The State of Cybersecurity in Mexico: An Overview

By Luisa Parraguez Kobek

January 2017

Disclaimer: Any opinions, findings, conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect those of the Wilson Center's Mexico Institute. *This paper was finalized by the author in January 2017. Special thanks to Francisco Garcia Gonzalez, Abil Razo, Mario Abrego, Georgina Campero, Alberto Ugarte, Daniela Peña, Diorella Islas, and Adrian Trulin.*

The State of Cybersecurity in Mexico: An Overview

"Cyberspace is increasingly an essential part of daily life in the Americas and is indispensable to its full development."

- Luis Almagro, Secretary General of the OAS

1. The Regional Cybersecurity Context

The cost of cybercrime incidents in the world has gone from US$3 trillion in early 2015 to a projected US$6 trillion by 2021.[1] As the world becomes more interconnected by the use of faster and larger digital networks, the Organization of American States (OAS) is looking to enhance hemispheric policies that protect governments and civil society against illicit cyber activities. The Secretariat of Multidimensional Security – specifically through the organization's Inter-American American Committee against Terrorism (CICTE) – works to coordinate the efforts of member nations and strengthen regional cooperation in security. Luis Almagro, the Secretary General of the OAS, acknowledged that information and communication technologies (ICTs) and its multiple uses continue to evolve at a rapid pace in the region and countries are highly vulnerable to potentially devastating cyberattacks.

According to the OAS and the Inter-American Development Bank's 2016 Cybersecurity Report, four out of five countries in the region do not have cybersecurity strategies or plans to protect critical infrastructure, and two out of three of them do not have a command and control center or the capacity to prosecute cybercrimes. Furthermore, cybercrime costs the world US$575 million dollars per year, which represents 0.5% of the world GDP and in Latin America it tolls up to US$90 million per year.[2]

Cybersecurity, sustainability and resilience are not only necessary for Mexico's safekeeping but they are also important factors in its social and economic development. When 10% of the population in developing countries is connected to the Internet, the country's GDP grows by 1% to 2%, and even doubling mobile broadband data use can lead to a 0.5% increase in GDP.[3] Lowering or eliminating taxes on mobile telephones even by 1% can increase

[1] Cybersecurity Ventures. (2016). *Hackerpocalypse: A Cybercrime Revelation.* Retrieved on December 1, 2016 from: https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report/

[2] Organization of American States & Interamerican Development Bank. (2016). *Cybersecurity: Are we Ready in Latin America and the Caribbean?* Retrieved on December 1, 2016 from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

[3] Hathaway, M. & Spidalieri, F. (2016). Sustainable and Secure Development: A Framework for Resilient Connected Societies. Organization of American States & Inter-American Development Bank. *Cybersecurity Are we ready in Latin America and the Caribbean?* Retrieved on December 1, 2016 from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

broadband penetration of 1.8% resulting in an economic growth increase of 0.7%.[4] In addition, Mexico´s Internet use went from 5%, or around 5 million users in 2000, to 41%, or 50 million users in 2014.[5] Moreover, there are 77.7 million people who use mobile telephones, and two out of three have a smartphone.[6] Some reports say there are as many as 12 million mobile phone subscriptions.[7] There is indeed an enormous area of opportunity for Mexico to ride the Internet wave towards a more stable and sustainable social and economic development.

2. Internet Users in Mexico

According to Mexico's Census Bureau, INEGI, there are 62.4 million Internet users which account for a total of 57.4% of the population.[8] Likewise, 73.6% of those who use the Internet in Mexico are between the ages of 6 to 34 years old. Yet the study reveals that those who use the Internet with more frequency are between 25 and 34 years old and are located in the central zone of the country, making up 26% of the national total. With regards to homes with Internet access, 44.44% have access and 55.56% do not. Not surprisingly, Mexico City has the highest Internet connectivity in the country with 63.1%, which is 24% above the national average. Other states with a high percentage are Nuevo Leon, Baja California Sur, Sonora, Baja California and Quintana Roo, where around half of the population has Internet access. On the other hand, states such Oaxaca and Chiapas have the lowest connectivity ratios that reflect in only one out of seven family households.[9]

In March 2016, the Mexican Internet Association published its 12th annual report on Internet habits in Mexico.[10] The Association places Internet penetration at 59.8% which is equivalent to 65 million Internet users. According to the report, Mexicans spend an average of 7 hours and 14 minutes a day on Internet activities, that is 1 hour and 3 minutes more than in 2015,

---

[4] Darrell West. (February 13, 2015). *Digital Divide: Improving Internet Access in the Developing World through Affordable Services and Diverse Content*. Brookings Institution Report. Retrieved on December 5, 2016 from: https://www.brookings.edu/wp-content/uploads/2016/06/West_Internet-Access.pdf

[5] PwC Mexico. (2015). *Cybersecurity in Mexico*. Retrieved on December 11, 2016 from: https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf

[6] Mexican Census (INEGI). (May 2016). *Estadísticas a propósito del día mudial de Internet* [International Internet Day Statistics]. Retrieved on December 11, 2016 from: http://www.inegi.org.mx/saladeprensa/aproposito/2016/internet2016_0.pdf

[7] Organization of American States & Interamerican Development Bank. (2016). *Cybersecurity: Are we Ready in Latin America and the Caribbean?* Retrieved on December 1, 2016 from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

[8] Mexican Census (INEGI). (May 2016). *Estadísticas a propósito del día mudial de Internet*. [International Internet Day Statistics]. Retrieved on December 11, 2016 from: http://www.inegi.org.mx/saladeprensa/aproposito/2016/internet2016_0.pdf

[9] Mexican Census (INEGI). (May 2016). *Estadísticas a propósito del día mudial de Internet*. [International Internet Day Statistics]. Retrieved on December 11, 2016 from: http://www.inegi.org.mx/saladeprensa/aproposito/2016/internet2016_0.pdf

[10] Mexican Internet Association (AMIPCI). (2016). *12° Estudio sobre los Hábitos de los Usuarios de Internet en México 2016* [12th Study on the Habits of Internet Users in Mexico 2016]. Retrieved on December 11, 2016 from: https://amipci.org.mx/images/Estudio_HabitosdelUsuario_2016.pdf

and 79% of that time is used to access social media. The most popular sites are: Facebook at 92%, although it has experienced a 6 point drop in one year; WhatsApp at 79%, which is Mexico´s most used social media site with Mexicans spending up to 5 hours and 15 minutes a day; YouTube at 66%; Twitter at 55%; Instagram at 39%, and a 5 point rise from the previous year. Most users are hooked up to five different social media sites. Households remain the most common place for connection with 87% of people logging-in, and the main device to access the network is a Smartphone with a 77% usage, up 19 points from 2015.

The Internet has changed the daily habits of Mexicans, for example in leisure activities such as listening to music, watching movies, managing finance and accessing social networks. The main reason they currently connect for the first time on the Internet is to access social media networks, which is also the most important leisure activity. The leading barriers that block access to the Internet are a slow connection (47%), high costs (31%), those who do not know how to use it (26%), and technical problems from the Internet service provider (24%).[11]

With regards to the levels of education and Internet use in Mexico, 94.5% of those with University education used the Internet on a regular basis as part of their activities, 83% of those with High School education and 46.1% of those with Elementary schooling.[12] INEGI also points out in its most recent census that 55.2% of homes without Internet access mentioned a lack of resources as the reason not to obtain the service.

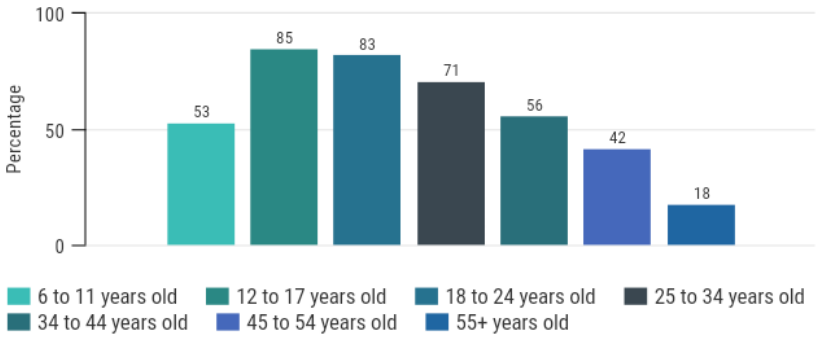
[11] Mexican Internet Association (AMIPCI). (2016). *12° Estudio sobre los Hábitos de los Usuarios de Internet en México 2016* [12th Study on the Habits of Internet Users in Mexico 2016]. Retrieved on December 11, 2016 from: https://amipci.org.mx/images/Estudio_HabitosdelUsuario_2016.pdf

[12] Mexican Census (INEGI). (May 2016). *Estadísticas a propósito del día mudial de Internet*. [International Internet Day Statistics]. Retrieved on December 11, 2016 from: http://www.inegi.org.mx/saladeprensa/aproposito/2016/internet2016_0.pdf

INTERNET USAGE IN MEXICO

Internet users in Mexico

Per age group



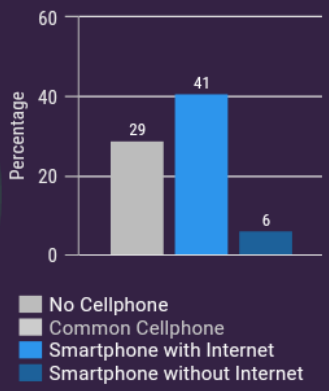
Households with a computer

Yes 44.44%

No 55.56%

62.4 million Internet Users in Mexico

Cellphone users



(INEGI 2016)

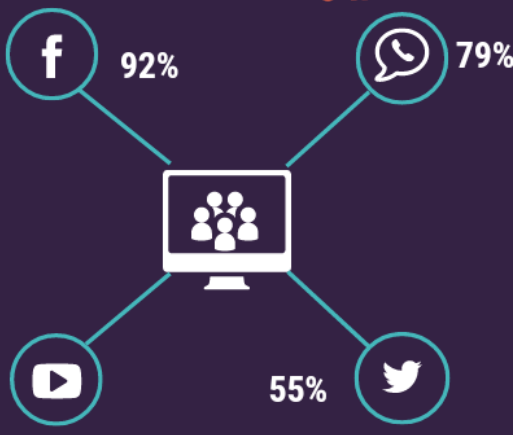
SOCIAL MEDIA IN MEXICO

Average time spent daily on Internet per user

7h 14 min

Internet users access on smartphone

77%



(AMIPCI 2016)

3. Foreign Direct Investment and Cyberattacks

Mexico's economy and geostrategic location is an attractive target for illicit cyber activities. On the one hand, it is enjoying considerable Foreign Direct Investment (FDI) and a solid GDP growth and on the other, it is still relatively vulnerable in cybersecurity and cyber defense. Mexico´s total FDI showed an 11% increase from 2014 to 2015 which is equivalent to a total of 28 billion dollars in 2015.[13] According to the World Bank (2015), Mexico also presents a solid GDP growth with a 2.5% increase from 2014 to 2015, which is higher than the 2.4% the United States reached in 2015.[14] Among the 20 countries with the highest cumulative threat score – in which Mexico ranks as number 10 – its GDP correlated with the severity of cyberattacks.[15]

Mexico ranks as the second country in Latin America with the most cyberattacks, with a 40% growth in the number of attacks between 2013 and 2014, and approximately 10 million victims in 2014.[16] Given that 57.4% of Mexico's estimated 127 million population are Internet users, bridging the gaps in its cybersecurity environment is an important task with implications for a large and growing portion of its population. The government, the private sector, and civil society must be able to keep up with the constant innovation in the information technology (IT) sector, both as users and as possible targets for attacks. Mexico ranks second after Brazil among countries that send spam to the network; these two countries plus Colombia wire 75% of spams in the Latin American continent.[17]

The International Telecommunications Union identifies 17 National Computer Security Incident Response Teams (CSIRT) in Latin America and ranks Mexico's preparedness for cyber threats at 18 out of 29 spots.[18] Mexico is a member of the Forum of Incident Response and Security Teams (FIRST) and the Mexican Government's interaction with the international community for cybersecurity is mostly represented by Mexico's Computer Emergency Response Team (CERT-MX) created in 2010. It groups experts from the government, commercial, and academic sectors in order to prepare Mexico to respond to cyberattacks and is involved in protecting critical infrastructure. The Federal Police (*Policía Federal*) is responsible for investigating cybercrimes at the national level.

---

[13] Kate Cornman. (April 4, 2016). *Infographic: Foreign Direct Investment in Mexico*. Mexico Center, Woodrow Wilson Center. Retrieved on December 15, 2016 from: https://www.wilsoncenter.org/article/infographic-foreign-direct-investment-mexico

[14] World Bank. (2015). *GDP growth (annual %).* Retrieved on December 15, 2016 from: http://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?year_high_desc=true

[15] Control Risks. (2015). *Cyber Threats to the Mexican Financial Sector*. Retrieved on December 15, 2016 from: https://www.controlrisks.com/en/services/security-risk/cyber-threats-to-the-mexican-financial-sector

[16] PwC Mexico. (2015). *Cybersecurity in Mexico*. Retrieved on December 15, 2016 from: https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf

[17] CISCO Systems Inc. (2016). *Spam Overview.* Retrieved on December 15, 2016 from: https://www.senderbase.org/static/spam/#tab=4

[18] International Telecommmunications Union. (April 2015). *Global Cybersecurity Index & Cyberwellness Profiles*. Retrieved on December 15, 2016 from: http://www.itu.int/pub/D-STR-SECU-2015

CYBERSECURITY IN MEXICO

An Overview:

Population: 127 million
(World Bank 2015)

GDP: US $1.144 trillion
(World Bank 2015)

62.4 million
Internet users in Mexico
(INEGI 2016)

2nd Largest Economy in Latin America
GDP per capita: US $9,009
(World Bank 2015)

18/29
Global Cybersecurity Index (ITU 2016)

2nd country in Latin America with the most cyberattacks
(Control Risks 2015)

2nd
Spam sender in Latin America (CISCO 2016)

Main vulnerabilities:

Wrong system configurations

Outdated versions

404
Application problems
(OAS 2015)

4. Mexico´s Cybersecurity Environment

According to the 2015 Global Security Index & Cyberwellness Profiles Report of the International Telecommunications Union (ITU), Mexico does not have a national governance roadmap for security in cyberspace.[19] Its main vulnerabilities are a lack of a cyber security culture, a wrong system configuration, outdated versions to be replaced by new and compatible technology, and application problems.[20] Incidents in cyberspace pose a challenge to Mexico due to a lack of institutional structures and there is a need to strengthen capabilities since it does not have any specialized government or public sector agencies certified under internationally recognized standards.[21] The Cybersecurity 2016 OAS Report emphasizes that "improvement of national capabilities is important to boost confidence in private and public digital services, which paves the way for an emerging digital economy and reliable e-governance".[22]

The Council of Europe's Convention on Cyber-crime, also known as the Budapest Convention of November 2001, is the first multilateral treaty on crimes committed through the Internet that seeks "a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation."[23] The Convention divides cyber-crime into four dimensions: 1. Offenses against the confidentiality, integrity and availability of computer data and systems (hacking, phishing, espionage, interception, interference); 2. Content-related offenses (child pornography, hate speech, gambling, libel, scam); 3. Computer-related offenses (fraud, forgery, identity-theft, laundering); and 4. Copyright and trademark-related offenses (file sharing).

Mexico was invited in January 2007 to adhere to the Convention and it has expressed its willingness to do so but has not signed due to national legislative considerations, regulation issues and because it is difficult to carry out and comply with all of the provisions. In 2014, Mexico hosted a workshop on "Cybercrime Legislation in Latin America" that brought together countries in the region, the Organization of American States, the U.S. Department of Justice, the European Council, the Mexican Executive, Legislative and Judicial

---

[19] International Telecommunications Union. (2016). *Global Cybersecurity Agenda*. Retrieved on December 15, 2016 from: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

[20] Organization of American States & Trend Micro. (April 2015). *Report on Cybersecurity and Critical Infrastructure in the Americas*. Retrieved on December 15, 2016 from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf

[21] International Telecommmunications Union. (April 2015). *Global Cybersecurity Index & Cyberwellness Profiles*. Retrieved on December 15, 2016 from: http://www.itu.int/pub/D-STR-SECU-2015

[22] Organization of American States & Interamerican Development Bank. (2016). *Cybersecurity: Are we Ready in Latin America and the Caribbean?* Retrieved on December 15, 2016 from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

[23] Council of Europe. (November 23, 2001). *Convention on Cybercrime. European Treaty Series 185*. Budapest, Hungary. Retrieved on December 15, 2016 from: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

representatives, the private sector, civil society and academia.[24] The Government of Mexico has not enacted specific legislation on cybersecurity, but it is included in the Federal Criminal Code, mostly regarding financial crimes, information security, and the use of technology in other crimes, such as terrorism, kidnapping, and drug trafficking.

Mexico has a Specialized Information Security Committee, which was tasked to create a National Strategy for cybersecurity. However, this has not yet happened, and the Federal Police currently handles issues on a case-by-case basis through its Cyber Police and Scientific Division. The ITU Report states that "personnel at the Scientific Division have received and continue to participate in specialized training from the Police Development System of Mexico (SIDEPOL), as well as from numerous other security and law enforcement organizations in countries including Colombia, the US, Holland and Japan."[25] Although Mexico has approved privacy and data protection legislation, it cannot keep up with the level of activity thus making it difficult to prosecute these acts. The Federal Police has dealt with 123,368 cybersecurity cases dealing with viruses and ITC vulnerabilities and has taken down 10,745 sites during the current administration.[26] In addition, Mexico passed a telecommunications law in 2014 that stipulates different data retention provisions; this information can be accessed by public authorities without a court order and can be stored for up to 24 months.[27]

The cybersecurity dilemma[28] is also important to consider: on the one hand, national security concerns are placed in the forefront of policymaking with a clear defense and intelligence dimension; on the other hand, the government must likewise strike a balance in protecting privacy rights, freedom of expression and association of its citizens. To meet the first objective, the Government of Mexico launched the 2014-2018 National Security Program with new strategies to defend its national interest against organized crime, radical and dissident groups. As for the second one, the National Institute of Transparency, Access to

---

[24] This 341 page document contains the presentations made by each of the participants. Memoria del "Taller Sobre Legislación en Materia de Ciberdelincuencia en América Latina" [Documents from the Workshop on Cybercrime Legislation in Latin America]. Government of Mexico & the Council of Europe. (2014). Retrieved on December 15, 2016 from: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/Memoria%20Taller%20Ciberdelito.pdf

[25] International Telecommunications Union. (2016). *Global Cybersecurity Agenda*. Retrieved on December 15, 2016 from: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

[26] Mexican Federal Police, Press. (May 26, 2016). *Policía Científica Federal participa en 2do Congreso Latinoamericano de Ciberseguridad* [Federal Scientific Police Participates in the 2nd Latin American Congress on Cybersecurity]. Retrieved on December 15, 2016 from: https://www.gob.mx/policiafederal/prensa/policia-cientifica-federal-participa-en-2-congreso-latinoamericano-de-ciberseguridad

[27] Ley de Telecomunicaciones y Radiodifusión, 2014. Fundaçao Getúlio Vargas. (2016). Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean. *Cybersecurity: Are we Ready in Latin America and the Caribbean?* Organization of American States & Interamerican Development Bank. Retrieved on December 15, 2016 from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

[28] Myriam Dunn Cavelty. (April 30, 2014). Breaking the Cybersecurity Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Springer*. Retrieved on December 15, 2016 from: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Breaking_the_Cyber-Security_Dilemma_2014.pdf

Information and Protection of Personal Data protects personal information of Mexican citizens. Although Mexico's digital infrastructure has reached around half of the population, the vulnerabilities are prevalent and President Enrique Peña Nieto's administration has been required to adapt towards the era of smart grids, telecommunications and online finance.

In 2010, the Government of Mexico created CERT-MX[29] which is responsible for protecting critical infrastructure (CI), managing cyber incident response, investigating electronic crimes, analyzing evidence, and responding to digital threats that would affect the integrity of critical networks.[30] Disregarding Mexico's structural reform on energy in 2014 and its impact on the development of a more efficient critical infrastructure, significant cyberattacks have not taken place in this sector. Mexico's academic sector experienced more attacks than any other with 39% out to the total incidents, and cyber threats in Mexico had also affected civil population due to the sprout of phishing activities by 409% in 2013.[31]

5. Cybersecurity and National Security Strategy

At the end of 2012, President Enrique Peña Nieto presented the 2013-2018 Plan for Development establishing the cornerstone for the National Security Program 2014-2018, which focuses on Mexico´s strategic interests and national objectives.[32] Likewise, it created the Specialized Information Security Committee, tasked with the drafting the National Strategy for Information Security. The Program is founded on the idea of multidimensional security[33] that encompasses traditional threats and new ones, and is an important element in the preservation of peace and stability in the country and the region. The Program focuses on specific policy for cybersecurity to protect and promote national interests and the main undertakings outlined within are to: promote actions to prevent and combat cyber-attacks; strengthen mechanisms for preventing incidents in the Federal executive sites; uphold compliance and development of procedures to evaluate and strengthen the performance of the response teams to incidents of cyber security in the Federal executive branch; improve human capital skills and technological infrastructure to address cyber security incidents; establish international cooperation on cyber security and cyber defense in particular with

[29] CERT-MX stands for *Centro Especializado en Respuesta Tecnológica de México*.

[30] Organization of American States & Trend Micro. (2014). *Latin American and Caribbean Cybersecurity Trends and Government Responses*. Retrieved on December 19, 2016 from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

[31] Organization of American States & Interamerican Development Bank. (2016). *Cybersecurity: Are we Ready in Latin America and the Caribbean*? Retrieved on December 19, 2016 from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf

[32] Gobierno de México. (2014). *Programa para la Seguridad Nacional 2014-2018: Una política multidimensional para México en el siglo XXI.* Retrieved on December 19, 2016 from: http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf

[33] The Multidimensional model mentioned by the Government of Mexico refers to a broader concept of justice and social inclusion, the fight against poverty, quality education, the prevention and attention to illnesses, the protection of the environment, economic, social and political development and securing information and communication technologies (ICTs).

North American countries to prevent and address attacks on the computer systems of the country.

Although Mexico may not pose a high risk for terrorism, it is still required to take preventive measures to identify its vulnerabilities and safeguard itself from external threats and risks. The Government of Mexico established a series of measures and actions in the National Security Program 2014-2018 to help identify potential attacks against national security. In addition, Mexican experts maintain a close and constant collaboration with more than 300 teams from 69 countries to prevent and combat these crimes.[34] Mexico is also a member of the Forum of Incident Response and Security Teams (FIRST), a grouping of 369 teams in 78 countries, and it participates in four teams.[35]

Information security in the network has become increasingly important with the rising threat in cyberspace. The Federal Government has focused on strengthening cybersecurity and promoting relevant legislation in order to guarantee its National Security and lower the level of violence. It recognizes the global challenges that entail technological, energy, demographic and environmental issues, and outlines the vulnerabilities of the State.

[34] PwC Mexico. (2015). *Cybersecurity in Mexico*. Retrieved on December 19, 2016 from: https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf
[35] The four teams are: CERT-MX, Mnemo-CERT, Scitum-CSIR and UNAM-CERT. FIRST. (2016). https://www.first.org/members/map#mexico

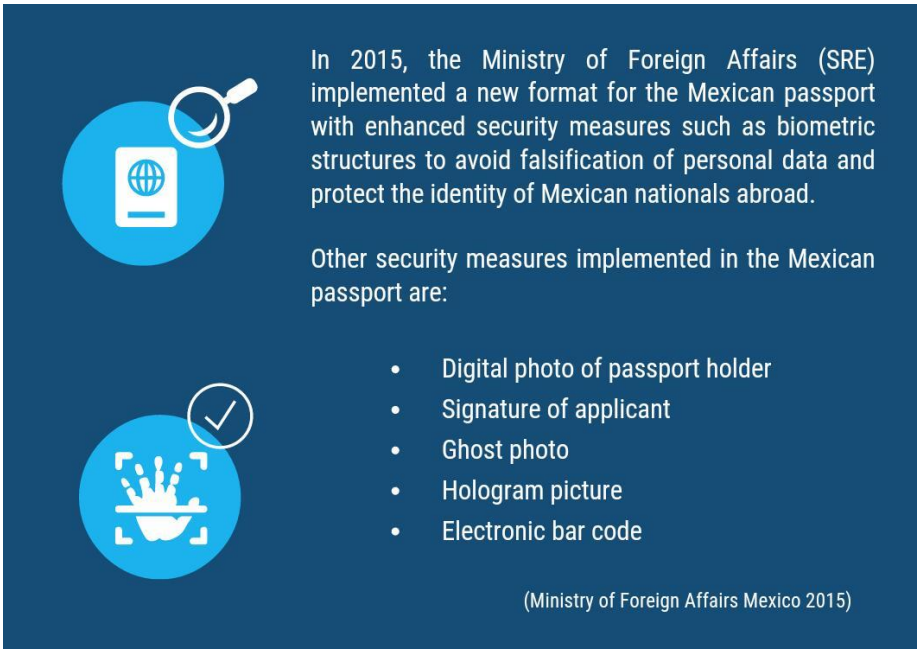

National Security Strategy
2014-2018
Exchange information with regional partners through agreements made by both diplomatic and institutional means
Develop State policy in the field of cybersecurity and cyber defense to ensure the economic, political and military interests in cyberspace
Develop processes for the protection of Critical Infrastructure to prevent it from being infringed
Train specialized personnel in the cybersecurity and defense fields
Incorporate mechanisms and specialized information exchange according to bilateral cooperation agreements on technology and cybersecurity intelligence material
Increase training in military and naval personnel in cybersecurity and cyber defense
(Government of Mexico 2014)

6. Document Security Measures

The protection of personal data has gained attention from governments and private companies alike. The right to privacy and the protection of personal information for both individuals and corporations is an extremely relevant issue for international organizations and the public sector. If cybersecurity laws are not created and strengthened, Mexico may become a vulnerable target to the threats of criminal agents. The Inter-American Committee against Terrorism (CICTE) of the Organization of American States established a Document Security and Fraud Prevention Program (DSFP) to enhance security in the issuance and control of travel and identity documents.[36]

In Mexico, the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI)[37], is the body that guarantees, protects and regulates the information rights of all individuals and corporations through the Federal Law on Protection of Personal Data, which entered into force on July 6th, 2010. In order to preserve national security, the Government of Mexico has tried to protect the privacy and integrity of not only its citizens, but also its public institutions.

Although the Federal Government has implemented new measures to prevent identity theft through the protection of personal data, there is still a long way to go regarding these laws. Some areas of opportunity will require the government to cooperate with private institutions, as well as international organizations to make laws more effective and reduce the risks of new criminal agents in cyberspace.



[36] Inter-American Committee against Terrorism. (2016). *Document Security and Fraud Prevention*. Retrieved on December 19, 2016 from: http://www.oas.org/en/sms/cicte/programs_fraud.asp

[37] INAI. (2016). Retrieved on December 19, 2016 from: http://inicio.inai.org.mx/SitePages/English_Section.aspx

7. Critical infrastructure

Cybercrimes entangle a variety of threats for the State's economic and political development. Due to the digitalization and systematization of critical infrastructure, the Government of Mexico is vulnerable to cyberattacks. Private companies and institutions are enabling a new relationship between the government and the private sector in order to carry out technological development that boosts better cybersecurity protocols and regulations.

Mexico has around 3,000 strategic installations, 47% of them belong to the Mexican Petroleum State-owned company (PEMEX), 17% of them to the National Water Commission (CONAGUA), 13% to the Federal Commission of Electricity (CFE), as well as 16 major ports, 40 smaller ports, and 56 international airports.[38] Since 2013, there has been an increase in the number of attacks corresponding to the critical infrastructure network. Due to the extension and development of the smart grid, the energy sector has been more affected by cyberattacks. A special report from US-CERT (United States Computer Emergency Readiness Team) estimates that 32% of the attacks were directed at energy companies. As critical infrastructure plays a strategic role in national security, most OAS members have encouraged new protocols in order to protect their key industries. Data displayed on Brazil, Argentina and Mexico shows that a vast majority of the vulnerabilities are related to "wrong configurations" within the software platform as well as the use of old versions.[39]

Mexico remains the second largest investor in IT management. Nonetheless, based on Micro Trend analysis, the Government of Mexico is not well prepared to counterbalance cyber-attacks, which points to its vulnerabilities and areas of opportunities due to the rise of attacks between 2013 and 2014. Oil and gas revenues, managed through PEMEX, provide about one-third of all the Mexican government's revenue.[40] The Latin American private sector still shows a lack of information regarding the dangers of cyberattacks to critical infrastructure. According to Mexico´s Energy Regulating Commission only 21% of companies are leading protocols in the resistance against hackers, bad ware and other cyberattacks.

[38] Government of Mexico. (2014). *Programa para la Seguridad Nacional 2014-2018: Una política multidimensional para México en el siglo XXI.* Retrieved on December 21, 2016 from: http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf

[39] Organization of American States & Symantec. (June 2014). *Latin American + Caribbean Cyber Security Trends*. Retrieved on December 21, 2016 from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

[40] Cohen, B. (2015). *Geopolitics: The Geography of International Relations*. Retrieved on December 21, 2016 from: goo.gl/6R0bzS

8. Industry and Cybersecurity

Mexico is the 15th largest economy in the world, the second largest economy in Latin America after Brazil, it has one of the highest GDP per capita in the region (around US$9,009 per capita), it is the 12th largest exporter of goods and 4th largest producer of petroleum and other liquids in the Americas after the United States, Canada and Brazil.[41] Mexico is a young country with half of its population under the age of 26 years old thus providing an active work force.[42] The World Bank classifies Mexico as an "upper middle income" nation, and it is a member of the Organization of Economic Cooperation and Development (OECD).

Mexico´s rising economy and the increase in connectivity are among the main factors that draw cybercriminals to engage in illicit activities for profit. Mexico ranks as the second country in Latin America after Brazil with the largest number of cyberattacks. Many companies do not report the attacks for fear of damaging their reputations, while some are unaware of the infringement. According to PwC Mexico, "91% of Mexican companies have prioritized cybersecurity in their organizations and Mexico is the country with the most investment in cybersecurity in Latin America."[43] The financial sector has led the way in this area, followed by telecommunications, both of which are also Mexico's most globalized economic sectors.

Nonetheless, their actions are severely limited by the lack of specific legislation. According to the Security Industry Association over half a billion dollars is spent per year on security firms. The Latin American cybersecurity market is expected to grow from US$5.29 billion in 2014 to US$11.91 billion in 2019, at a compound annual growth rate (CAGR) of 17.6% for the period.[44] Companies like Symantec, Trend Micro and various other security firms have found a fertile market to promote their products in order to combat the rising threats that cyberattacks pose to fledging communications infrastructure. This is an intermediary link between government and the private sector collaborating to safeguard individual information.

The Mexican financial sector has reported less sophisticated cyberattacks using Distributed Denial of Service (DDoS), which refers to targeting a single system with multiple compromised systems to result in a denial of service, and Trojans, malicious computer programs used in hacking activities. Control Risks declares that Mexican organized crime

---

[41] World Bank. (2015). *Gross domestic product 2015*. Retrieved on December 21, 2016, from: http://databank.worldbank.org/data/download/GDP.pdf /; World Bank (2015). *DDO per capita (current US$).* Retrieved on December 21, 2016 from: http://data.worldbank.org/indicator/NY.GDP.PCAP.CD?year_high_desc=true / Energy Information Administration (2014). *Mexico Overview*. Retrieved on December 21, 2016 from: https://www.eia.gov/beta/international/analysis.cfm?iso=MEX

[42] Government of Mexico. (2014). *Programa para la Seguridad Nacional 2014-2018: Una política multidimensional para México en el siglo XXI.* Retrieved on December 21, 2016 from: http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf

[43] PwC Mexico. (2015). *Cybersecurity in Mexico*. Retrieved on December 21, 2016 from: https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf

[44] Cybersecurity Ventures. (2015). *Cybersecurity Market Report 2015*. Retrieved on December 21, 2016 from: http://cybersecurityventures.com/cybersecurity-market-report-q3-2015/

targeted individual actors rather than big corporations. In fact, the main cyber threats reported in 2014 by financial companies were malware and spams that were used as a method of extortion and data falsification.[45]

9. Organized Criminal Activity in Mexico and Cybercrime

According to the World Economic Forum´s 2017 Global Risk Report, massive incident of data fraud/theft is considered to be the 5th most likely global risk.[46] The exponential increase of movement in cyberspace has led to a correlated escalation in criminal activity in Mexico in particular with regards to illegal hacking, identity theft, credit card fraud, and online exploitation of minors. The organized criminal groups in Mexico, have used digital media in their favor to control, manipulate and disseminate information, while some threaten with violence those who publish unfavorable information on their organizations. They not only silence those who "snitch" on social media, but they seek to dominate this space by targeting those who use it against them. This creates a vacuum that they then occupy to establish their own power, consolidate their legitimacy while down-playing the role of their competitors with negative propaganda.

The U.S. Drug Enforcement Administration (DEA) identified the following drug trafficking organizations (DTOs) as dominant in Mexico: Sinaloa, Los Zetas, Tijuana/AFO, Juarez/CFO, Beltran Leyva, Gulf, and La Familia Michoacana and many analysts suggest that these 7 seem to have now fragmented to 9 or as many as 20 major organizations.[47] These groups are run like companies, with extensive production and distribution networks, intelligence apparatus and security systems, and they use social media to communicate and the Internet to post their activities. They are involved in all types of criminal activity, including: identity theft, fraud, extortion, kidnappings, and trafficking of humans, organs and firearms.

Along with Facebook and Twitter, there are websites that report activity carried out by the different organized criminal organizations. There is a rise in "cybervigilante" groups that use the Internet to denounce drug cartel activities which at times are also created by their rivals. In 2011, an online activist collective, Anonymous, took security issues in its own hands and had a virtual show-down in the port city of Veracruz with Los Zetas cartel. The *#opcartel* or Cartel Operation was established to denounce criminal activity, government corruption, kidnappings and rape in passenger bus commutes on highways. When one of Anonymous' hacktivists was allegedly kidnapped by the cartel in retaliation for the online activities, it demanded his release and threatened to reveal the identities of over 70 of the cartel´s members and colluded politicians, business people, military personnel, journalists and taxi drivers. The cartel, in turn, hired "narcohackers" to locate the vigilante members and

[45] Control Risks. (2015). *Cyber Threats to the Mexican Financial Sector*. Retrieved on December 21, 2016 from: https://www.controlrisks.com/en/services/security-risk/cyber-threats-to-the-mexican-financial-sector

[46] World Economic Forum. (2017). *The Global Risks Report 2017, 12th Edition*. Retrieved on January 15, 2017 from: http://www3.weforum.org/docs/GRR17_Report_web.pdf

[47] June S. Biettel. (July 22, 2015). *Organized Crime and Drug Trafficking Organizations. Congressional Research Service*. Retrieved on January 15, 2017 from: https://fas.org/sgp/crs/row/R41576.pdf

announced they would murder them.[48] Anonymous backed down and the kidnapped member is said to have been released.[49] Taking into consideration the enormous amount of resources managed by the criminal organized groups in Mexico, there is little doubt that they have recruited security experts and "black hatters" to establish their own digital counterintelligence units.

In 2013, Mexico held the number one position in the world for pornographic material involving minors and second place for its Internet production.[50] There were 1,330 websites, 116,000 web searches a day, and at least 80,000 children who were exploited.[51] Mexican criminal organizations have also been linked to the prostitution of minors. An estimated 800,000 adults and 20,000 children are trafficked for sexual exploitation, where some of the children become part of Mexico´s lucrative US$30 million a year pornography industry.[52] Two trends are currently prevalent in online child sexual exploitation: home produced material, and livestream activity in real time.[53] Predators are also using peer-to-peer (P2P) networks to avoid downloading material from sites, thus making it more difficult to trace them. Like most things cyber, legislation has not been able to keep up to the activities.

[48] Scott Stewart. (Nov. 2, 2011). *Anonymous vs. Zetas Amid Mexico´s Cartel Violence*. Stratfor. Retrieved on January 15, 2017 from: https://www.stratfor.com/weekly/20111102-anonymous-vs-zetas-amid-mexico-cartel-violence

[49] Charles Arthur. (November 2, 2011). "Anonymous Retreats from Mexico Drug Cartel War." *The Guardian*. Retrieved on January 15, 2017 from: https://www.theguardian.com/technology/2011/nov/02/anonymous-zetas-hacking-climbdown; OpCartel. (2011). *Kids, Trust Me…You Are Not Up to This Operation*. Retrieved on January 15, 2017 from: https://krypt3ia.wordpress.com/2011/11/03/opcartel-kids-trust-me-you-are-not-up-to-this-operation/

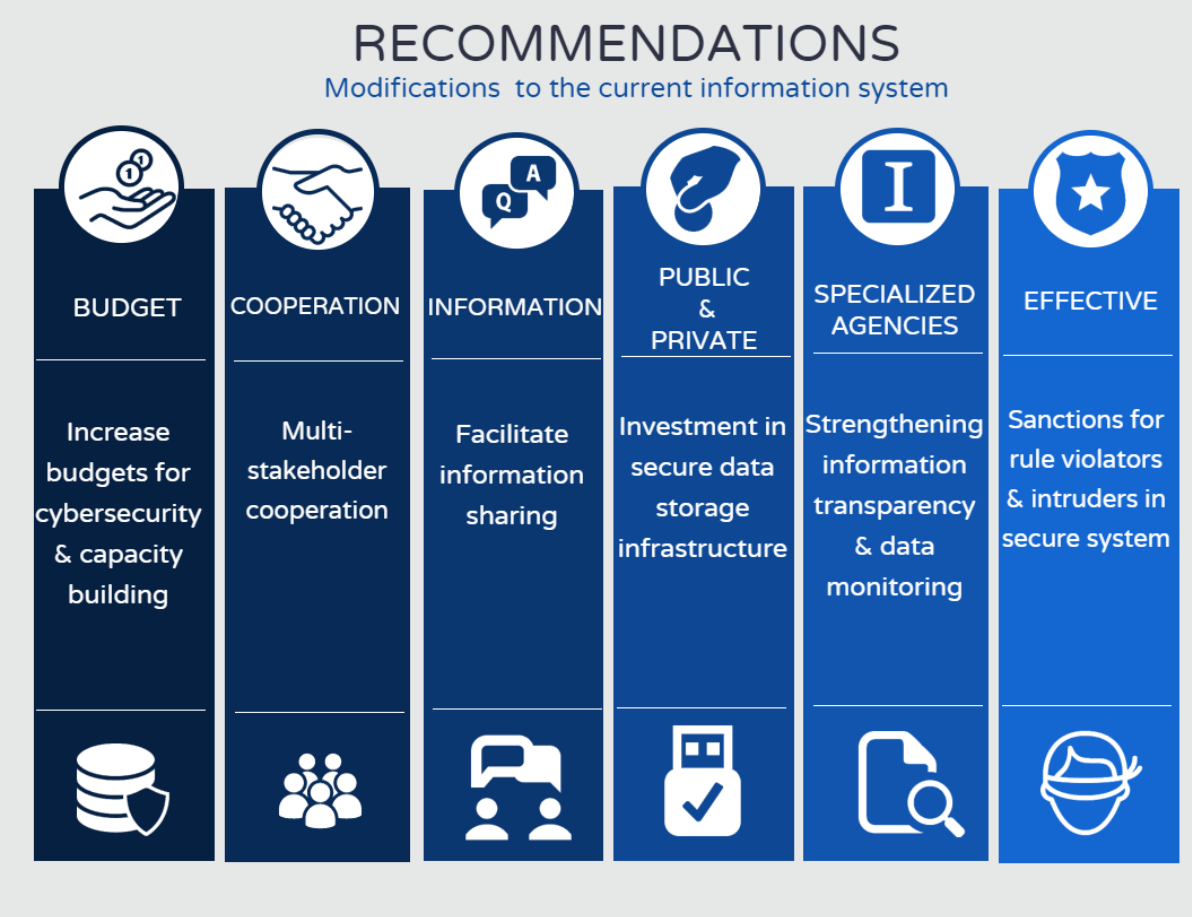
[50] Senate, Government of Mexico. (September 25, 2013). *Foro Combate a la Pornografía de niñas, niños y adolescentes* [Conference on Combating Child and Adolescent Pornography]. Retrieved on January 15, 2017 from: http://www.pan.senado.gob.mx/2013/09/palabras-del-senador-victor-hermosillo-y-celada-al-clausurar-el-foro-combate-a-la-pornografia-de-ninas-ninos-y-adolescentes/#!prettyPhoto[21254]/0/

[51] Marguerite Cawley. (September 27, 2013). *Mexico is World Leader in Child Pornography: Officials.* InSight Crime. Retrieved on January 15, 2017 from: http://www.insightcrime.org/news-briefs/mexico-is-world-leader-in-child-pornography

[52] Marguerite Cawley. (September 27, 2013). *Mexico is World Leader in Child Pornography: Officials*. InSight Crime. Retrieved on January 20, 2017 from: http://www.insightcrime.org/news-briefs/mexico-is-world-leader-in-child-pornography

[53] Global Initiative against Transnational Crime. (April 7, 2014). *Stolen Innocence: The Online Exploitation of Children*. Retrieved on January 20, 207 from: http://globalinitiative.net/stolen-innocence-the-online-exploitation-of-children/

10. Recommendations & Conclusions



Conclusions

> *"If there is a message that needs to be conveyed, it's that a trusted Internet is not achieved by a single treaty or piece of legislation; it is not solved by a single technical fix, nor can it come about because one company, government or individual decides security is important… The promise of the digital economy - one that will bring innovation, growth and social prosperity - will not be met without an open, trusted Internet. The responsibility lies with all of us and it's one we can take on together."*
>
> -*The* Internet Society, Global Internet Report 2016

Cybersecurity strategies are aimed at both protecting society against harmful cyber threats and reinforcing economic and social development based on a sound information and communication technologies (ICTs) environment. The modifications to the current information system in Mexico include public/private investment of secure data storage infrastructure. The progress on information technologies is rapidly increasing.

If Mexico wants to be a pioneer of data rights in the Latin American, it must first replace its aging equipment for newer and faster data processing units that comply not just with national and regional directives, but with international protection of information practices. At the same time, the new infrastructure must effectively adapt to changes in the way information is transmitted around the world. For this solution to take effect, there has to be a source of funding. It would be productive for the Government of Mexico to finance the operation in conjunction with private firms. The benefits of furthering research on the issue of data protection would be mutually beneficial, which makes it a promising research opportunity for joint funding initiatives.

Budgets for cybersecurity and capacity building must be increased, with corresponding accountability mechanisms to keep track of their productivity. Greater investment in human capital and the growth of new technologies are fundamental to Mexico's development. Greater information sharing must be facilitated and multi-stakeholder cooperation is essential to strengthening CERT-MX as public-private partnerships are established in a collective action which also takes into account privacy matters of the population.

The Government of Mexico should also effectively sanction those who intrude in secure systems or propagate personal information. It should enforce laws regarding data, especially concerning legal sanctions for any and all involved in criminal activities that endanger information whether it be personal, public or governmental. Similarly, data should be better monitored, not to violate individual privacy but to maintain order and to demonstrate to citizens that their information is safe. Updating relevant regulations and practices related to data protection would, in the long run, facilitate legal proceedings and bring about swifter resolutions to security issues.

Mexico has established the National Institute of Transparency, Access to Information and Protection of Personal Data to protect information transparency and data monitoring. It keeps the Government accountable for its actions and provides information to any individual that requests a copy of their personal data. The INAI must be given the economic and logistical support to focus on expertise, tools, resources, and most importantly, the necessary training to deal with data intrusions. Having more experts in this particular area can provide citizens with the confidence required to place more of their trust on Government.

As with all things in information technology, digital activities in Mexico are only just beginning. This is only the tip of the iceberg as the internet-of-things becomes more prominent, and Mexico's online population continues its use of Internet-enabled devices. The more online activity there is, the more economic activity that is generated and, in turn, there is a corresponding increase in the level of vulnerabilities. Mexico needs to engage with its national, regional and international partners to combine resources, multi-stakeholder initiatives and facilitate information sharing to ensure its security in cyberspace.

Bibliography

Abebe, D. (2016). Cyberwar, International Politics, and Institutional Design. *The University of Chicago Law Review, 83*(1), 1-22.

Arthur, C. (November 2, 2011). "Anonymous Retreats from Mexico Drug Cartel War". *The Guardian*. Retrieved from: https://www.theguardian.com/technology/2011/nov/02/anonymous-zetas-hacking-climbdown;

Asociacion Mexicana de Internet. (2016). *12° Estudio sobre los Hábitos de los Usuarios de Internet en México 2016* [12th Study on the Habits of Internet Users in Mexico 2016]. Retrieved from: https://amipci.org.mx/images/Estudio_HabitosdelUsuario_2016.pdf

Asociacion Mexicana de Internet. (2012). *Study on Protection of Personal Data among Users and Companies*. Retrieved from: https://www.amipci.org.mx/estudios/proteccion_de_datos_personales/est_proteccion_datos-ingles.pdf

Bradley, N., Alvarez, M., McMillen, D., & Craig, S. (2016). *Reviewing a year of serious data breaches, major attacks and new vulnerabilities: Analysis of cyber attack and incident data from IBM's worldwide security services operations*. Retrieved from: http://www-03.ibm.com/security/data-breach/cyber-security-index.html

Castro, D. (2012). U.S. Federal Cybersecurity Policy. In K. Andreasson (Ed.), *Cybersecurity: Public Sector Threats and Responses*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Cawley, M. (September 27, 2013). Mexico is World Leader in Child Pornography: Officials. InSight Crime. Retrieved from: http://www.insightcrime.org/news-briefs/mexico-is-world-leader-in-child-pornography

Chavez, G. (January 25, 2016). Ciberseguridad, el riesgo del que México no habla. *CNN Expansión*.

CISCO Systems Inc. (2016). *Spam Overview.* Retrieved from: https://www.senderbase.org/static/spam/#tab=4

Cohen, B. (2015). Geopolitics: The Geography of International Relations. Retrieved from: goo.gl/6R0bzS

Comision Nacional de Seguridad. (2015). Comunicado de Prensa No. 700 [Press release].

Consejo de Seguridad Nacional. (2014). *Programa para la Seguridad Nacional 2014-2018*. Mexico City: Presidencia de la República.

Control Risks. (2015). *Cyber Threats to the Mexican Financial Sector*. Retrieved from: https://www.controlrisks.com/en/services/security-risk/cyber-threats-to-the-mexican-financial-sector

Cornman, K. (April 4, 2016). *Infographic: Foreign Direct Investment in Mexico*. Mexico Center, Woodrow Wilson Center. Retrieved from: https://www.wilsoncenter.org/article/infographic-foreign-direct-investment-mexico

Council of Europe. (November 23, 2001). Convention on Cybercrime. European Treaty Series 185. Budapest, Hungary. Retrieved from: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Cybersecurity Ventures. (2016). Hackerpocalypse: A Cybercrime Revelation. Retrieved from: https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report/

Cybersecurity Ventures. (2015). Cybersecurity Market Report 2015. Retrieved from: http://cybersecurityventures.com/cybersecurity-market-report-q3-2015/

Diniz, G., & Muggah, R. (June 2012). A Fine Balance: Mapping cyber (in)security in Latin America. *Strategic Paper 2*.

Donaldson, S., Siegel, S., Williams, C., & Aslam, A. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*. New York: Apress.

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. Retrieved from: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Breaking_the_Cyber-Security_Dilemma_2014.pdf

Energy Information Administration (2014). Mexico Overview. Retrieved from: https://www.eia.gov/beta/international/analysis.cfm?iso=MEX

Espina-García, E. (2012). Centro Nacional de Respuesta a Incidentes Cibernéticos CERT-MX [Press release].
Fischer, E. (2009). *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*. New York: Novinka.
Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict and Security in Cyberspace*. Lausanne: EPFL Press.
Global Initiative against Transnational Crime. (April 7, 2014). Stolen Innocence: The Online Exploitation of Children. Retrieved from: http://globalinitiative.net/stolen-innocence-the-online-exploitation-of-children/
Gourley, S. (2014). Cyber Sovereignty. In P. Yannakogeorgos & A. Lowther (Eds.), *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton, FL: Taylor & Francis.
Government of Mexico. (2014). *Programa para la Seguridad Nacional 2014-2018: Una política multidimensional para México en el siglo XXI.* Retrieved from: http://cdn.presidencia.gob.mx/programa-para-la-seguridad-nacional.pdf
Gutierrez, B. (2015). Criptopunks y América Latina: de la soberanía tecnológica a la era de las filtraciones. *Revista Teknokultura, 12*(3), 549-576.
Hayden, M. (2014). The Future of Things Cyber. In P. Yannakogeorgos & A. Lowther (Eds.), *Conflict and Cooperation in Cyberspace: The Challenge to National Security*. Boca Raton, FL: Taylor & Francis.
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2016). Retrieved from: http://inicio.inai.org.mx/SitePages/English_Section.aspx
Instituto Nacional de Estadística y Geografía (INEGI). (May 2016). *Estadísticas a propósito del día mudial de Internet*. Retrieved from: http://www.inegi.org.mx/saladeprensa/aproposito/2016/internet2016_0.pdf
International Telecommunications Union. (2016). Global Cybersecurity Agenda. Retrieved from: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
International Telecommmunications Union. (2016). Definition of Cybersecurity. Retrieved from: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
International Telecommmunications Union. (April 2015). *Global Cybersecurity Index & Cyberwellness Profiles*. Retrieved from: http://www.itu.int/pub/D-STR-SECU-2015
Internet Society. (2016). *Global Internet Report 2016*. Retrieved from: https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf
ISACA & Cybersecurity Nexus. (January 2015). *2015 Global Cybersecurity Status Report - Latin America Data*.
Jackson, R. (August 2015). Mexico Sets Sights on Cyber Security. *Defence IQ*.
Joseph-Harris, S. (September 2015). Mexico's Cyber Security Problem, Ten Years Later... *Defence IQ*.
Kapellmann, D., & Reyes, B. (2015). Retos de Ciberseguridad para México. Retrieved from: http://the-ciu.net/nwsltr/381_1Distro.html
Martin, P.-E. (July 24, 2015). *Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos*. Retrieved from: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO79-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf
Mexican Federal Police, Press. (May 26, 2016). *Policía Científica Federal participa en 2do Congreso Latinoamericano de Ciberseguridad*. [Federal Scientific Police Participates in the 2nd Latin American Congress on Cybersecurity]. Retrieved from: https://www.gob.mx/policiafederal/prensa/policia-cientifica-federal-participa-en-2-congreso-latinoamericano-de-ciberseguridad
Mexidata.Info. (March 5, 2012). Mexican Drug Lords vs. Cybervigilantes and the Social Media. Retrieved from: http://www.mexidata.info/id3288.html
Ministry of Foreign Affairs, Government of Mexico. Nuevas medidas de seguridad en el pasaporte mexicano tipo "E". Retrieved from: https://embamex2.sre.gob.mx/espana/images/stories/SeccionConsular/pasaportelibretae.pdf

Ministry of Public Education, Government of Mexico. (2009). Comunicado 226.- Lanza la SEP el programa Impúlsate para la enseñanza de idiomas y computación [Press release]. Retrieved from: http://www.sep.gob.mx/wb/sep1/bol2260909 - .V8Oe5pPhCRs

National Institute of Transparency, Access to Information and Protection of Personal Data (INAI). (2016). Misión Visión y Objetivos. Retrieved from: http://inicio.ifai.org.mx/SitePages/misionViosionObjetivos.aspx

Navarro-Isla, J. (June 2011). Cyber regulation in Latin America. *Newsletter eLAC*(15).

Obiso, M., & Fowlie, G. (2012). Toward a Global Approach to Cybersecurity. In K. Andreasson (Ed.), *Cybersecurity: Public Sector Threats and Responses*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

OpCartel. (2011). "Kids, Trust Me…You Are Not Up to This Operation". Retrieved from: https://krypt3ia.wordpress.com/2011/11/03/opcartel-kids-trust-me-you-are-not-up-to-this-operation/

Organization of American States. Inter-American Committee against Terrorism. (2016). *Document Security and Fraud Prevention*. Retrieved from: http://www.oas.org/en/sms/cicte/programs_fraud.asp

Organization of American States, & Inter-American Development Bank. (2016). *Cybersecurity: Are we Ready in Latin America and the Caribbean?* Retrieved from: https://publications.iadb.org/handle/11319/7449?locale-attribute=en&

Organization of American States & Symantec. (June 2014). *Latin American + Caribbean Cyber Security Trends*. Retrieved from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Organization of American States & Trend Micro. (April 2015). *Report on Cybersecurity and Critical Infrastructure in the Americas*. Retrieved from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf

Pemex. (2014). *A Turning Point: Defining the Future of Midstream and Downstram Activities.* Retrieved from: http://www.pemex.com/ri/herramientas/pemexday/PemexDay/4_PEMEX%20Day%20NY_IT_2014.pdf

Portnoy, M., & Goodman, S. (2009). *Global Initiatives to Secure Cyberspace: An Emerging Landscape*. Atlanta: Springer.

Potomac Institute for Policy Studies. (November 2015). *Cyber Readiness Index 2.0. A Plan for Cyber Readiness: A Baseline and an Index.* Retrieved from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CyberReadiness_EN.pdf

PwC Mexico. (2015). *Cybersecurity in Mexico*. Retrieved from: https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf

Robinson, N. (2012). European Cybersecurity Policy. In K. Andreasson (Ed.), *Cybersecurity: Public Sector Threats and Responses*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Saavedra, B. (2015). Cybersecurity in Latin America and the Caribbean: The State of Readiness for the Defense of Cyberspace. *William J. Perry Center for Hemispheric Defense Studies*. Retrieved from: https://www.hsdl.org/?abstract&did=794507

Saavedra, B. (2016). Las infraestructuras críticas en América Latina: conectada, dependiente y vulnerable. *William J. Perry Center for Hemispheric Defense Studies*. Retrieved from: http://chds.dodlive.mil/files/2016/05/Pub-OP-Saavedra.pdf

Senate, Government of Mexico. (September 25, 2013). *Foro Combate a la Pornografía de niñas, niños y adolescentes.* Retrieved from: http://www.pan.senado.gob.mx/2013/09/palabras-del-senador-victor-hermosillo-y-celada-al-clausurar-el-foro-combate-a-la-pornografia-de-ninas-ninos-y-adolescentes/#!prettyPhoto[21254]/0/

Singer, P., Newton, M., Sterio, M., & French, S. (2014). *A Discussion on Cyber Warfare/Interviewer: M. Scharf*. Talking Foreign policy, Case Western Reserve Journal of International Law, Cleveland.

Sonneland, H. (2015). Mexico City 2015 Blog: The State of Cybersecurity. Retrieved from: http://www.as-coa.org/blogs/mexico-city-2015-blog-state-cybersecurity

Stewart, S. (Nov. 2, 2011). *Anonymous vs. Zetas amid Mexico´s Cartel Violence*. Stratfor. Retrieved from: https://www.stratfor.com/weekly/20111102-anonymous-vs-zetas-amid-mexico-cartel-violence

UNAM-CERT. (2016). Estadísticas de incidentes en 2015. Retrieved from: http://www.cert.org.mx/estadisticas.dsc

West, D. (February 13, 2015). *Digital Divide: Improving Internet Access in the Developing World through Affordable Services and Diverse Content*. Brookings Institution Report. Retrieved from: https://www.brookings.edu/wp-content/uploads/2016/06/West_Internet-Access.pdf

Wheeler, D. (2012). Understanding Cyber Threats. In K. Andreasson (Ed.), *Cybersecurity: Public Sector Threats and Responses*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Wilson Center. (2016). Foreign Direct Investment in Mexico. Retrieved from: https://www.wilsoncenter.org/article/infographic-foreign-direct-investment-mexico

World Bank. (2015). Gross Domestic Product 2015. Retrieved from: http://databank.worldbank.org/data/download/GDP.pdf / World Bank (2015). DDO per capita (current US$). Retrieved from: http://data.worldbank.org/indicator/NY.GDP.PCAP.CD?year_high_desc=true

World Bank. (2016). Information & Communication Technologies: Overview. Retrieved from: http://www.worldbank.org/en/topic/ict/overview

World Economic Forum. (2015). *The Global Information Technology Report 2015.* Retrieved from: http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf