

Session Title: Cybersecurity enhancement for the use and harnessing of ICTs in favour of sustainable development.

Session Format: Panel 60 minutes.

Theme: Cybersecurity, Trust and Privacy.

Proposer: Jimena Sierra.

Organizers: Juan Carlos Hernández Wocker and Víctor Manuel Martínez Vanegas.

Bio Juan Carlos Hernández Wocker.

He was born in the City of Mexico. He studied International Relations at the Colegio de México and obtained a scholarship from the British Council to study a Master's degree in International Relations and European Politics at the University of Edinburgh, Scotland. In 2001 he joined the Mexican Foreign Service. At the Ministry of Foreign Affairs, he was Director for Bilateral Relations with several European countries, and between 2004 and 2014 he served as Diplomatic Advisor to the Presidency of the Republic. Since November 2014 he holds the position of General Coordinator of International Affairs of the Federal Institute of Telecommunications.

Speciality: International Relations.

Bio Víctor Manuel Martínez Vanegas.

He was born in 1979, Mexico, is the Director of International Policy of the Federal Telecommunications Institute (IFT) since October 2014. He is responsible for elaborating and promoting the international policy of IFT in the fields of telecommunications, broadcasting and competition. Moreover, he coordinates IFT's cooperation with the Ministry of Communications and Transportation (SCT) in the processes carried out before competent international organizations in order to obtain orbital resources in favor of the Mexican State.

As part of his international experience, he has served as Alternate Head of the Mexican Delegation, in many meetings, Conferences and Assemblies of the Inter American Telecommunications Commission and the International Telecommunications Union in the period of 2010 and 2014.

Mr. Martínez has a Bachelor of Science in Law and holds many seminars and workshops in Telecommunications Services Regulations.

Speciality: International Telecommunications, free trade and standardization.

Proposer information: Jimena Sierra, Deputy Director of International Affairs, Federal Telecommunications Institute, México.

Email addresses of organizers (comma separated): asuntosinternacionales@ift.org.mx; victor.martinezv@ift.org.mx

Speakers: (No more than 5, no less than 3) Mails:

1. **Javier Juarez. Federal Telecommunications Institute of Mexico. Technical Community-Latin America and Caribbean.**
2. **Muataz Elsadig Ishag. Sudan CERT. Government. African Group.**
3. **Aparajita Bhatt. National Law University Delhi. Civil Society. Asia-Pacific Group.**
4. **Berger Cathleen. Mozilla. Private Sector. Western European and Others Group (WEOG).**
5. **Abdel-sadek Adel. Arab Center for Cyberspace Research-ACCR. Intergovernmental Organization.**

Relevance of the Issue

The Internet has transformed many aspects of our lives; many of these changes are for good. However, the Internet is also a powerful weapon, allowing anyone from a tech-savvy teenager to a State to carry out a cyber-attack. According to Global Risk Report 2018, issued annually by the World Economic Forum, cyber-attacks and data theft are among the most pressing risks that we will face in the next 10 years.

Cybersecurity risks are growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails.

Another growing trend is the use of cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning.

Therefore, in order to counteract this type of actions, it is necessary to implement cybersecurity strategies. According to the International Telecommunications Union (ITU), cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability

- Integrity, which may include authenticity and non-repudiation
- Confidentiality

In the case of Mexico, in November 2017, the National Cyber Security Strategy was issued as a document that establishes the vision of the Mexican State in this matter, based on the recognition of the importance of information and communication technologies (ICT), as a factor of political, social and economic development of the country. The strategy also recognizes the risks associated with the use of technologies and the growing number of cybercrimes and the need for a cybersecurity culture.

This strategy indicates that the increase in risks, threats and sophisticated computer attacks, the emergence of new forms and techniques to exploit vulnerabilities, as well as the increase of criminal behaviors that are committed through ICT, are circumstances that make cybersecurity a complex issue.

Content of the Session

In the current international context, for its part, there are a series of efforts focused on the establishment of international cooperation schemes, recommendations to protect critical infrastructure, standards that reduce the levels of vulnerability of communications, guidelines for the collaboration of all those involved, creation of CSIRTs and establishment of a cybersecurity culture. These are tools that could be useful for all stakeholders to enrich their perspectives with respect to cybersecurity.

Furthermore, as part of the economic agenda inside the different countries the digital transformation and development of ICTs play relevant roles, one important issue to consider in this sense is the need for resilience and better security to mitigate possible disruption of economic and social activities by cybersecurity incidents.

Traditionally understood as breaches of availability, integrity and confidentiality of ICTs and data, cybersecurity incidents are increasingly frequent and sophisticated. They can disrupt the activities of all businesses larger firms, governments and individuals and generate financial and reputational harm.

Interventions

Based on the above, the proposed panel aims to discuss the threats related to surveillance, privacy, resilience and security associated with the growing digitization, which has caused these risks to become increasingly complex, especially for data circulating through the Internet infrastructures.

The panel also seeks to promote discussion about the digital security of the critical infrastructure and the resilience of the network, as well as addressing issues such as network stability, computer attacks, culture and education about cybersecurity, the development of the culture of security in the user and education or creation of capacities, taking a focus towards sustainable development.

In the light of the above, a group of experts from Africa, Latin America, Middle East, Asia Pacific and Europe, from the academy, government, technical community, private sector and international organizations will debate the next issues:

- The relevance of the ICTs as a factor for the social and economic development.
- The necessity to improve the culture, educations programs and awareness - rising about the cybersecurity.
- The increase of risks, cybernetics attacks and emergence of new technologies to take advantage of the vulnerabilities of the ICTs products.
- The interchange of good practices in cybersecurity.
- The actions aimed to the development, adoption and enhancement of standards and technical criteria in cybersecurity.

Discussion topics will include:

- Education and awareness – rising about Cybersecurity.
- Programmes aimed to provide relevant knowledge and skills.
- Research, development and innovation on ICTs.
- Standardization and technical criteria.
- Legal framework.

Diversity

1. Male: Javier Juarez. Federal Telecommunications Institute of Mexico. Technical Community-Latin America and Caribbean.
2. Male. Muataz Elsadig Ishag. Sudan CERT. Government. African Group.
3. Female. Aparajita Bhatt. National Law University Delhi. Civil Society. Asia-Pacific Group.
4. Female Berger Cathleen. Mozilla. Private Sector. Western European and Others Group (WEOG).
5. Male. Abdel-sadek Adel. Arab Center for Cyberspace Research-ACCR. Intergovernmental Organization.

Onsite Moderator

Female. Arda Gerkens. EOKM/ Senate. Civil Society. Western European and Others Group (WEOG).

Online moderator

Edna Ferrer. Federal Telecommunications Institute. Mexico.

Rapporteur

Jimena Sierra. Federal Telecommunications Institute. Mexico.

Online participation

Online attendees will have a specific time after each intervention to give them the queue, the workshop moderator will have the online participation session open, and will be in close communication with the workshop's trained online moderator, to make any adaptations necessary as they arise, in order to give online participants opportunity to ask, comment and participate remotely.

Discussion Facilitation

Panel discussion. The workshop will begin with a brief introduction presented by the moderator who is going to explain the main objective of the panel and the detonator questions over which the panel will be addressed. Panelists will subsequently have 5 minutes to explain their views on the preliminary target points of the panel previously presented by the moderator.

Following these interventions, the moderator will ask the questions to the panelists to initiate a debate between them. Subsequently, the panel will be open to the public so that the audience can participate with comments or questions remotely and in site.

Finally, the moderator will have a few minutes to complete the most important points discussed at the meeting.

Sustainable Development Goals

"The Sustainable Development Goals Report 2017 of the Secretary- General of the United Nations, point out that the Infrastructure, industrialization and innovation are three drivers of economic growth. When inclusivity, resilience and sustainability are factored into the implementation of these driving forces, economic growth can support sustainable development. This report shows that the coverage by a mobile cellular signal has become almost universal. In 2016, 95 per cent of the world's population was in range of at least a second-generation (2G) signal and 84 per cent received at least a third-generation (3G) signal.

The workshop proposal is directly linked to Goal 9 of the SDGs: "Build resilient infrastructures, promote inclusive and sustainable industrialization and promote innovation". In this regard, this Objective recognizes that greater investment in infrastructure is essential to achieve sustainable development and empower communities in many countries.

It also highlights that one of the goals of the said Objective is to "significantly increase access to information and communication technology and to strive to facilitate universal and affordable access to the Internet in the least developed countries at the latest in 2020. "

XXII. Additional Reference Document Link (Optional)

- Informe de los Objetivos de Desarrollo Sostenible 2017, Naciones Unidas.

Link: http://ggim.un.org/documents/TheSustainableDevelopmentGoalsReport2017_Spanish.pdf

- "Securing the Net: Global Governance in the Digital Domain"
http://www.ggfutures.net/fileadmin/user_upload/publications/130826_GG2022_Cyber_Report_web.pdf

- World Development Report 2016: Digital Dividends, World Bank.

Link: <https://goo.gl/FD4Fsh>

- Cyber Security: Turning National Solutions Into International Cooperation
<https://books.google.com.mx/books?id=rn4iHxIJ9hwC&printsec=frontcover&dq=cybersecurity&hl=es-419&sa=X&ved=0ahUKEwi9jbKq7ZfbAhVOeKwKHY6nBXsQ6AEIKjAA#v=onepage&q=cybersecurity&f=false>

- Broadband Policies for Latin America and the Caribbean: A digital Economy Toolkit, Organization for Economic Cooperation and Development; Inter-American Development Bank

Link: <https://goo.gl/QNFZbm>

- Open Statement from the Broadband Commission for Sustainable Development to the UN High-Level Political Forum "Ensuring that No One is Left Behind".

Link: <https://goo.gl/p3RFI4>

- IGF Policy Options for Connecting the Next Billion. Final Compilation (Phase 1)

Link: <https://goo.gl/kw6rnw>

- Policy Options for Connecting & Enabling the Next Billion(s): Phase II

Link: <https://goo.gl/RjMGnX>

- Cómo superar las barreras al despliegue de servicios de comunicaciones móviles. Hoja de ruta de México, Banco de Desarrollo de América Latina

Link: <https://goo.gl/wBe1aD>

- Global Risk Report 2018

Link: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

- Estrategia Nacional de Ciberseguridad

Link:

https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf