INSTITUTO FEDERAL DE TELECOMUNICACIONES

OFICINA DEL COMISIONADO
JAVIER JUÁREZ MOJICA
IFT/100/PLENO/OC-JJM/007/2018

Ciudad de México, a 9 de marzo del 2018.

JUAN JOSÉ CRISPÍN BORBOLLA
SECRETARIO TÉCNICO DEL PLENO
P R E S E N T E

En cumplimiento a lo dispuesto en el artículo 23, fracción II, de la Ley Federal de Telecomunicaciones y Radiodifusión, y en el artículo 15, fracción I, del Estatuto Orgánico del Instituto Federal de Telecomunicaciones, me permito enviar para conocimiento del Pleno de este Instituto el informe sobre mi participación en el taller "Seguridad digital y resiliencia en infraestructura crítica y servicios esenciales", realizado por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), así como sobre diversas reuniones bilaterales que tuvieron lugar del 13 al 16 de febrero del año en curso en París, Francia.

Se anexa el informe de actividades correspondiente al evento mencionado.

Sin otro particular, reciba un saludo.

ATENTAMENTE,

JAVIER JUÁREZ MOJICA
COMISIONADO

387
Instituto Federal de Telecomunicaciones
RECIBIDO
Con anexo
09 MAR. 2018
AREA STP
NOMBRE Y HORA Juan 09:26 hrs

Insurgentes sur 1143,
Col. Nochebuena, C.P. 03720
Delegación Benito Juárez,
México, D.F.
Tels. (55) 5015 4000

INSTITUTO FEDERAL DE TELECOMUNICACIONES

INSTITUTO FEDERAL DE TELECOMUNICACIONES
OFICINA DEL COMISIONADO
JAVIER JUÁREZ MOJICA

Ciudad de México, a 8 de marzo del 2018.

PLENO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES
PRESENTE

Informe que presenta el Comisionado Javier Juárez Mojica respecto a su participación en representación del Instituto Federal de Telecomunicaciones en el taller "Seguridad digital y resiliencia en infraestructura crítica y servicios esenciales" y en otras reuniones realizadas en París, Francia, durante los días 13 al 16 de febrero del 2018.

Bajo el auspicio de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) se llevó a cabo el taller "Seguridad digital y resiliencia en infraestructura crítica y servicios esenciales" con la finalidad de debatir e intercambiar opiniones sobre el impacto de la transformación digital en las políticas públicas de seguridad digital, finanzas, energía, transportes y manejo de riesgos con el objetivo de identificar elementos comunes que puedan integrarse a las políticas de alto nivel contempladas en la iniciativa *Going Digital: Making the Transformation Work for Growth and Well-Being*, proyecto concebido para que los países de la OCDE aprovechen al máximo los beneficios de la digitalización.

Dentro de los temas abordados en el taller destacan:

- Los cambios en la protección de infraestructura crítica y la administración de riesgos de seguridad como resultado de la transformación digital.
- Mejores prácticas internacionales para promover la adecuada administración de riesgos digitales en las organizaciones.
- ¿Cómo promover la confianza entre gobiernos e instituciones para intercambiar información sobre amenazas, vulnerabilidades e incidentes?

Adicionalmente, la agenda de trabajo incluyó reuniones bilaterales con funcionarios de la OCDE pertenecientes a la División de Política Regulatoria y del Directorado de Ciencia, Tecnología e Innovación, con quienes se abordaron los resultados de la colaboración entre el Instituto y ese organismo internacional, además de futuros proyectos entre ellos que permitan profundizar la participación del IFT en la Red de Reguladores Económicos, órgano subsidiario del Comité de Política Regulatoria.

Asimismo, se llevó a cabo una reunión con la Embajadora Mónica Aspe, representante permanente de México ante la OCDE, con quien se abordaron posibles temas de cooperación que involucran al Instituto.

Insurgentes Sur 1143,
Col. Nochebuena, C.P. 03720
Delegación Benito Juárez,
México, D.F.
Tels. (55) 5015 4000

Por otro lado, se llevó a cabo una reunión con el Comisionado Pierre-Jean Benghozi, miembro del Comité Directivo de la Autoridad Reguladora de las Comunicaciones Electrónicas y de Correos (ARCEP) de Francia, instancia encargada de la asignación de frecuencias, licencias móviles, evaluación de tarifas, el control de calidad de los servicios y la publicación de indicadores sobre las redes y servicios de comunicaciones. Durante la reunión, el Comisionado Benghozi compartió la visión de ARCEP sobre diversos temas de regulación y administración del espectro tales como la "regulación basada en datos" (*régulation par la data*), la visión del Estado plataforma, neutralidad de la red, entre otros asuntos de interés para el IFT.

Tanto la participación en el taller como las reuniones bilaterales con otras autoridades permitieron fomentar el intercambio de experiencias y puntos de vista con reguladores y actores relevantes en el ámbito internacional, lo que contribuye a la adquisición de información relevante para el desarrollo de las actividades del IFT.

La intervención activa en los proyectos de organismos multilaterales como la OCDE y la interacción con homólogos y otras autoridades permiten tomar parte en el desarrollo de referentes internacionales en temas que corresponden a las facultades del Instituto.

Este informe se acompaña con el programa de actividades de la comisión internacional, así como con el programa del taller de la OCDE.

Atentamente

JAVIER JUÁREZ MOJICA
COMISIONADO

INSTITUTO FEDERAL DE TELECOMUNICACIONES

ANEXO

PROGRAMA DE ACTIVIDADES

13 AL 16 DE FEBRERO DE 2018

JUEVES 15 DE FEBRERO 2018

1. Taller "Seguridad digital y resiliencia en infraestructura crítica y servicios esenciales".

2. Reunión con Nick Malyshev, titular de la División de Política Regulatoria de la Organización para la Cooperación y el Desarrollo Económicos.

VIERNES 16 DE FEBRERO 2018

1. Taller "Seguridad digital y resiliencia en infraestructura crítica y servicios esenciales", en el marco del proyecto Going Digital, *de la Organización para la Cooperación y el Desarrollo Económicos.*

2. Reunión con Karine Perset, del Directorado para la Ciencia, Tecnología e Innovación, y Anne Carblanc, responsable de los temas de información comunicaciones y política del consumidor, de la Organización para la Cooperación y el Desarrollo Económicos.

3. Reunión con Sam Paltridge, analista senior, y Verena Weber, analista de política económica, del Directorado para la Ciencia, Tecnología e Innovación de la Organización para la Cooperación y el Desarrollo Económicos.

4. Reunión con el Comisionado Pierre-Jean Benghozi, integrante del Consejo Directivo de la Autoridad Reguladora de las Comunicaciones Electrónicas y de Correos (ARCEP) de Francia.

5. Reunión con la Embajadora Mónica Aspe, representante permanente de México ante la Organización para la Cooperación y el Desarrollo Económicos.

insurgentes sur 1143,
Col. Nochebuena, C.P. 03720
Delegación Benito Juárez,
México, D.F
Tels. (55) 5015 4000

OECD Going Digital Project:
Making the Transformation Work for Growth and Well-Being

Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services

Digital Security in Energy, Transport, Finance, Government, and SMEs

15-16 February 2018

OECD Conference Centre, 2 rue André Pascal, Paris, France

Registration at Goingdigital@oecd.org

OECD Going Digital Collaborative Project co-organised by:

OECD Directorates for Science Technology and Innovation (STI), Public Governance (GOV), Financial and Enterprise Affairs (DAF) - International Energy Agency (IEA) - International Transport Forum (ITF) - OECD Centre for Entrepreneurship, SMEs, Local Development and Tourism

The workshop will discuss the effects of growing digital transformation on the resilience of critical infrastructures and essential services which rely increasingly on cross-border digital infrastructure. It will explore cross-sector dependencies and avenues for coordination among stakeholders within countries as well as across borders.

It will also discuss how an integrated whole-of-government approach to digital transformation of the economy and society can best help address the protection of critical infrastructure and essential services against digital security risk.

To this end, the workshop will bring together experts from several policy communities focusing on digital security, energy, finance, transports, national risk management and SME in a collaborative discussion, cutting across silos of expertise, with a view to identifying common high-level policy messages for the *OECD Going Digital project*.

9 Jan. 2018

The ongoing digital transformation of the economy and society holds many promises to spur innovation, generate efficiencies, and improve services, and in doing so boost more inclusive and sustainable growth as well as enhance well-being.

Highly automated processes enabled by big data and artificial intelligence, distributed in the cloud, and combined with technologies bridging the digital and physical worlds (Internet of Things) are enabling digital transformation of critical infrastructure and essential services. Smart grids, Fintech, and automated vehicles for example are unleashing new opportunities for innovation and growth, environmental protection and other important global challenges, while transforming business processes and markets. Digital technologies also improve how governments manage critical risks and crises and how they build resilience in society.

But these benefits go hand-in-hand with disruptions. Our interactions with one another and with society more broadly are being transformed, as are the nature and structure of organisations and markets, raising important issues such as around jobs and skills and how to ensure that technological changes benefit society as a whole, among others.

A key challenge for policymakers is to identify the policy mix that will enable their economies to maximise the benefits of an increasingly digitalised global economy and adequately address the related challenges. Only a coherent and comprehensive policy approach will have the scope to harness the benefits of the digital transformation for stronger and more inclusive growth.

To chart the road ahead, the OECD has launched a multidisciplinary project on *Going Digital: Making the Transformation Work for Growth and Well-Being*. It aims to help policymakers in all relevant policy areas better understand the digital revolution taking place across all economic sectors and in the society as a whole.

This project brings a whole-of-OECD perspective through the involvement of 14 OECD committees and 9 directorates. It will articulate recommendations for pro-active policies that will help to drive greater growth and societal well-being and address the challenges of slow productivity growth, high unemployment and growing inequality in many countries. It will also develop an integrated whole-of-government policy framework to guide governments in adopting the range of policies needed to ensure a holistic and coherent policy approach in the digital age.

One important issue inherent to digital transformation is the need for resilience and better security to mitigate possible disruption of economic and social activities by digital security incidents. Traditionally understood as breaches of availability, integrity and confidentiality of ICTs and data, digital security incidents are increasingly frequent and sophisticated. They can take advantage of the global nature of the Internet to rapidly propagate across jurisdictional, organisational and sectoral boundaries, as demonstrated by the recent Wannacry, notPetya, and Dyn attacks. Digital security incidents can generate financial, reputational as well as physical damage as demonstrated by interruptions of electricity grids in 2015 and 2016.

Higher dependency on digital technologies increases the potential for security vulnerabilities along value chains and the exposure to security threats which can create disruptions in the activities of businesses, including SMEs, governments and individuals. Such security incidents could evolve into large scale crisis affecting infrastructures critical to the functioning of the economy and society such as essential energy, transports, finance, or government services. In addition to such catastrophic scenarios, digital security incidents affecting critical infrastructures and essential services can also have subtle but long-term negative effects by limiting innovation, slowing down adoption of new technologies, undermining trust in the digital environment as well as hampering the digital transformation and its related benefits.

Objectives of the workshop

The workshop will discuss the effects of growing digital transformation on the resilience of critical infrastructures and essential services which rely increasingly on cross-border digital infrastructures. It will explore cross-sector dependencies and avenues for co-ordination among stakeholders within countries as well as across borders.

It will also discuss how an integrated whole-of-government approach to digital transformation of the economy and society can best help address the protection of critical infrastructures and essential services against digital security risk.

To this end, the workshop will bring together experts from several policy communities focusing on digital security, energy, finance, transports, national risk management and SME in a collaborative discussion, cutting across silos of expertise, with a view to identifying common high-level policy messages for the *OECD Going Digital project*.

Issues and challenges to be discussed include in particular:

- **To what extent is digital transformation changing the protection of critical information infrastructures and the management of digital security risk?** How is the risk evolving along the value chain, including beyond/across sectors? Are "hybrid threats" as well as threats against confidentiality and privacy becoming increasingly challenging in relation to the protection of critical infrastructures and essential services against digital security risks? What is the role of individuals?
- **To what extent are cross-border and cross-sector interdependencies addressed?** How can stakeholders take into account globally distributed digital infrastructures (e.g. Cloud computing) as well as potential systemic risk from widespread vulnerabilities (e.g. Meltdown and Spectre)?
- **What are good policy practices to encourage digital security risk management by all organisations, including SMEs?** What is the right balance between mandatory and voluntary policy measures to protect critical infrastructures and essential services? What should be the respective roles of digital security agencies, public safety departments and sectoral regulators? Are SMEs a weak link in essential services' value chains?
- **How can governments foster trust with and among private operators** to enable information sharing on threats, vulnerabilities and incidents? How can they encourage information sharing between operators competing in the same sector? How can SMEs be included in trust frameworks?

In each session, panellists and workshop participants will address the above issues and challenges and share related good practice with respect to a different policy area, with the exception of the SME policy perspective which will be addressed in each session. Sessions' moderators will then gather in a final session to identify and discuss the key policy messages to be delivered from the workshop to the broader Going Digital Project.

Expected participants include representatives from:

- Government bodies in charge of digital security, energy, finance and transports policy and regulation, as well as ministries and agencies in charge of critical risk and crisis management policy;
- Business and industry, including SMEs, in particular operators of critical infrastructures and essential services, as well as digital security firms;
- Civil society, academia and the technical community.

Preliminary Draft Agenda

The workshop language will be English. With the exception of panellists' presentations, the proceedings will not attribute discussions to named individuals or organisations.

DAY 1 - 15 February 2018

14:00 - 14:15	**Welcome / opening: Digital security of critical infrastructure and essential services within the OECD Going Digital project**	15 minutes

These opening remarks will introduce the broader OECD Going Digital project and explain how the workshop will contribute to its objectives.

- Keynote speakers (tbd)

14:15 - 15:45	**Session 1. Digital security risks in the financial sector**	90 minutes

As a custodian of financial assets with a significant dependence on digital technologies, the financial sector has been a major target of cybercrimes and has been working to address digital security risks for many years. The sector is also internationalised with significant cross-border infrastructure to manage cross-border payment, inter-bank transfer and foreign exchange settlement systems.

As a result, financial regulators have placed increasing attention on digital security risks at the institutions they oversee, and implemented a number of international coordination initiatives to share experience and ensure the integrity of the common systems on which they depend.

At the same time, policymakers and regulators have an interest in ensuring an efficient and innovative financial system that meets the needs of its users, creating an effort to balance the need for high security standards to maintain the integrity of the financial systems while ensuring sufficient openness to new innovation.

This session will explore these issues with a focus on the payment capture and settlement systems, which has seen significant innovation as the result of new technologies for making and capturing payments. It will examine how new entrants (e.g. fostered by EU's Revised Payment Service Directive (PSD2)) and traditional infrastructure providers manage the potentially competing objectives of openness to innovation and the need to maintain integrity.

Format: [proposed] presentations and panel discussion followed by open discussion with workshop participants
Moderator: [tbc: policy maker or industry association]
Panellists:

- [tbc: regulator; FS-ISAC; other]
- [tbc: Swift representative]
- [tbc: Mastercard representative]
- [tbc : FinTech payments company representative]

Coffee Break 15:45 – 16:00

16:00 - 17:30	Session 2. Digital security risks to energy infrastructure: electricity	90 minutes

Maintaining a stable supply of energy is increasingly critical to all aspects of human life; attacks to energy infrastructure can therefore be particularly disruptive.

The energy sector has been an early adopter of digital technologies, which bring many opportunities but also many technical, security or regulatory challenges. Power utilities already in 1970s used emerging technologies to facilitate grid management and operation. But the growth of the IoT combined with the diversification and decentralisation of energy technologies will link millions of new small-scale prosumers and billions of devices into the electricity system. Digital technologies used in centralised energy systems are also changing, with a move from proprietary or vendor-specific solutions to newer open-protocol industry standards, more automation and a shift to cloud computing. These newer systems might have a higher general level of security, but lose the protection provided by secrecy of proprietary product design ("security through obscurity") and by the need for potential attackers to acquire knowledge highly specialised energy system . The attack surface is thus changing and vastly expanding.

While disruptions to energy systems caused by digital security incidents and attacks have so far been relatively limited when compared to more "traditional" causes such as extreme weather, notable examples do exist and energy systems can also increasingly be affected by generic attacks such as NotPetya. Credible low-probability, high-risk scenarios of attacks shutting down the entire electricity grid of a major economic region for a period of days or even weeks can be envisaged.

Building system-wide resilience depends on all actors and stakeholders being aware of the risks, maintaining proper cyber hygiene and incorporating security objectives into research and design. Full prevention of digital security attacks is impossible, systems must therefore be designed in a way to withstand shocks and be able to quickly recover, while preserving the continuity of critical infrastructure operations.

Format: Three presentations and panel discussion followed by open discussion with workshop participants

Moderator: Russell Conklin, Senior Policy Analyst, Office of International Affairs, US Department of Energy [invited]

Panellists:

- Professor Tim Watson, Director, WMG Cyber Security Centre, University of Warwick. [confirmed]
- Stefano Bracco, Knowledge Manager, EU Agency for the Cooperation of Energy Regulators (ACER). [invited]
- Energy Web Foundation, Rocky Mountain Institute. [invited]

End of Day 1

9:00 - 10:30 Session 3. Digital security risks to Transport infrastructure: automated vehicles **90 minutes**

The transport sector is an essential enabler for public services, freight transport and logistics, and provision of necessary mobility demand, including employment, education, trade, etc. Its underlying physical (and increasingly data-related) infrastructure is critical for a wide range of services from emergency services and law enforcement to waste disposal. Any major disruptions to transport infrastructure will thus have far reaching effects.

The wider transport sector is in the early stages of undergoing what many experts predict to be a revolution in terms of how mobility is provided. Key trends include ride-sharing platforms and vehicle automation; much of this being enabled through the emergence of big data analytics and progress in the field of data science. Here data can be seen both as a potential as well as a challenge.

The key trend of vehicle automation, particularly when combined with e-hailing, but possibly also with urban freight delivery, is likely to be among the first use cases to be implemented. In this context the enabling technology of car-to-car/-infrastructure communication needs strong data security safeguards to prevent digital security attacks on critical transport infrastructure and to ensure acceptable resilience levels in response to incidents.

Format: Presentations and panel discussion followed by open discussion with workshop participants

Moderator: Yves-Alexandre de Montjoye, Imperial College, Data Science Institute, UK [tbc]

Panellists:

- Gereon Meyer, Head of Strategic Projects, VDI/VDE Innovation + Technik GmbH, Germany [tbc]
- Philip King, Product Owner of cloud based services for Autonomous Driving cars, Volvo Cars
- Sebastian Rohr, CEO, accessec GmbH, Germany
- Demosthenes Ikonomou, Head of Information Security & Data Protection Unit, European Union Agency for Network and Information Security ENISA [tbc]

Coffee Break 10:30 – 10:45

10:45 - 12:15	Session 4. Digital security risks to Government and public services	90 minutes

Governments provide the apparatus for developing and administering laws and regulations to preserve public welfare and smoothly operating markets, and they also provide numerous public services, such as public safety, health, education and defence. As such, many of their facilities and agencies are critical infrastructure and providers of essential services. In recent years, governments have faced a growing deluge of threats, both targeted and untargeted, that are increasingly sophisticated, stealthy and dangerous.

Among the different forms of attacks on governments are those by cyber-criminals who hold government data for ransom; by State-sponsored actors who aim to steal State secrets (including diplomatic channels and even the personal information of civil servants); and by political activists to disrupt and deface government websites as a means to protest against policies they disagree with.

For governments, digital risk goes beyond vulnerabilities to digital security attacks. Public trust in governments per se is vulnerable to "hybrid" threats such as the use of online channels to spread disinformation campaigns that aim to influence political elections or erode social cohesion.

Many governments are still not able to mitigate advanced digital security attacks or agile enough to develop timely counter narratives to hybrid threats. This session will discuss the policies, procedures and structures to counter digital threats, in their several forms that target government.

Format: Three presentations and panel discussion followed by open discussion with workshop participants

Moderator: [tbd]
Panellists:

- Speaker from government of the United States
- Speaker from government of Finland
- Speaker from government of Republic of Korea (tbc)

Lunch Break 12:15 – 13:30

13:30 - 15:00	Session 5. Whole-of -Government Approaches to Digital Security in Critical Infrastructure and Essential Services	90 minutes

With digital transformation, governments are struggling to create the conditions for a higher level of digital security in all essential services and critical infrastructures. While many digital security risk and risk management practices are similar across sectors, some aspects are sector-specific, for example to take into account sophisticated technical equipment, particular market characteristics (e.g. value chain structure) and regulatory requirements (e.g. minimum service requirements), etc. Governments need to adopt whole-of-government frameworks to enable cross-cutting measures such as training and information sharing, as well as to increase sector-specific digital security risk management expertise and practices.

Governments' national digital security strategies and policies for Critical Information Infrastructure Protection (CIIP) generally provide such whole-of-

government frameworks. This session will bring together policy experts in charge of these frameworks. It will discuss challenges they face to develop and implement them such as how to incentivise operators of essential services, which degree of regulatory requirement is appropriate, how to encourage information sharing within and across sectors, how to address cross-border and cross-sector interdependencies, etc.

Format: after a brief introduction by each panellist, the moderator will invite discussions among them and with the workshop participants.

Moderator: Peter Burnett, Meridian co-ordinator (confirmed)
Panellists:

- Jean-Baptiste Demaison, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), France (invited)
- Bob Gordon, Canadian Cyber Threat Exchange (CCTX) (confirmed)
- Gus Hosein, Privacy International (invited)
- Government or business speaker (tbd)
- Business representative (tbd)

15:00 - 16:30	Concluding session: identifying key policy messages and closing remarks	90 minutes

Moderators from each session will discuss the key findings from their session and possible high-level policy messages from the workshop.

Format: after a brief summary of key discussions in each section by the rapporteur (10 min), moderators of Session 1 to 5 will be invited to discuss together and with the workshop participants, including representatives of stakeholder groups.

Moderator: (tbd)
Panellists:

- moderators of Session 1 to 5.

Close of Workshop 16:30