical security functions, whether in the network, applications, cloud, or mobile environments. Fortinet is ranked # 1 with the most security devices shipped globally to more than 385,000 customers.
http://www.fortinet.com

BlackBerry

BlackBerry provides intelligent security software and services to businesses and governments around the world. The company insures more than 500 million terminals, including 175 million cars on the road today. Headquartered in Waterloo, Ontario, the company leverages artificial intelligence and machine learning to deliver innovative solutions in the areas of cybersecurity, security, and data privacy solutions, and it is a leader in the areas of endpoint security management, encryption, and integrated systems. BlackBerry's vision is clear: to secure a connected future you can trust. Blackberry. intelligent security. Everywhere. For more information, visit BlackBerry.com and follow **@BlackBerry.**

Q - Mission Corp

Cyber-attacks are steadily intensifying, both in prevalence and complexity and having potential impact on individuals, organizations, nations, and society at large. Cyberspace knows no borders, and coalitions of governments and private sector partners are critical to mitigating risks and managing the cyber threat landscape. Q-Mission Corp., an innovator of cyber defense solutions, provides cyber capability enhancement with its Unified Cyber Platform, Q-Mission ™UCP, for the next generation cyber warrior to empower, develop, influence and operate. **www.qmission.net - demo@qmission.net**

ElevenPaths

ElevenPaths is Telefónica´s cybersecurity company, part of the Telefónica Tech holding, which focuses on preventing, detecting, responding and reducing the possible attacks that companies face. They guarantee the cyber resilience of their clients through a 24/7 support fully managed from eleven i-SOCs from around the world with global operational capacity. They also work with organizations and leading entities such as the European Commission, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, IADF, EuroPol, INCIBE, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Industrial Cybersecurity Center (CCI) and APWG.

III. SUMMARY

II Cyber Defense Conference

The II Cyber Defense Conference was held virtually from September 28 to 29, 2020, encouraging multilateral, bilateral and national cyber defense discussions, which serve to inform strategy and decision making at the highest level in the Western Hemisphere. The 2020 Conference reviewed and developed the key issues that had been addressed in 2019, considering a hemispheric approach to cyber defense.

Background

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 I Cyber Defense Conference in Bogotá, Colombia. The 2019 Conference focused on issues that require a multilateral perspective in order to gain a full understanding of them, as well as reaping the benefits of addressing these issues collectively. The full **report** of the 1st Cyber Defense Conference is available online.

Objectives

The objectives of the II Cyber Defense Conference, Western Hemisphere, include:

1. To strengthen cyber defense strategies and response capacity in the Western Hemisphere
2. To improve collaboration, communication, and information exchange within and between military institutions and the governments of the Americas
3. To promote multilateral interests
4. To strengthen relationships and promote learning
5. To support the establishment of the Cooperation Framework for Cyber Defense in the Americas

The first and second conferences were centered on strengthening regional cooperation in cyber defense along the following lines: threat awareness, cyber education and training, protection of critical infrastructure, regulatory frameworks, exchange of unclassified information and collaboration with the academic world and private sector agents. The Inter-American Defense Board (IADB) and the Inter-American Defense Foundation (FID) will continue to act as catalysts to strengthen partnerships, promote multilateral interests, and learn from their allies and partners.

Participants

The participants included the highest relevant authorities in cyber defense and cybersecurity, as follows: Ministers of Defense, Commanders of the Armed Forces, Commanders of Joint Cybernetic Commands and the people responsible for public security of the 29 Member States of the IADB. Also present were the private sector, academia and international organizations from the Western Hemisphere, among others.

IV. TOPICS ADDRESSED DURING THE CONFERENCE

This powerful event of multilateral cyber defense conversations covered the most relevant trending topics in the field of cyber defense, with speakers and presenters from all the related fields (defense, government, critical infrastructure, industry, academia, forces and state security bodies and international organizations and institutions). The comprehensive approach designed for this event delivered invaluable intellectual outcomes. The most relevant topics in the conference are as follows:

A) Cyberspace as a Field of Military Operations
B) The Need for Cooperation in Cyber Defense
C) The National Governance of Cyber Defense and Cybersecurity
D) The Need to Share Information
E) Training and Talent Retention
F) Cyber Resilience
G) Cyber Threat
H) The War of Disinformation
I) The Fight against Cybercrime
J) Protection of Critical Infrastructure
K) The Impact of Malicious Activities in Cyberspace
L) The Impact of COVID-19 on Cyberspace
M) The Protection of Democratic Principles and Values
N) Transparency
O) International Law Applied to Cyberspace
P) The Cyber Defense Industry
Q) Advanced Concepts of Cyber Defense
R) The Evolution and Future of Cyber Defense

Each topic will be addressed in detail below.

A) Cyberspace as a Field of Military Operations

Numerous statements and reflections by international leaders delved into the role of the armed forces in cyberspace and the particularities of cyberspace as a field of operations. The first consideration is that cyberspace is currently not an emerging domain but a domain in continuous evolution, a complex battlefield, a potential theater of war where all sovereign nations participate actively.

The five lessons learned by General Paul M. Nakasone, Commander of the United States Cyber Command, during the construction of the United States Cyber Command (USCYBERCOM) in the past decade are worth highlighting: focus on defense, consider cybersecurity as an automated team sport including public-private cooperation, develop a training program aimed at ensuring compliance with the mission, retain cyber defense personnel through the establishment of an attractive cyber defense career path, and transparency in communication with the nation's bodies.

> **Cybercommand is responsible for the game of war, operating abroad under the notion of persistent confrontation.**
>
> *General Paul Nakasone*
> Commander, United States Cyber Command

General Paul M. Nakasone confirmed that the Cybercommand is responsible for the game of war, operating abroad under the notion of persistent confrontation based on two premises: sharing information and intelligence with partners and allies and action based on defensive operations, information support operations and effects generation operations. In 2010, a few nations had a cyberspace component in their armed forces; now more than 120 nations have developed a capacity to use the internet as a weapon to generate military effects.

> **A cyber-attack using hybrid or asymmetric methods can potentially trigger a response in accordance with article 5 of the Alliance.**
>
> *Antonio Missiroli*
> Assistant Secretary General ESCD, NATO

In the same vein, Vice Admiral Myers, Commander of the U.S. Fleet Cyber Command, said that in order to face the deliberate and systematic cyberattack campaigns against the interests of the nation and its allies, the U.S. Fleet Cyber Command must obtain and maintain cyber superiority. It is authorized to seek cyber superiority on the battlefield to guarantee freedom of action and deny it to the adversary.

Lastly, Dr. Antonio Missiroli, Assistant Secretary General for Emerging Security Challenges Division of the North Atlantic Treaty Organization (NATO), noted that when we speak of hybrid or asymmetric threats, we refer to a wide spectrum of tools, techniques and instruments that blur the line between peace, crisis and war, as well as between the military and the civilian realms. The allies are certain that a cyber-attack using hybrid or asymmetric methods can potentially trigger a response in accordance with article 5 of the Alliance that would support a collective response to an attack on one of the allies.

B) The Need for Cooperation in Cyber Defense

The need for cooperation has been, perhaps, the most recurrent issue throughout the conference, with regard to international cooperation, and also with regard to public-private cooperation, universal digital cooperation and especially cooperation between the countries of the Western Hemisphere.

General Luciano Penna, President of the Inter-American Defense Board, emphasized that the Cyber Defense Conference represents the best opportunity for cooperation in the Western Hemisphere and that the IADB and its Foundation will continue to serve as catalysts to strengthen relations, promote multilateral interests, share best practices and learn with our partners.

Admiral Craig S. Faller, Commander of the United States Southern Command, notes that we face a global problem, the cyberspace environment is ubiquitous, and our physical location is so relevant that physical proximity provides us with a shared appreciation of problems. No single nation has the ability to solve cyberwarfare. During this conference we acquire an awareness of shared challenges and a sense of opportunities that we would not achieve if we did not work together.

Jennifer Loten, Director General of Canada's Bureau for International Crime and Terrorism, Global Affairs, highlighted Canada's commitment, together with the OAS, INTERPOL, UNODC and the IDF, to build an open, free and secure cyberspace in the Americas with the OAS capacity-building program.

Threats can exceed states' capacity for prevention, reaction and resilience, says Diana Abaunza, Vice Minister of Defense of Colombia, and therefore states need cooperation and joint responsibility strategies. In particular, the countries of the Western Hemisphere need the exchange of lessons learned, good practices, and public-private cooperation. Cooperation between all strategic sectors of the national critical infrastructure, industry and the university is necessary. The Ibero-American Cyber Defense Forum is an ideal instrument for cooperation on cyber defense in the Americas.

Cristian de la Maza Riquelme, Vice Minister of Defense of Chile, stressed that we must learn from the most advanced countries, but first we must raise awareness of cybersecurity and take advantage of the IADB and the OAS cooperation programs.

> **Threats can exceed states' capacity for prevention, reaction and resilience and therefore states need cooperation and joint responsibility strategies.**
>
> *Diana Abaunza Millares*
> Vice Minister of Defense, Colombia

Vice Admiral Ross Myers stated that all allies must learn from each other, from our successes and challenges, and work to strengthen mutual trust in our relationships and interoperability to compete and win this current global competition, especially with China and Russia. We cannot navigate the waters of cyberspace alone.

> **We cannot navigate the waters of cyberspace alone.**
>
> *Vice Admiral Ross A. Myers*
> U.S. Fleet Cyber Command

Antonio Missiroli underlined that cyberspace is a collective space and therefore cyber defense must be a shared responsibility. NATO works with more than 40 countries, as well as with numerous institutions, industries and the academic sector, and exchanges information in real time. An effective alliance and cooperation are crucial for success, which is why NATO will continue to maintain dialogue with the nations of the Western Hemisphere.

Bradford Willke, interim Deputy Director of the United States Cybersecurity and Infrastructure Security Agency (CISA), sees a positive trend in public-private cooperation and believes that cooperation and information sharing should be carefully planned because "this is about cooking and eating together; it is not a matter of everyone bringing cutlery and no food, or vice versa.

Antonio Missiroli highlighted the broad concept of public-private cooperation that should not focus exclusively on operators but also on innovators, with special attention to startups.

> **In information sharing, this is about cooking and eating together, not a matter of everyone bringing cutlery and no food, or vice versa.**
>
> *Bradford Willke*
> Deputy Director CISA, USA

The UN representatives presented another panorama of cooperation, closer to disadvantaged groups:

> **The UN has prepared a roadmap (Connect, Respect, Protect) to make technology available to everyone, especially to the most disadvantaged groups.**
>
> *Yu Ping Chan*
> UN

Yu Ping Chan, Senior Program Officer of the Office of the Special Adviser to the Secretary General of the United Nations, reports that the UN works to improve access to technology for all humanity and solve the associated risks. It has therefore developed a process consultation for digital cooperation involving governments, civil society, technology companies, scientists and experts.

As a result, the UN has prepared a roadmap (Connect, Respect, Protect) to make technology available to everyone. The objectives are: universal access to the internet, respect for human rights online, ensure digital inclusion; promote internet access to the most disadvantaged groups (women, disadvantaged groups, refugees, migrants) and create a more effective architecture.

Jamal Edwards, Technology Policy Adviser to the Office of the Special Adviser to the United Nations Secretary General, reminds us that the UN works to ensure universal digital security and trust with the establishment of the necessary measures to bridge the digital divide and be able to reach to the most disadvantaged groups. For this, it is necessary to build capacities among all states.

This initiative would help to achieve the sustainable development goals of the 2030 Agenda; in particular SDG-3 (Ensure healthy lives and promote well-being for all at all ages), SDG-4 (Ensure inclusive and equitable quality education and promote lifelong learning) and SDG-9 (Build resilient infrastructure, promote sustainable industrialization and foster innovation). In addition, it is an opportunity to raise the awareness of all the actors involved (governments, civil society and technology companies) in their responsibilities in the 2030 Agenda and their commitments to the digital future, and leaving no one behind.

Neil Walsh, Chief of the Cybercrime, Anti-Money Laundering and Counter-Financing of Terrorism Department of the United Nations Office on Drugs and Crime, indicates that there are countries with little capacity to defend themselves against cyber-attacks and cybercrime, which concerns and raises alarms at the UN.

The need to promote teamwork was another of the most recurrent themes of the conference and its close relationship with the issue of cooperation.

General Luciano Penna reminds us that cyber defense is fundamental to conducting modern military operations and cyberspace is not limited to a single country; protecting interests in cyberspace means teamwork. Together we are stronger. Jennifer Loten agrees with General Penna that together we are stronger and for this it is necessary to share information to increase the security of the collective by working together for a safer and more stable cyberspace.

> **Protecting interests in cyberspace means teamwork. Together we are stronger.**
>
> *LG Luciano Penna*
> President Inter-American Defense Board

Admiral Craig S. Faller believes that teamwork wins in all facets of war and prevents conflicts we never wish we had. Lastly, General Nakasone reminds us that cyberspace is an automated team sport. It is not effective to work alone. Cooperation with all the powers of the State is necessary.

C) The National Governance of Cyber Defense and Cybersecurity

Lieutenant General Guido Amin Naves, Brazil's Cyber Defense Commander, reminds us that good national governance entails top-down strategic planning that helps structure demand to focus on what is relevant. We must raise awareness at the political level so that they allocate the necessary resources, that they see the cost-benefit relationship clearly.

The participation of all sectors of the country is essential to face cyber threats, as Brigadier General Bayron Sergio Reyes Cifuentes, Vice Minister of Defense Policy and Planning of the Ministry of National Defense of Guatemala reminds us. You need a detailed plan and an immediate response.

> **Good national governance entails top-down strategic planning that helps structure demand to focus on what is relevant.**
>
> *LG Guido Amin Naves*
> Cyber Defense Commander Brazil

> **Gaining trust in institutions is a key factor in this era in which any source of information is mistrusted.**
>
> *BG Jay H. Janzen*
> Director General of Military Public Affairs for the Armed Forces Canada

Bradford Willke believes that awareness at all levels makes a difference in an organization or country, when all levels have the right knowledge. However, Brigadier- General Jay H. Janzen, Director General of Military Public Affairs for the Canadian Armed Forces, notes that gaining trust in institutions is a key factor in this era in which any source of information is mistrusted.

Regarding cyberoperations, General Patrice Sabourin, Director General Information Capabilities Force Development of the Department of National Defence of Canada, considers that they should be the responsibility of the armed forces and always under the control of the states.

D) The Need to Share Information

Information sharing and international collaboration make us stronger, wiser and better in our responsiveness, Jennifer Loten reminds us.

Sergio de la Peña, Deputy Assistant Secretary of Defense for Western Hemisphere Affairs of the Office of the Secretary of Defense of the United States, informs us that the US DoD has set goals to improve the exchange of information and sharing of knowledge in the hemispheric region: to deepen relations with the countries of the region to face the challenges of global security more effectively; to promote collaboration with the armed forces and state security bodies and agencies; to help strengthen regional collaboration to respond to humanitarian disasters in the region; and to help build more resilient defense and security forces.

> **Information sharing and international collaboration make us stronger, wiser and better in our responsiveness.**
>
> *Jennifer Loten*
> Director General, Bureau for International Crime and Terrorism
> Global Affairs Canada

Lastly, Cristián de la Maza Riquelme noted that information exchange between CSIRTs is needed in real time, with common protocols that facilitate automatic exchange.

E) Training and Talent Retention

General Nakasone reported on the need to develop a comprehensive cyber defense training program to ensure the fulfillment of the mission, based on the following criteria: train as you fight and fight as you train; individual training is developed by the armies and supervised by the Cyber Command; the use of joint training standards by all armies is necessary; it is necessary to establish a persistent environment of cyber defense training and it is necessary to build the triad of trust, capabilities and success, in other words wash, rinse and repeat.

> **It is necessary to train not only in technical skills but also in operational skills, from a military perspective, training to maneuver.**
>
> *BG Patrice Sabourin*
> Director General Information Capabilities Force Development
> Department of National Defence Canada

Likewise, several speakers spotlighted the enormous economic investment that countries are making towards training and developing their staff. This staff, in many cases, ends up in the private market, because it is not possible to compete with the salaries of that sector. This undoubtedly represents a significant competitive disadvantage for the armed forces. In order to avoid this situation, the armed forces must stop considering cyber defense as a secondary specialization and make it a fundamental specialty, a branch. To seek a competitive advantage, it is necessary to create a career progression through a foundational cyberspace specialty to recruit, train, develop, and retain staff.

General Sabourin agrees with General Nakasone: success does not lie in training but in retaining talent, offering the incentive of a special career on a permanent basis to those who have the potential. It is necessary to train not only in technical skills but also in operational skills, from a military perspective, training to maneuver.

Mark Hakun, Acting Deputy Chief Information Officer for Cybersecurity of the Department of Defense of the Office of the Chief Information Officer of the United States, believes that in order to train personnel, cooperation with universities is necessary. He noted that the Department of Defense of the United States is associated with more than 300 universities for cyber defense training.

Several experts agreed that certification does not necessarily show talent. Currently, it is not enough to have the certification to identify talent, but rather to have the necessary experience.

Alberto Roncallo, Founder/CEO of Q-Mission Corp., remarked that it is necessary to combine general knowledge and practices to orchestrate operations and not only train in the use of security devices.

Randy Pestana, Director of Education and Training in Cybersecurity at Florida International University, provided information on the situation of the demand for cybersecurity positions that in some way will impact retention of cyber defense personnel: there are currently more than 500,000 vacant positions in the cybersecurity area.

> **It is necessary to combine general knowledge and practices to orchestrate operations and not only train in the use of security devices.**
>
> *Alberto Roncallo*
> Founder/CEO of Q-Mission Corp.

Oscar Niss, Undersecretary of Cyber Defense of the Argentine Ministry of Defense, considers that it is easier to retain military personnel because of their sense of belonging to the group.

F) Cyber Resilience

As attacks become more sophisticated and persistent, Thomas C. Wingfield, Deputy Assistant Secretary of Defense for Cyber Policy in the Office of the Secretary of Defense of the United States, suggests moving from a cybersecurity-based model to one based on cyber resilience, focused on anticipation. Cyber resilience is necessary to anticipate and recover from cyber-attacks, ultimately, to effectively maintain the functionality of networks and activities.

> **As attacks become more sophisticated and persistent, it is important to move from a cybersecurity-based model to one based on cyber resilience, focused on anticipation.**
>
> *Thomas C. Wingfield*
> Deputy Assistant Secretary of Defense for Cyber Policy, USA

He believes that cybersecurity is based on a reactive mentality that assumes that the adversary will eventually gain access to our networks. We need to anticipate and prepare for cyberattacks rather than react when they are occurring. In the realm of national security, cyber resilience is more than a matter of protection, it is about maintaining operations and assuring the mission.

Cyber resilience is built on cybersecurity. Cybersecurity is the responsibility of the IT staff, but cyber resilience is the responsibility of the entire organization. It means understanding cyber resilience according to the NIST definition, the ability to anticipate, resist, recover and adapt to adverse conditions, stresses, attacks or compromises in systems that use or are enabled by cyber resources.

G) Cyber Threats

The current panorama of cyber threats and their evolution has been one of the most widely remarked issues at this conference. The approach on how to deal with them has been clearly open and focused, especially on specific cyber threats from States.

On several occasions, it was highlighted that cyber threats are increasingly frequent, complex, destructive and coercive, in their respective areas of responsibility in the Western Hemisphere. Today's cyber threats takes many different forms, appearing from multiple directions simultaneously. It is necessary to adapt to their constant evolution.

Some countries agreed that China and Russia challenge the free and open international order and wish to shape cyberspace to obtain diplomatic, economic and security advantages. China, Russia and also Iran and North Korea conduct persistent campaigns to obtain asymmetric advantages by carrying out cyberattacks below the threshold that would legitimize a military or any other response, undermining the security and prosperity of nations. For most countries, the goal is to win without going to war.

Vice Admiral Myers views persistent cyber-attack campaigns from Russia and China as a risk to the free world. Specifically, the Mandiant report and CrowdStrike denounce systematic campaigns of theft of intellectual property and industrial secrets by China. These campaigns have been denounced by the US, with little success so far.

> **The new cyber threats aim to impose a new world order.**
>
> *Diana Abaunza Millares*
> Vice Minister of Defense Colombia

The Chinese People's Liberation Army (PLA) deliberately and systematically carries out cyber espionage attacks in accordance with a five-year planning of war campaigns. General Janzen reminds us of a few words from Rand Waltzman: Russia considers itself to be in a permanent state of information warfare, while the West does not. Diana Abaunza believes that the new cyber threats aim to impose a new world order.

> **There are two types of organizations: those that know they have been attacked and those that do not know. Organizations must anonymously share all the information regarding the cyber-attacks sustained.**
>
> *Marc Asturias*
> Vice President of Government Affairs, Fortinet

Marc Asturias, Vice President of Government Affairs at Fortinet, emphasizes that it is necessaryfor all to be prepared and trained to face changing situations, while recalling that there are two typesof organizations: those that know they have been attacked and those that do not know that they have been attacked. For this reason, organizations must become aware that in order to face the current panorama of cyber threats, it is necessary to anonymously share all the information regarding the cyber-attacks sustained, including the kill chain, reduce detection time and consolidate public-private partnerships.

Cyberthreats do not distinguish between private and public sectors and they increase faster than physical threats, therefore states must give rapid responses, General Amin considers.

In relation to cyber threats, Neil Walsh observes that we must look beyond what we are used to and assume that we must be comfortable being uncomfortable, when we do not have all the information.

H) The War of Disinformation

The fight against disinformation is not necessarily at the level of cyber defense but at a political level. It incorporates elements of cyber defense, but it is a political issue that must be confronted politically with the support of cyber defense techniques and other instruments of power and influence, recalls Cristián de la Maza Riquelme.

General Janzen describes a disturbing landscape regarding disinformation, considering that artificial intelligence will take disinformation to a new level where it will be increasingly difficult to differentiate between information generated by a person and that generated by a machine. The intersection between the two forces, information and cyber, has enormous potential.

> **Artificial intelligence will take disinformation to a new level where it will be increasingly difficult to differentiate between information generated by a person and that generated by a machine.**
>
> *BG Jay H. Janzen*
> Director General of Military Public Affairs for the Armed Forces

We live in the era of post-truth in which objective facts have less influence in shaping public opinion than the appeal of emotions and religious beliefs. The following may be the era of post-reality.

I) The Fight Against Cybercrime

Cybercrime is on the rise, Jennifer Loten noted. The Canadian Centre for Cybersecurity considers cybercrime to be the most likely threat that a Canadian citizen will encounter; it is increasingly adaptive and effective in theft or fraud against Canadians.

For his part, Craig Jones, INTERPOL's Director of Cybercrime, reveals that INTERPOL is a neutral organization in all its activities and it only focuses on crime and not on defense activities. INTERPOL is developing several projects aimed at making it easier for nations to fight crime, with different specific purposes: promoting global coordination to ensure compliance with the law, developing information exchange platforms, providing the best information on the Budapest Convention, improving the cyber capabilities of countries in the Asian region, the Americas and Africa and organizing awareness campaigns.

INTERPOL relies on regular meetings with a group of global cybercrime experts and with the Singapore Fusion Centre. But the key to success is to develop a system for aggregating data from the police and the private sector in all countries and to create an effective global database, complying with different national standards.

J) Protection of Critical Infrastructure

We must seek the resilience of the national critical infrastructure through the sharing of information. Bradford Willke pointed out that the US government does not own critical infrastructure, but it guarantees its protection through public-private cooperation and the establishment of partnerships and standards.

"The Panama Canal is a critical infrastructure, the object of numerous cyber threats, but is resilient thanks, among other measures, to the use of manual mechanisms.

Ricaurte Vásquez Morales
Administrator of the Panama Canal

There are certain ubiquitous technologies (Microsoft, Adobe, Java, etc.) that are used by all critical infrastructure information and control systems. We must raise awareness about the challenge and the needs of cybersecurity, seeking the interdependence of all sectors and modern society. It is necessary to protect electoral processes, the supply chain and protect against ramsonware-type attacks that are increasingly used by unscrupulous opportunists who are only after money and are indifferent to the harm they cause on the way (health infrastructure, water and food distribution, etc.)

Ricaurte Vásquez Morales, Administrator of the Panama Canal, warns that to prevent critical infrastructures from being overwhelmed by cyber threats, it is essential to share information and examine the risks systemically. He stressed that the Panama Canal is an international critical infrastructure, the object of numerous cyber threats. Paradoxically, the Panama Canal is resilient thanks, among other measures, to the use of manual mechanisms.

K) The Impact of Malicious Activities in

During the conference, concrete data was delivered on the impact generated by malicious activities in cyberspace which helps to illustrate the magnitude of the damage.

Admiral Faller reported that the vicious circle that threatens democratic states and values is reinforced by criminal organizations that take advantage of this environment to earn (steal) 19 trillion dollars a year, carrying out transactions in cryptocurrency. This has to be stopped in some way.

Mark Asturias illustrated the fact: if all of Latin America were not to work for one year, that would be the amount of money lost to cybercrime.

"If all of Latin America were not to work for one year, that would be the amount of money lost to cybercrime.

Marc Asturias
Vicepresident Government Affairs, Fortinet

In 2019, the US lost between $225 and $600 trillion in software piracy and theft of secrets, says Vice Admiral Myers.

Neil Walsh observes that cyberattacks cause human deaths. Recently, numerous ramsonware-type attacks on hospital services have been reported. Even in Germany, a cyberattack was detected to have the aim of causing the death of a patient in a hospital.

L) The Impact of COVID-19 on Cyberspace

There have been many mentions of the increase in malicious activity that has taken advantage of the vulnerabilities associated with the pandemic, especially during the confinement phases.

Jennifer Loten highlighted that cybercrime has made the most of the COVID-19 pandemic by committing cyberattacks against the health sector (health institutions and medical research facilities), threatening the efforts made in prevention and medical care and conducting continuous influence campaigns and disinformation creating mistrust in official statements, data and statistics, abating the capacity to respond to the pandemic and generating uncertainty and anxiety in society. Canada is addressing this influence campaign and misinformation through awareness programs reporting these threats and providing accurate medical data and recommendations.

During the pandemic, activity related to cybercrime and cyberterrorism has increased and has been more effective by leveraging the decrease in victims' cyber defense capacity due to sick leave, confinement and telework. This has also affected the personnel responsible for cybersecurity areas and the members of the state security forces responsible for the fight against cybercrime and cyber-terrorism.

We have witnessed how far cyber-attackers are willing to go to achieve their objectives, said Antonio Missiroli. We have seen attacks on health systems, misinformation campaigns to generate mistrust, and attacks aimed at stealing information from vaccine development companies. In June, NATO issued a statement condemning these attacks in the context of the pandemic and calling attention to respect international law and for states to conduct responsible behavior in cyberspace.

Beneficial opportunities have also been observed and have been accelerated by the effect of the pandemic. General Nakasone asserted that the COVID-19 pandemic has sped up the need for virtual training, which will be something normal in the near future.

In a short time, the numbers of teleworkers have increased significantly, and countries have created virtual remote capacities in cooperation with the private sector. This effort has no turning back.

Likewise, Ricaurte Vázquez considers that the COVID-19 pandemic has also granted us the opportunity to work collaboratively, which did not occur previously.

M) The Protection of Democratic Principles and Values

> **The S DoD recognizes that the security of the nation depends on the security of the region, so cooperation is necessary with all the partners who share the same values of defense of democracy, respect for human rights, the rule of law and peace.**

Sergio de la Peña
Deputy Assistant Secretary of Defense for Western Hemisphere Affairs, Office of the Secretary of Defense, USA

Admiral Faller warns that everything we share in the Western Hemispheric Region is in peril from a vicious cycle of threats that includes young democracies and institutions that stand out for engaging in corruption, external state actors and foul nations in the region that are regrettably not democracies and do not share the same democratic values.

The value of the neighborhood makes us share democratic values, and a common appreciation for freedom, freedom of expression, human rights and the professionalization of the armed forces. These values are not universally shared so they provide us with a solid foundation of understanding and collaboration.

Sergio de la Peña indicates that the United States Department of Defense recognizes that the security of the nation depends on the security of the region, so cooperation is necessary with all the partners who share the same values of defense of democracy, respect for human rights, the rule of law and peace.

N) Transparency

A novel issue spotlighted in this conference is the need to change the paradigm in terms of communication at all levels of the State regarding cyber operations.

Specifically, General Nakasone underscored the need for a change of model in the way of communicating with the nation. For decades, the United States has been silent on everything related to cyber operations. It is increasingly difficult to maintain this posture of silence due to the unstoppable growth of activities in cyberspace, both public and private. Avoiding a silent stance on cyber defense and sharing information about cyber threats is part of the new normal.

> **Avoiding a silent stance on cyber defense and sharing information about cyber threats is part of the new normal.**

General Paul Nakasone
Commander, US Cyber Command

O) International Law Applied to Cyberspace

> **The Budapest Convention is the best international tool to fight cybercrime. It is a solid framework for cooperation on legal matters and for the defense of privacy, freedom of expression and human rights.**

Jennifer Loten
Director General Global Affairs, Canadá

Issues related to international law in cyberspace were one of the most addressed blocks in this conference, dealing with issues such as the Budapest Convention, the responsible behavior of states in cyberspace or gender balance.

Jennifer Loten believes that there are international legal instruments, standards, guides and good practices that aid in coordinating and taking action against cybercrime. Specifically, Canada considers the Budapest Convention the best international tool to fight cybercrime. It is a solid framework for cooperation on legal matters and for the defense of privacy, freedom of expression and human rights.

In addition, Canada promotes peace and security concerning women through the international agenda (Fellowship Program) and encourages the participation of women in the negotiations of the Open Working Group (OWG) on the Sustainable Development Goals and improving gender balance in cyberspace.

Thomas C. Wingfield considers that in addition to technological solutions, rules and procedures, it is essential to have legal authorities with responsibility in cyberspace to execute operations and missions with the speed and agility required, as well as to strengthen the international relations to promote responsible behavior by states in cyberspace in peacetime and that they can be held accountable for their actions.

P) The Cyber Defense Industry

Industry is part of the solution, but we need more secure technology, said Argentina's Under Secretary of Cyber Defense Oscar Niss. Most IT tools present vulnerabilities ranked in the top 30. The shorter the time between development and deployment, the higher the level of vulnerabilities.

The information technology and cybersecurity industry has to be responsible for the errors and failures of its products, just like any other industry. The industry must solve the problems that it has created. Governments must enforce the industry by requiring standards, certifications and by slowing down the implementation of technologies in critical sectors, such as national critical infrastructure and the defense sector. The industry is part of the solution.

Alberto Roncallo believes that one must have an open mind when it comes to acquiring cyber weapons. The defense departments go to the arms industry to acquire weapons and so do the criminals. In terms of acquiring cyber weapons, the same thing happens. And we must not forget the dark web which is also prepped to acquire weapons.

General Amin emphasizes that it is difficult to have a complete cyber defense capacity only with products from the national industry; the important thing is to master the codes and tools to ensure their continued use and customization.

> **We should not be obliged to use the latest technology but the most convenient.**
>
> *Oscar Niss*
> Under Secretary of Cyber Defense Ministry of Defense, Argentina

Q) Advanced Cyber Defense Concepts

During the conference, numerous speakers agreed that the technological future of cyber defense involves employing proactive, non-reactive concepts, driven by emerging technologies (machine learning and artificial intelligence) and based on three security aspects: secure by design, zero-trust, and endpoint security.

> **The organization that makes a difference is the one that distinguishes technological opportunity at the right time. Now is the time for cyber-physical systems, based on the convergence of the cyber domain and the physical domain.**
>
> *Phil Quade*
> CISO, Fortinet

Phil Quade, Fortinet CISO, believes that the organization that makes a difference is the one that distinguishes technological opportunity (cloud, BYOD, 5G, AI) at the right time; and now is the time for cyber-physical systems (CyPhy), based on the convergence of the cyber domain and the physical domain, with the exchange of data between domains at the three levels: core network, cloud and endpoints. Powerful organizations integrate these three parts with a real-time threat intelligence platform.

Phil Quade believes that a Cyphy is not simply a new technology but an opportunity to create great things in the world. It is the greatest technology that has been seen in the last 15 years to solve any problem related to leadership (governance of a country, national security and management of the economy).

Decision-making in cyber defense is a complex process that requires strong cyberspace situational awareness that provides data to the human mind for decision-making.

Dr. Martin Trevino, Member of the Board of Directors of the Inter-American Defense Foundation, considers that decision-making processes are currently taking technology into consideration and not the particularities of the human mind. The human mind is a master of deception.

People, decision makers (in this case), trust their own perception of the data and not the data itself, so it is necessary to include artificial intelligence that understands the human being in decision processes (Cognitive Augmented Intelligence) that takes into account the psychology of the decision maker two-fold: actively (identifying situations in which the decision maker has not considered some relevant information and showing it to the decision maker); and passively (eliminating cognitive errors and biases from the decisions that have been made under the influence of the emotions of the moment).

In order to achieve a supremacy of the decision, which is fundamental in cyber defense, it is necessary to have cognitive supremacy that is acquired through a process in which machines, the human being and increased cognitive intelligence intervene, concludes Martin Trevino.

> **In order to achieve a supremacy of the decision (fundamental in cyber defense), it is necessary to have cognitive supremacy that is acquired through a process in which machines, the human being and increased cognitive intelligence intervene.**
>
> *Martin Trevino*
> Member of the Board of Directors of the Inter-American Defense Foundation.

5G technology is an opportunity that must be directed towards good and diverted from evil. It is necessary to involve a layer based on zero trust security, national encryption and audits, and implement a more robust layer in the Defense and Critical Infrastructure sectors, says Cristián de la Maza Riquelme.

> **In implementing 5G, it is necessary to involve a layer based on zero trust security, national encryption and audits, and implement a more robust layer in the Defense and Critical Infrastructure sectors.**

Cristian de la Maza Riquelme
Deputy Minister of Defense, Chile

Patricia Diez Muñoz, Global Network and Customer Devices Security Manager in the Telefónica office, believes that organizations must prepare for the entry of 5G technology and the associated challenges. Confidence and resilience of its implementation is not only a technological issue, but it is fundamentally based on the solidity of national and international standards and their implementation and a robust configuration, operation and security management.

With 5G, the exposure surface increases exponentially due to increased risk because of the excessive growth of devices (billions of IoT devices including industrial IoTs) where any of them can be the weakest link; due to loss of control considering the confluence of numerous manufacturers (third party risk), due to the risks associated with virtualization and the radio spectrum, and due to the proliferation of attacks on end users through DDoS or MiTM.

The added improvements to 5G in relation to its predecessor 4G (better latency, speed/bandwidth, radio spectrum efficiency, device density, frequency utilization, degree of penetration) implies great opportunities and new use cases in all areas of activity of modern societies (health, industry, government, etc.).

Taking advantage of all these opportunities requires a secure implementation based on the principles of security by design, which indicates a multi-layered and proactive approach to security; zero-trust based networks; security of applications in users and end devices (endpoint security); design of new advanced security solutions powered by AI and ML and shifting of the paradigm of operational security management from SOC to SOAR. All these concepts are part of Telefónica's DNA.

> **Taking advantage of all these opportunities requires a secure implementation based on security by design, zero-trust, endpoint security, AI and orchestrators. All these concepts are part of Telefónica's DNA.**

Patricia Diez Muñoz
Global Network and Customizer Devices Security Manager, Telefónica GCTO Office

> **To "tame" the current chaotic, complex and uncertain environment of cybersecurity through solutions that comprehensively provide protection, detection and response in end devices, threat detection in mobile devices (MTD), continuous authentication, data loss prevention and secure web gateway.**

John E. McClurg
Senior Vice President and Chief Information Security Officer, Blackberry

Today's virtual world is dominated by chaos, complexity and conundrums. To provide order to this situation, John E. McClurg, Vice President and Chief Information Security Officer at Blackberry, proposes to move from a reactive model based on detection to a proactive model based on prevention through convergence, minimization of network cores and high connectivity, facing the increase in cyber risks due to the implementation of the internet of all things and teleworking and making the concepts of zero-trust reconcilable (only identified, authorized and confirmed accesses that are not malicious) and zero-touch (instant access to resources to improve productivity) through the effective use of machine learning and artificial intelligence technologies.

Specifically, he proposes a new comprehensive approach to "tame" the current chaotic, complex and uncertain environment of cybersecurity through solutions that comprehensively provide protection, detection and response in end devices, threat detection in mobile devices (MTD), continuous authentication, data lossprevention and secure web gateway.

R) The Evolution and Future of Cyber Defense

Antonio Missiroli considers that cyber defense has a leading role in the current technological environment of competition to master and adopt innovative technologies with disruptive potential (such as artificial intelligence or autonomous applications), in a safe way. It is important that countries adapt to the new strategic realities and be prepared for the future. To do this, NATO works in seven technological areas with disruptive potential: data, artificial intelligence, autonomy, space, hypersonic missile technology, biotechnology and quantum technology.

> **Oil is no longer the strategic resource, it is data.**
>
> *BG Jay H. Janzen*
> Director General of Military Public Affairs for the Armed Forces Canada

The Vice Minister of Defense of Colombia, Diana Abaunza, highlighted that the centers of excellence are the ideal instruments available to the states for the development of education, doctrine and cyber defense operations.

Lastly, General Janzen presented five considerations to take into account in the near future: it is not necessary to consider the virtual, physical and cognitive environments individually but jointly; data is a strategic resource; the conflict of the future will focus on imposing meaning on people, not on military power; the future war will focus on virtual networks and human networks–who influences whom?; and deterrence will become increasingly complex (information deterrence is difficult because disinformation activities do not cause serious one- time harm, it is the aggregation of information over time that does the real harm).

Isabel Niewola, Executive Director of the Inter-American Foundation, indicated that cooperation in cyberspace will inevitably lead us to a more secure and prosperous future, although it is necessary that efforts begin with understanding and culminate inaction.

V. GENERAL CONCLUSIONS:

1. Cyberspace is currently not an emerging domain but a continuously evolving domain, a complex battlefield, a potential theater of war.

2. To confront deliberate and systematic cyber-attack campaigns against national interests, cyber commands must obtain and maintain cyber superiority on the battlefield to guarantee freedom of action and deny it to the adversary.

3. No nation individually is fully equipped to solve cyberwar; international cooperation is necessary to build an open, free and safe cyberspace.

4. In this global digital competition, we must not leave behind the most disadvantaged groups; the UN works to eradicate this digital divide.

5. Achieving trust in institutions is a key factor in this era in which any source of information is mistrusted..

6. Information sharing and international collaboration make us stronger, wiser and better in our responsiveness.

7. The public cyber defense sector cannot compete in salaries with the private market, therefore, in order to retain expert personnel, it is necessary to establish an attractive career path based on a fundamental specialty or service within the armed forces.

8. In order to cope with increasingly sophisticated and persistent cyber-attacks, it is necessary to move from a cybersecurity paradigm to one of cyber resilience focused on anticipation.

9. Cyber threats are becoming more frequent, complex, destructive and coercive, undermining the security and prosperity of cyberspace. To deal with this situation, it is necessary for nations and organizations to anonymously share all the information regarding the cyberattacks sustained, reduce detection time and establish a solid public-private collaboration.

10. Artificial intelligence will take the war of disinformation to a new level where it will be increasingly difficult to differentiate between information generated by a person and that generated by a machine.

11. The COVID-19 pandemic has brought with it an increase in malicious activity in cyberspace, taking advantage of victims' decreased cyber defense capacity due to sick leave, confinement and telework; but it has also accelerated the establishment of new, more efficient forms and attitudes of remote work.

12. The security of each nation depends on the security of its geopolitical region and therefore cooperation is necessary with all the partners who share the same values of the defense of democracy, respect for human rights, the rule of law and peace.

13. A new communication model is necessary in cyber operations based on transparency within the national bodies.

14 The Budapest Convention can be a good international tool to fight cybercrime.

---

15 The technological future of cyber defense involves employing proactive and non- reactive concepts, driven by emerging technologies (machine learning and artificial intelligence) and based on three security aspects: secure by design, zero-trust andendpoint security.

Speakers

Lieutenant General
Luciano Penna
President
Inter-American Defense Board

Admiral
Craig S. Faller
Commander U.S. Southern Command
USA

Jennifer Loten
Director General
Bureau for International Crime and Terrorism
Global Affairs Canada

General
Paul Nakasone
Commander, U.S. Cyber Command
USA

Sergio De La Peña
Deputy Assistant Secretary of Defense for Western Hemisphere Affairs Office of the Secretary of Defense
USA

Thomas C. Wingfield
Deputy Assistant Secretary of Defense for Cyber Policy Office of the Secretary of Defense
USA

Phil Quade
CISO
Fortinet

Dr. Martin Trevino
Member of the Board of Directors
Inter-American Defense Foundation

Brigadier General
Jay H. Janzen
Director-General Military Public Affairs Canadian Armed Forces
Canada

Vice Admiral
Ross A. Myers
U.S. Fleet Cyber Command/U.S. 10th Fleet
USA

Craig Jones
Director of Cybercrime
INTERPOL

Patricia Diez Muñoz
Global Network and Customer Devices Security
Manager Telefónica GCTO Office

John E. McClurg
Senior Vice President and Chief Information Security Officer
Blackberry

Yu Ping Chan
Senior Program Officer/Team Leader, Digital Cooperation
Office of the Special Adviser to the Secretary-General United Nations

Jamal Edwards
Technology Policy Adviser
Office of the Special Adviser to the Secretary General
United Nations

Neil Walsh
Head of the Cybercrime, Anti-Money Laundering Section
United Nations Office on Drugs and Crime

Dr. Antonio Missiroli
Assistant Secretary General for Emerging Security Challenges Division
North Atlantic Treaty Organization

Isabel Niewola
Executive Director
Inter-American Defense Foundation

Panelists

Dra. Diana Abaunza Millares
Vice Minister of Defense
Colombia

Cristian de la Maza Riquelme
Deputy Minister of Defense
and Retired Vice Admiral of
the Chilean Navy

Teniente General
Guido Amin Naves
Cyber Defense Commander
Brazil

Brigadier General
Sergio Bayron Reyes Cifuentes
Vice Minister of Defense
Policy and Planning
Guatemala

Oscar Niss
Undersecretary of Cyber Defense
Ministry of Defense
Argentina

Tal Goldstein
Head of Strategy Centre for Cybersecurity
World Economic Forum

Dr. Ricaurte Vásquez Morales
Administrator
Panama Canal

Marc Asturias
Vice President of Government
Affairs
Fortinet

Bradford Willke
Assistant Director (acting) of the Cybersecurity
and Infrastructure Security Agency
USA

Mark Hakun
Acting Deputy Chief Information Officer
for Cybersecurity
Department of Defense
Office of the Chief Information Officer
USA

Brigadier General
Patrice Sabourin
Director General Information Capabilities
Force Development, Department of
National Defence,
Government of Canada

Alberto Roncallo
Founder/CEO
Q-Mission Corp.

Moderators

Chelsey Slack
Deputy Head of the Cyber
Defense Section
North Atlantic Treaty
Organization

Miguel Rego
Vice President for Defense and
National Security of Telefónica
Cybersecurity Tech and Former
General Director of INCIBE

Scott E. Jones
Head
Canadian Centre for Cyber Security
Communications Security Establishment
Canada

Randy Pestana
Director of Education and
Training Cybersecurity
Florida International University

Countries


Antigua and Barbuda


Argentina

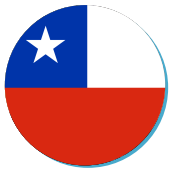

Barbados


Belize


Bolivia


Brazil


Canada


Chile


Colombia


Dominican Republic


Ecuador


El Salvador


Granada


Guatemala


Guyana


Haiti


Honduras


Italy


Jamaica


Mexico


Nicaragua


Panama


Paraguay


Peru


Portugal


Saint Kitts and Nevis


Spain


Surinam


Trinidad and Tobago


United Kingdom


United States


Uruguay


Venezuela

Organizations

World Economic Forum

North Atlantic Treaty Organization

INTERPOL

United Nations

Florida International University

Agenda

28 September

Day 1

	INAUGURATION
09:00	**Collaboration in Cyberspace in the Western Hemisphere** Lieutenant General Luciano Penna, President, Inter-American Defense Board
09:10	**Strengthening Partnerships to Counter Threats in Cyberspace** Admiral Craig S. Faller, Commander, U.S. Southern Command, USA
09:20	**Canada's Commitment to Cyber in the Americas** Jennifer Loten, Director General, Bureau for International Crime and Terrorism, Global Affairs Canada, Canada
	PROGRAM BEGINS
09:30	**Mission Accomplishment in the "New Normal"** General Paul Nakasone, Commander, U.S. Cyber Command, USA
10:00	**Empowering Cyber Resilience in the Western Hemisphere** Sergio de la Peña, Deputy Assistant Secretary of Defense for Western Hemisphere Affairs, Office of the Secretary of Defense, USA Thomas C. Wingfield, Deputy Assistant Secretary of Defense for Cyber Policy, Office of the Secretary of Defense, USA
10:45	BREAK
11:00	**Cyber Physical Systems: New Tools for Decision-Makers** Mr. Phil Quade, CISO, Fortinet
11:30	**Advanced Concepts in Cyber** Dr. Martin Trevino, Board Member, Inter-American Defense Foundation
10:45	BREAK
14:00	**PANEL: Cyber Defense Strategies - Leadership, Legislation and Budgets** Devising and advancing multifaceted cyber defense strategies for the future requires visionary leadership, comprehensive legislation and dedicated budgets, especially in times of crisis. **Panelists:** • Cristian de la Maza Riquelme, Vice-Minister of Defense and Retired Vice Admiral of the Chilean Navy, Chile • Dr. Diana Abaunza Millares, Vice-Minister of Defense, Colombia • Lieutenant General Guido Amin Naves, Cyber Defense Commander, Brazil **Moderator:** Miguel Rego, Vice President for Defense and National Security at Telefonica Cybersecurity Tech and
14:50	Q&A

Agenda

28 September — Day 1

15:00	**PANEL: Collaboration in Cyberspace** The private sector is essential in meeting today's complex cyber challenges and industry is part of the solution when increasing capabilities. **Panelists:** • Oscar Niss, Undersecretary of Cyber Defense, Ministry of Defense, Argentina • Brigadier General Sergio Bayron Reyes Cifuentes, Viceminister of Defense Policy and Planning, Guatemala • Tal Goldstein, Head of Strategy, Centre for Cybersecurity, World Economic Forum Moderator: Chelsey Slack, Deputy Head, Cyber Defence Section, North Atlantic Treaty Organization (NATO)
15:50	Q&A
16:00	**BILATERAL MEETINGS** Virtual meeting rooms will be made available to hold bilateral meetings in 20 minute slots.
18:00	END OF CONFERENCE DAY ONE

29 September — Day 2

09:00	**PANEL: Defining and Protecting Critical Infrastructure** Cross-sector cooperation with multiple stakeholders is essential to protecting critical infrastructure and is a shared responsibility. **Panelists:** • Dr. Ricaurte Vásquez Morales, Administrator, Panama Canal • Marc Asturias, Vice President, Government Affairs, Fortinet • Bradford Willke, Assistant Director (Acting), Cybersecurity and Infrastructure Security Agency (CISA), USA **Moderator:** Scott E. Jones, Head, Canadian Centre for Cyber Security, Communications Security Establishment, Canada de las Comunicaciones, Canadá
09:50	Q&A
10:00	**The Intersection of Information and Cyber Conflict – Implications for Western Democracies** Brigadier-General Jay H. Janzen, Director-General Military Public Affairs, Canadian Armed Forces, Canada
10:20	**US Navy's Fleet Cyber Command Perspectives on Cyber Espionage, Influence & Attacks** Vice Admiral Ross A. Myers, U.S. Fleet Cyber Command/U.S. 10th Fleet, USA
10:40	BREAK

Agenda

29 September

Day 2

11:00	**INTERPOL Global Cybercrime Programme – Aggregation as the Key Enabler** Craig Jones, Cybercrime Director, INTERPOL
11:20	**Securing the 5th Domain - 5G** Patricia Diez Muñoz, Global Network and Customer Devices Security Manager, Telefónica GCTO office
11:40	**The New Reality: Bringing Order to Chaos with Unified Endpoint Security** John E. McClurg, Senior Vice President and Chief Information Security Officer, Blackberry
12:00	BREAK
14:00	**PANEL: Future of CyberTalent – Readiness andTraining** Multi-level cyber education and training are essential to strengthening a culture of awareness and developing the appropriate technicalskills, which ultimately translate to improved capability and capacity. **Panelists:** • Mark Hakun, Acting Deputy Chief Information Officer for Cybersecurity, Department of Defense, Office of the Chief Information Officer, USA • Brigadier-General Patrice Sabourin, Director General Information Capabilities Force Development, Department of National Defence, Canada • Alberto Roncallo, Founder/CEO, Q-Mission Corp. **Moderator:** Moderator: Randy Pestana, Director of Education and Training, Cybersecurity, Florida International University
14:50	Q&A
15:00	**UN Roadmap for Digital Cooperation: from Countering Cybercrime to Achieving the SDGs through Digital Trust and Security** • Yu Ping Chan, Senior Programme Officer/Team Leader, Digital Cooperation - Office of the Special Advisor to the Secretary-General, United Nations • Jamal Edwards, Technology Policy Advisor, Office of the Special Advisor to the Secretary-General, United Nations • Neil Walsh, Chief of the Cybercrime and Anti-Money Laundering Section, United Nations Office on Drugs
15:30	**Cybrid Warfare** Dr. Antonio Missiroli, Assistant Secretary General for Emerging Security Challenges, North Atlantic Treaty Organization (NATO)
15:45	**Closing Remarks** Isabel Niewola, Executive Director, Inter-American Defense Foundation
16:00	**BILATERAL MEETINGS **** Virtual meeting rooms will be made available to hold bilateral meetings in 20 minute slots.
18:00	**END OF CONFERENCE DAY TWO**