arpel REGIONAL ASSOCIATION OF OIL, GAS AND BIOFUELS SECTOR COMPANIES IN LATIN AMERICA AND THE CARIBBEAN

Organization of American States | More rights for more people

Ministerio de Modernización Presidencia de la Nación

Ministry of Foreign Affairs and Worship Argentine Republic

Cybersecurity, a key aspect in a hyperconnected world

ARPEL Seminar

December 2016

ARPEL PUBLICATION N° EV03-2016

EVENTS REPORTS

// Contents

Introduction

The event “Cybersecurity in critical infrastructures in a technologically dependent and interconnected world” took place October 18-19, 2016, in the Palacio San Martin (photo) in Buenos Aires.
Organized by **ARPEL** (through its Working Group on Cybersecurity), the **Organization of**
(OAS) and the **Ministries of Modernization and**
Foreign Affairs and Worship of the Argentine Republic, the
This event brought together nearly 200 professionals from the Information Technologies (IT) and Technologies of the Operation (OT)During these two days, experts and high-level government authorities analyzed the challenges posed by cybersecurity for the integrity of infrastructures, as well as the most recent technologies, methodologies, management systems and case studies.
The main conclusions of this event are summarized in this report with the purpose of helping companies and governments to be better prepared in the face of emerging and increasing threats raised by cybersecurity.

01 //
New Cybersecurity Risks and Threats

Hyperconnection, the new context

The rapid development and dissemination of information technologies, mainly in the past 20 years, have delineated a completely different world from what we knew a generation ago.
It is now possible to disseminate and validate news to the whole planet in seconds without the need of teletypewriters, faxes, international calls, through operators, or intermediaries. This process of enhancement of communication is not only irreversible but also desirable, as it has a democratizing, equalizing role, providing freedom of access to information and improving the quality of life. As stated by José Hirchson, representative of the Ministry of the Modernization of Argentina, the challenge for States is how to ensure security while increasing network access in order to create equality.
On the other hand, the new opportunities offered at the level of communication have substantially changed the productive activity and marketing channels, generating new business, but also undoing other, in a typical process of innovation and creative destruction. This has allowed increasing the productivity of industrial companies, for example, through real time monitoring of work processes or remote control of units, but has, in turn, given rise to a series of new risks to

”

"In the past 40 years, cyberspace has brought a new era with new challenges - sales, social networks, virtually infinite communication"

José Hirschson
Ministry of Modernization

infrastructures. In brief, today everything is connected, and everything that is connected is controllable remotely.
It is in this context of hyperconnection where operational areas can no longer manage operational information as watertight compartments within the organization and where new risks of penetration in the operational networks through corporate networks materialize.

"We must work together, this challenge cannot be overcome individually"

"The challenge is to improve security knowing that access must continue to increase in order to create equality"

José Hirschson
Ministry of Modernization

New Threats

According to data from the U.S. Department of Homeland Security, 245 cyberattacks on critical infrastructures were reported in 2015. That number is much higher when the attack is not linked to critical infrastructures.
The above-mentioned issue regarding hyperconnection and the storage of critical information in the cloud, a platform of services via a network, usually the Internet, go along with another issue that will tend to grow exponentially in the coming years and will increase vulnerability: the Internet of Things (IoT), i.e. the internetworking of devices of everyday life to achieve their remote control. The issue was addressed by **Erik de Pablo**, Spanish consultant, and also by **Paul Vaquero, Yeffry el Jammal** and **Federico Tandeter**, specialists from Accenture.
The industrial Internet of Things (IIoT) is seen as a trend with an immense potential since it establishes a bridge between the different levels of

"If cybersecurity poses threats, the Internet of things makes things much worse"

Erik de Pablo
Director of Investigation - ISACA Madrid

information of companies throughout the organization and the value chain, allowing the monitoring of indicators in real time, but it is in this flow of information that a number of new risks emerge. The remote control of lights, cameras, doors, cars, industrial facilities and even pacemakers are examples of this.

On the other hand, **Jeimy Cano**, Coordinator of Information Security and Privacy of Ecopetrol, and researcher on this subject, made a characterization of cyberattacks and their environment, highlighting the increase of the exposure or contact surface, not only because of what relates to the Internet of Things, but also to other areas that increase vulnerability, such as cloud computing, mobile computing, social networks, big data and, finally, cognitive computing, i.e., artificial intelligence. He also added that data are “the oil of 21st century,” on which a new industrial and digital era is based within what today is called the Digital Economy.

> ““…what we need is to generate a new adaptive capacity, that is the new frontier in cybersecurity”
>
> **Jeimy Cano**
> Fellow and Professor - GECTI - School of Law - University of Los Andes

Greater connectivity, greater digital reliance, more dispersed, mobile and less prepared users, and the easy access to technology and knowledge by cybercriminals shape the scenario of increasing vulnerability of personnel and facilities security. The attached table shows some examples of cyberattacks.

2010

Iran - Nuclear – Around 1,000 centrifuges enriching uranium were destroyed through a computer worm.

2015

Ukraine - Electrical grid – 30 substations were disabled, around 230,000 people were left without electricity during a period of one to six hours. The hackers entered the operating system during months to understand its operation, and executed an attack through several vectors, which succeeded in shutting down the substations, changing the display of control operators and blocking all contingencies foreseen.

2016

United Kingdom - Water Purification – A water purification plant for human consumption was attacked from the corporate network and chemical parameters of the water modified by using the remote control of valves. In turn, personal information of 2,5 million customers became exposed. Fortunately, there were no consequences for the health of the community.

Bangladesh - Bank – A cyberattack through the SWIFT system of international transfers attempted to divert US$ 951 million.

Autonomous car – An autonomous car is hacked through a device costing US$ 70, which managed to generate false obstacles in the laser displays and make inadequate car maneuvers.

Pacemakers – It was also demonstrated that the pace of pacemakers can be altered using the remote control through a cyberattack.

An additional vulnerability that is added to this new scenario, which was also highlighted by Jeimy Cano, is the question of the cyberinsurance. Lloyd's stated that the cost of insuring, for example, the U.S. electrical grid would be 80 quintillion dollars.

https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout

New criminal logic

Cybercrime not only changes the profile of offenders, but also the profile of the offense. This means that, today, funds can be diverted from a bank or the operations of an industrial center may be affected from the comfort of an armchair, something that would have been impossible at another time. Another key aspect of the modus operandi of attacks on critical infrastructures is that the motive is not necessarily to affect the company, but the community. It is also for this reason that the approach to the defense of infrastructures should be carried out with a comprehensive vision that goes beyond the limits of the company and whose purpose is preserving the common good.
The difficulty of detection, malice, the cooperation among cybercriminals and the constant technology development are also new cybercrime challenges.

"Are we under attack? Yes, we see this permanently (…) governments and critical infrastructures are targets"

Óscar Morotti
Coordinator of Operations of the National Directorate of Critical Information Infrastructures and Cybersecurity, Ministry of Modernization of the Republic of Argentina

02 //
OT vs. IT, a necessary bridge between two worlds not so interconnected

Paradoxically, one of the highlights presented by the speakers was the need for a stronger connection as regards integrated management of IT and OT.
As explained above, there is a connection between these two worlds, i.e. between the industrial and corporate networks, at the level of computer systems. The new needs of companies lead to this trend, but in turn create new vulnerabilities.
Mr. **Julio Ardita**, Director of CYBSEC, presented a clear example. During the investigation of incidents that violated the industrial network, it was detected that in many cases the intrusion occurred through the corporate network. One of the main vulnerabilities currently existing in the effective protection against cyberattacks is precisely the lack of coordination between the IT and OT areas.
In all cases, it was agreed that a more integrated management was required,

"Good security is good business, not a cost."

Julio Ardita
Director of CYBSEC

"Until the limits of each model (IT/OT) are known, it will be difficult to develop convergences together."

Maximilian Kon
Director of Wiseplant

but also that these two "worlds" have their particular and differentiating characteristics, which poses a challenge to harmonization.
On this point, **Maximilian Kon** from Wiseplant, in his lecture " What is true, successes and failures when speaking about IT/OT?" was particularly clear in his description of these two "worlds" in terms of policies implemented, risks to be considered, priorities and mitigation, detection and protection actions. The conclusions are summarized in the following table:

IT	OT
Users dispersed, information concentrated in databases and greater standardization	Users concentrated (e.g.. SCADA), information dispersed, taken from field by different sensors from the lowest layers, lesser protocol standardization of protocols, times, etc.
Working on information security, and trying that it does not fall into the wrong hands. The most protected value is confidentiality	Works on the security of physical assets, is the integrity of the facilities, and the life and health of workers and the community what is at stake. The most important value is to ensure availability and physical safety .
Short life cycle of technology	The life cycle of technology is longer (in some equipment, 15-20 years)
Faster response to threats, more feasible to perform patches	Slower response to threats due to patching difficulties arising from the operations themselves

In turn, it was also mentioned that, due to the characteristics of these two “worlds”, a successful attack to an industrial infrastructure is more complex because it is necessary to know other technologies and protocols, more robust security measures must be violated and knowledge about the operation of control and monitoring systems is required, so a considerably longer time is needed.

As stated by **Santiago Paz**, from Agesic, when someone performs an attack to an infrastructure, it is likely that this person has already entered the network and violated security some time ago and that the contingencies have also been violated. A good example of this is the attack to the electrical grid of Ukraine, where the attackers entered the system during several months in order to learn how to operate it and understand its contingencies as well. The example given on the electrical grid in Ukraine is very instructive in this regard.

Building bridges between the IT and OT areas is a necessity, but at the same time it is a great challenge not to leave aside the institutional and cultural issues of each of these worlds, with their priorities and different characteristics.

03 //
Response to incidents

Cybersecurity risks evolve constantly and will only tend to grow as network connections continue to grow and integrate increasingly, thus increasing the scope of the attacks. The new criminal logic poses different requirements to respond to an emergency.
As rightly stated by **Marcos G. Salt**, Director of the National Cybercrime Program of the Ministry of Justice and Human Rights of the Republic of Argentina, a common front to face cybercrime should be created by all stakeholders. This call for collaboration and public-private cooperation against cybercrime is a message repeated in the different sessions throughout the event. Cooperation is therefore a fundamental aspect in the response to incidents, and organizations such as **ARPEL** and **OAS** are already working on this matter, since they have the capability to gather different stakeholders and promote such cooperation at the regional level. Among the most important stakeholders to develop this common front against cybercrime mentioned by Marcos G. Salt is the National Center of Response to Cybersecurity Incidents (CERT), the Executive Branch through its ministries, the Judiciary, the national defense institutions, the private sector, public enterprises and the academia. Their cooperation, with each one in their particular role and with a strong leadership from the State, is the best possible way to neutralize the hazards.

"In the end, it is the instability and uncertainty produced (by a cyberattack) which eventually affects the organizations (…), so eventually, cybersecurity seeks to ensure organizational resilience"

Jeimy Cano
Fellow and Professor - GECTI - School of Law - University of Los Andes

"Cybersecurity) must be part of a coordinated State policy to establish a common front against cybercrime"

Marcos G. Salt
Director of the National Cybercrime Program of the Ministry of Justice and Human Rights of the Republic of Argentina

The role of the CERTs

Santiago Paz, Director of Information Security in AGESIC , and founder of the National Center of Response to Cybersecurity Incidents of Uruguay, made an eloquent presentation on the role of Computer Emergency Response Teams (CERT), which reflected the need for cooperation, pragmatism, agility and flexibility to cope with information security threats and incidents. He also mentioned some good practices, such as the systematic and consistent use of audits to implement the opportunities for improvement identified.
He highlighted that the leitmotiv of a CERT is to coordinate and carry out activities of prevention and response to incidents, and he emphasized that an "agile" response management model should be applied. The CERT should be a facilitator capable of leading the response to an emergency through the training of agile teams of professionals from different disciplines, agencies and fields, with self-management capacity.
A CERT should not cover all fields of knowledge, simply because it would not be the most efficient or cost-effective, but there must be ways for the CERT to easily access knowledge through preset arrangements with different stakeholders, thus being able to activate an effective response.

"The key role of the CERT is to be the leader at the national level, the articulator that puts the right person in the right place to address a response"

Santiago Paz
Director of Information Security - AGESIC Uruguay

The proper functioning of these teams requires a well defined and organized "ecosystem-type response" where each stakeholder is able to fulfill its role. The Police Department, the Ministry of Defense, the Ministry of Industry, the University, the private sector, IT service providers and state-owned companies are some of the main stakeholders in this ecosystem in Uruguay.

Cybersecurity is a non-traditional, emerging threat, so to be successful in its prevention, the response must also go beyond traditional security management.

The need for regulation and the role of the Judiciary

During the second day of the event, a panel was held on “The need for a regulatory framework for industrial cybersecurity”, with the participation of **Raúl Palenque**, consultant to the Ministry of Foreign Affairs and Worship and **Marcelo Temperini**, a lawyer specializing in IT law.
There was a discussion about some desirable characteristics for these regulatory frameworks to be efficient to deal with cybersecurity issues in a scenario of greater vulnerability arising from the incorporation of technology in the production system and everyday life.

It was determined that it is necessary to work on the establishment of a regulatory framework for the protection of critical infrastructures, so as to lay the foundations for State leadership in this public-private cooperation required to address this issue, although the regulation by itself will not be sufficient.
Marcelo Temperini gave a presentation entitled “Law as a tool”, and was very emphatic in the fact that regulations must be pragmatic and efficient. After reviewing the situation and the progress made in Argentina in this regard, he stated that in order to

> “Beyond the regulatory frameworks, the first trench in the fight for security is technology”
>
> **Raúl Palenque**
> consultant to the Ministry of Foreign Affairs and Worship

achieve useful regulations, we should follow the good examples at the global level, such as the case of Spain, which was presented by Manuel Sicilia, Head of Cybersecurity Service Analysis Section - CNPIC, during the first day of the event. He also emphasized the need for the public sector to act as strong leader in the implementation, accompanying the private sector but defining clear roles and obligations, and punishing breaches, because a matter such as this should not be left to the goodwill of dispersed stakeholders, which is probably very difficult to achieve, and where there is no real awareness of the risks posed by cybersecurity for companies or individuals.

He and other speakers also highlighted the fact that regulations should not delve into the definition of new offenses that add redundancies and absorb resources. While in some cases this would be strictly necessary, the reality is that the existing codes already provide for several situations arising from cyberattacks. That is to say, in many cases what changes is not the type of offense, the triggering act, but the means used to commit it. A hacker who diverts funds from a bank through the Internet or who accesses the control of an industrial plant is perfectly punishable according to the laws in force, no matter the means used. It is clear that the issue of attribution is one of the additional challenges of cybercrime.

During the two days of the event, the presenters were also emphatic about the fact that it is necessary to work hard on training the Judiciary, something on which some countries are already progressing. From this perspective, the judges must be properly trained so that they can understand and properly interpret the criminal actions perpetrated through the network, this being another point of necessary cooperation between the public and the private sector.

Finally, it was also stated that although proper regulations are necessary, they are not enough to deal with this issue, as the challenge is too large and constantly evolving. Ultimately, it will be the capacity of the stakeholders to act in a coordinated fashion to face the threats which will protect the infrastructures from cybercrime, and regulation is only a fundamental aspect of this process.

Response to incidents

“I’m not saying that everything has to be all right overnight (...) Be selective, try to identify the risks, to prioritize which the requirements will be and start, start to do it (...) grow, define, begin to create procedures, educate, and begin to implement them. This is the way forward.”

“Know that you can, know that it is gradual and have the ability to tolerate frustration. This is my best advice”

Gabriel Faifman
Director of Strategic Programs of Wurldtech

Gabriel Faifman, Director of Strategic Programs of Wurldtech, a subsidiary of GENERAL ELECTRIC, gave a lecture presenting the benefits of the 62443 standard to implement cybersecurity in an industrial company and highlighted a number of recommendations for moving forward on this subject.

The 62443 standard is composed of 13 documents or good practice guidelines for the full implementation of cybersecurity. It is an umbrella which establishes the requirements and the functional areas to protect. He mentioned that, in spite of the existence of the standard, 66 % of the international companies surveyed in the report “2015 Global Megatrends in Cybersecurity” of Raytheon and Ponemon would not be prepared to manage a cyberattack. He noted that vulnerability is not a particular issue affecting Argentina or Latin America, but it is at the international level. He also stressed the opportunity this represents for Argentina, since at the time of updating their production systems, cybersecurity criteria could be included, which is possible today due to the current state of the art, with the potential to become a leader on this subject.

Among his main messages to address the preparation to cyberattacks, he highlighted the fact that the standards are based on maturity models, for which reason he insisted on the need to implement them gradually, but that we must move steadily in this direction. Performing risk analysis, prioritizing, designing procedures and training is the way to move forward in the implementation of cybersecurity, and these are things that can be done today. Finally, he was emphatic about the need to involve technology suppliers and be demanding to obtain best solutions and services.

How prepared are we?

During the panel on "The state of cybersecurity in Latin America", **Claudio Caracciolo** and **Nora Azúa**, coordinators of the Industrial Cybersecurity Center (CCI), presented the preliminary results of a study conducted recently in Argentina by this organization. This study is based on a survey of 18 companies of different sectors; its results are interesting while challenging in terms of preparedness against cyberattacks. Some important results are detailed below:

"We have always been one step behind and will always be so (..) The hackers have the advantage (...) It is a myth that the energy sector is and will be the most attacked. The most attacked sector will be the easiest to attack, the one with less protection to compromise equipment"

Claudio Caracciolo
Coordinator of the Industrial Cybersecurity Center (CCI)

"We see that companies are responding in a reactive manner"

Pablo Vaquero
Safety Manager, Accenture

- In 42 % of cases, the division responsible for cybersecurity was the IT area.
- An acceptable degree of training in IT areas was determined, while it was low in some other areas, such as human resources, quality, purchasing, security.
- Forty-one percent of the companies have not made any formal cybersecurity risk analysis.
- While cybersecurity requirements are usually present in new projects, in general they are very basic and in some cases they are delegated to the supplier.
- In more than 50 % of cases there is no incident management process, or its management was done in a reactive manner.
- The study also shows that many times the private sector is unaware of the initiatives taken by the public sector.

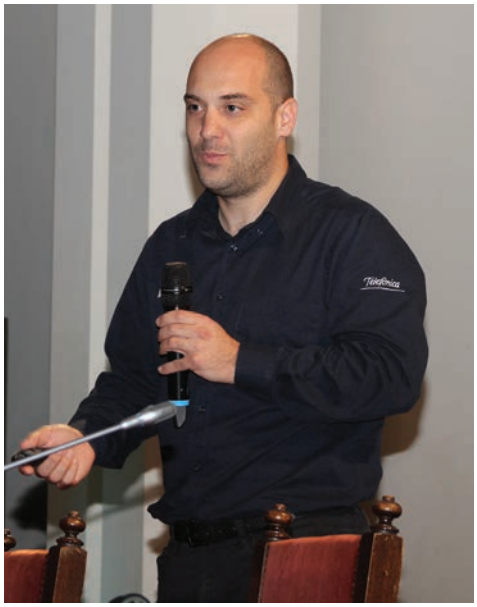
While the study cannot be considered statistically significant, it provides some interesting trends that would be worth examining in depth. It is pertinent to assume that there are gaps in terms of awareness and knowledge of threats, training, risk analysis and management of incidents.

Claudio Caracciolo, in his second presentation, entitled “Control and monitoring or simply lack of control?” stated that it is the most vulnerable enterprises and infrastructure that will be attacked and affected, and not a sector in particular. According to the study of the U.S. Department of Homeland Security for 2015, the energy sector had 16 % of the reported attacks, a great challenge for the industry as a whole.

Being open, cooperative and sharing information on the incidents were some of the highlighted points of the seminar, as one of the good practices that accelerate the learning curve and improve the preparation before incidents. In the United States, this has been the key point of the regulation and articulation of public-private cooperation in cybersecurity, an example that should be undoubtedly followed in our region.

Julio Ardita, Director of CYBERSEC, during the round table “Cases of cyberattacks to critical infrastructure” presented an analysis of different actual cases that were studied in Latin America, and used a hypothetical case to draw some general conclusions on the status of the response to emergencies in our region.

Some of the main gaps found in the investigations of incidents in the region are that there are few records



“If the recommended best practices are followed, the likelihood of attack is very low”

Julio Ardita
Director of CYBERSEC

(logs or blogs) of what happened, the ignorance of the subject by the engineers responsible for the operation and the little connection between the IT areas, the information security areas and the operational areas of the companies (OT vs. IT). Closing his address, he stated that the attacks are not only external but can also come from within the organization, and in these cases addressing them is much more complex. While cybersecurity poses challenges and a somewhat different logic if compared to traditional security, there are also good practices and international standards which, if effectively implemented, minimize the vulnerability to cyberattacks. Raising awareness, training, providing the appropriate software, sharing information and acting cooperatively were the main messages emerging from the workshop to improve protection against cyberattacks. Moreover, **Jeimy Cano** expressed the importance of thinking about the risks on the basis of scenarios built between several members and areas of the organization, in order to expand the perception of what is possible and act accordingly. In the same line, **Erik de Pablo** raised the need to think about cybersecurity risks in a non-linear way, unlike the way in which we think about HSE risks; because this would lead to underestimate costs, as there are other attack vectors, as malice, or the new logic of cybercrime. Thinking differently to face a different threat is a need to increase the levels of preparedness and, finally, the resilience of the organization.

> ""…we have to approach the business to explain the reality of what can happen, because they are different decision-makers."

Daniel Molina
Director General for Strategic Markets of Latin America, Karspersky Lab

04 //
Key Messages

As a conclusion, following are the key messages that were raised during the two days of work.

1

Cybersecurity is an emerging and growing threat, as it is correlated to the increase in connectivity to the network, which will tend to increase because of the possibilities it offers to improve productivity and the quality of life of the people.

2

- Cybersecurity is a latent, permanent and real threat from which nobody can escape, and that can bring consequences of the highest impact for infrastructures, companies and the community.

3

Cybersecurity changes the logic of security, and to be successful it should be addressed from an agile and pragmatic perspective, with comprehensive cooperation between public and private stakeholders. A common front against cybercrime must be created with the leadership of the State. Regulation is a necessary tool, but it is not enough.

4

Raising awareness, training, applying the appropriate computer tools, sharing information and being cooperative and open inside that front is a common need for effective prevention and response.

5

Although there are gaps and there is a lot of work to be done in each of the countries in the region, there are standards, knowledge, best practices and tools available that allow minimizing the possibility of a cyberattack. This is a manageable threat, where the key to be prepared lies in being able to make a correct implementation of these standards and good practices.

Click the titles or read the QR codes with your mobile device to access videos of the dissertations.

Download the application according to the operating system of your device.

ANDROID

iOS
APPLE

Opening Ceremony

José Hirschson | Deputy Secretary of Technology and Cybersecurity - Ministry of Modernization
Francisco Laines | Advisor of Multidimensional Secretary – OAS General Secretariat
Jorge Ciacciarelli | Executive Secretary - ARPEL

The importance of national CERTs

Santiago Paz | Director of Information Security - AGESIC Uruguay
Moderador: Mariana Galán | Legal Advisor of the Deputy Secretary of Technology and Cybersecurity - Ministry of Modernization

Panel: The cybersecurity situation in Latin America

Nora Alzua | Coordinadora - CCI en Argentina
Claudio Caracciolo | Coordinator- CCI Argentina
Moderador: Juan J. Dell'Aqua | Executive Director - USUARIA

Panel: IEC Standard 62443

Gabriel Faifman | Director of Strategic Programs - Wurldtech
Andre Ristaino | Managing Director - ISASecure
Moderador: Gerardo González | Industrial Cybersecurity and IC - YPF

Critical infrastructures

Erik De Pablo | Director of Investigation - ISACA Madrid

The protection of critical infrastructures: the case of Spain

Manuel Sicilia San José | Head of Cybersecurity Service Analysis Section - CNPIC

IT/OT convergence - What is true, successes and failures when speaking of IT/OT?

Maximillian G. Kon | Managing Director, WisePlant HQ

Panel: Prospects for cyberspace protection: Initiatives of the Argentine State

Leandro de la Colina | Deputy Secretary of Cyberdefense - Ministry of Defense
Marcos G. Salt | Director, National Program on Computer-Related Crime - Ministry of Justice and Human Rights
Jorge A. Teodoro | Director of Technology - Ministry of Security
Moderator: Eduardo Martino | National Director - Critical Infrastructures and Cybersecurity - Ministry of Modernization

Using Cyber Resiliency in the Always-on Enterprise

John Duronio | Senior Security Architect - INTEL

The risks of the new smart operation technologies: Industrial Internet of Things

Pablo Vaquero | Security Manager - Accenture
Yeffry El Jammal | Consulting Senior Manager - Accenture
Federico Tandeter |Security Senior Manager - Accenture
Moderator: Oscar Morotti | Technical Director of Information and Cybersecurity Critical Infrastructures - Ministry of Modernization

Control and monitoring, or just lack of control?

Claudio Caracciolo | Chief Security Ambassador - Eleven Paths

Round Table: Cases of cyber-attacks to critical infrastructure

Julio Ardita | Director - CYBSEC
Daniel Molina | General Director for Latin America Strategic Markets - Karspersky Lab
Moderator: Patricia Prandini - Ministry of Modernization

Panel: The need of a regulatory framework for industrial cybersecurity

Raúl Palenque | Consultant - Ministry of Foreign Affairs and Worship
Marcelo Temperini | Lawyer Specialized on Computer Law - AsegurarTe Consulting Firm
Moderator: Oscar Morotti | Operations Coordinator, Information and Cybersecurity Critical Infrastructures Division - Ministry of Modernization

Panel: The importance of protecting critical infrastructures and national defense

Aristides Sebastião Lopes Carneiro | Advisor - Cyber Command Brazil
Daniel Henao | Cyber Command Colombia
Oscar Mato | Representant - Cyber Command Argentina
Ricardo Uquillas Soto | Cyber Command Ecuador
Moderator: Leandro de la Colina | Deputy Secretary of Cyberdefense - Ministry of Defense

Panel: Justice against attacks to infrastructures

Horacio Azzolin | General Prosecutor - National Attorney General's Office
Daniela Dupuy | Prosecutor - National Attorney General's Office
Moderator: Mónica Abalo Laforgia | Legal Advisor - Ministry of Modernization

Development and analysis of cybersecurity scenarios

Jeimy Cano | Fellow and Professor - GECTI - School of Law - University of Los Andes

Panel: Security in critical infrastructures

Juan Camilo Reyes | Regional Leader of Safety Services - IBM
Walter E. Riveros | Director de Offensive Security - Deloitte
Pablo M. Almada | Manager IT Advisory - KPMG
Hernando Castiglioni | Manager System Engineering - Fortinet
Moderator: Gonzalo García-Belenguer | Project Officer - OEA

Industrial Cyber Security

Francisco Souto | Business Development Manager for Cyber Security - Honeywell

Closing remarks and reflection: Building a culture of cybersecurity for the protection of critical infrastructures

Eduardo Martino | National Director - Critical Infrastructures and Cybersecurity - Ministry of Modernization
Francisco Laines | Advisor of Multidimensional Secretary – OAS General Secretariat
Brian O´Durnin | Security Information Manager - YPF
Hernán Vázquez | IT Manager - ARPEL

General Event Clip

EVENTS REPORTS

Cybersecurity, a key aspect in a hyperconnected world

REGIONAL ASSOCIATION OF
OIL, GAS AND BIOFUELS SECTOR COMPANIES
IN LATIN AMERICA AND THE CARIBBEAN

ARPEL is a non-profit association gathering oil, gas and biofuels sector companies and institutions in Latin America and the Caribbean. Founded in 1965 as a vehicle of cooperation and reciprocal assistance among sector companies, its main purpose is to actively contribute to industry integration and competitive growth, and to sustainable energy development in the region. Its membership currently represents over 90% of the upstream and downstream activities in the region and includes national, international and independent operating companies, providers of technology, goods and services for the value chain, and national and international sector institutions.

This report was sponsored by

Regional Headquarters:
Javier de Viana 1018. CP 11200, Montevideo, Uruguay
Ph.: +(598) 2410 6993 | info@arpel.org.uy

www.arpel.org