Wilson Center
MEXICO INSTITUTE

Quo Vadis?

Mexico's National Cybersecurity Strategy

Luisa Parraguez Kobek

May 2018

Quo vadis?

Mexico's National Cybersecurity Strategy

> *"Cyber security should contribute to keeping the internet a place where democracy can be fully realized, socio-economic development can continue moving ahead, and human rights are respected."*
>
> -Alison August-Treppel, CICTE 2017

Introduction

In order to reach a destination, you have to know where you are going. Having a roadmap traces a path towards reaching a goal and that is the purpose of a national Cybersecurity strategy. Mexican society has become ever more reliant on information and communications technology (ICTs) and on-line government services. The financial sector and the national economy as a whole is increasingly dependent on digital platforms. Being interconnected, however, brings risks and having a national security strategy is fundamental to protecting the country's well-being. Mexico's National Cybersecurity Strategy sets forth a guide towards 2030 and aims to prepare the country for future activities in an increasingly complex digital world.

Cybersecurity affects everyone. No one is exempt from the effects of exponential growth, volume, speed, and sophistication of cyber activity in our linked, hyper-complex, digital world - the Fourth Industrial Revolution, better known as the digital revolution. This disruptive paradigmatic upheaval fuses technologies and stretches the limits of our imagination where augmented reality, virtual reality, and artificial intelligence are dramatically altering the way we work, play, experiment, think, and project.

About half of the entire world population, 3.5 billion people, use the Internet, and there are over 23.5 billion intelligent devices already interconnected which, according to Statista, will grow to 75 billion new devices by 2025. It is also an era of multidimensional threats exposing State weaknesses, in particular in Critical Infrastructure and financial platforms, pushing the need for a collaborated effort among all the stakeholders.

Crime follows money and Mexico's rising economy has made it an attractive target for cyber criminals. According to a 2017 Symantec report, cybercrime in Mexico rose from USD$3 billion in 2014 to USD$7.7 billion in 2017 affecting over 10 million people. Mexico announced its National Cybersecurity Strategy in November 2017. This came as the result of extensive national and international consultations, events, and government agency efforts to identify fragile areas and platform and software vulnerabilities to be able to increase the ability to bounce back from an intrusion and combat cybercriminal activity.

The Strategy aims to place Mexico as a resilient nation in Cyberspace. It is broad reaching and general to stand as a guide to new activity over time. There is a long stretch from strategy to public policy, however, and much has yet to be spelled-out. Launching the

Strategy as the current Enrique Peña Nieto Administration is gearing up for a July 2018 national election is a challenge as the incoming government will have to decide what the next steps will be to put the Strategy into effect. Finally, collaborating with other partners, including the United States, can be mutually beneficial as Mexico can learn from best practices and leapfrog towards a more secure future.

The International Cybersecurity Environment

Cyberpolitics in International Relations is a new concept coined by a group of researchers at the Massachusetts Institute of Technology and Harvard University. Classic notions of sovereignty, areas of interest, control, dominion, stability, and security are pinned against a new international backdrop integrated into cyberspace. Shaped by human ingenuity and used as a space of interaction, cyberspace is also an enabler of political leverage and power. State and non-State actors, formal and informal groups play a pivotal role in international cyberpolitics provoking more questions than answers where the issue of attribution is always a concern.

Estonia is perhaps the first major case of cyberpower aggression of the 21st century. In 2007, it was hit by an orchestrated swarm of internet traffic sent by a network of digital robots called ‘botnets’ to banks, media outlets, and government bodies creating disturbance and instability by swamping servers in a ‘distributed denial-of-service’ (DDoS) attack. This forced several of the country’s government, financial, and health services to shut down in different intervals at a time. Hundreds of thousands of computers around the world had been hijacked, turned into ‘zombies,’ and used to send up to 4 million packets per second in a repeatedly network-clogging mission squeezing the entire country’s bandwidth capacity. Although some argue it was State-sponsored by Russia for political reasons, it has been difficult to attribute to the Kremlin as individual hackers, hacktivists, and criminal digital gangs were involved. Estonia today, however, has one of the world´s most decentralized and open digital environments with one of the fastest broadband capacities in the globe.

In December 2014, Sony suffered a major cybersecurity breach as it was about to release a film that portrayed an unfavorable image of the North Korean leadership. Hackers erased, stole, and released movies, private information, and sensitive documents that seriously damaged the company. The alleged perpetrators are North Koreans working either for the government or in support of its position. Once again, attribution is a difficult matter be it to safeguard your own expertise and technical knowhow or to point a political finger at one or multiple intruders.

In addition, in May 2017, the WannaCry ransomware hit the world’s computers running on Microsoft Windows operating systems by encrypting information held for ransom and that could only be decrypted by paying in electronic currency called ‘bitcoins.’ In total, over 150 countries were affected with over 200,000 victims and 300,000 computers infected in hospitals, schools, factories, banks, and government offices. Then in June

2017, NotPetya ransomware hit businesses around the world, destroying data and IT assets, which Cybereason estimates cost organizations USD$1.2 billion in revenue. The trend will continue as new forms of cyber aggression are developed, and State and non-State actors need to be better able to deal with these new threats.

According to Cybersecurity Ventures, cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades. The cost of cybercrime incidents in the world has gone from USD$3 trillion in early 2015 to a projected USD$6 trillion annually by 2021. "This represents the greatest transfer of economic wealth in history, it risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined," according to the company. In addition, the International Telecommunications Union (ITU) has published that digital attacks increased 30 percent between 2011 and 2012, affecting 550 million people around the globe at an economic cost of USD$110 billion. Even more alarming in its figures of a global rise, the 2018 Norton Symantec reports that 978 million people in 20 countries were affected by cybercrime for a total loss of USD$172 billion.

The Internet of Things (IoT), through nanotechnology and innovation, uses sophisticated sensors, chips, platforms, and applied analytics to share large quantities of data. Likewise, augmented reality, mostly through intelligent mobile devices and visual aids, is increasing people's daily experiences at home, work, the supermarket, subways, and social gatherings as people's physical environment merges with a virtual environment. Big-data analytics is processing zettabytes – that is 10^{21} volume – of digital information in fractions of a second, and the use of e-clouds for massive storage is in growing demand. Research in artificial intelligence (AI), although still a couple of decades away from a world where machines may be able to make rational, independent, and ethical decisions for us, is nonetheless starting to be developed.

Mexico's International Participation

In light of the fact that the digital revolution is expanding at an exponential rate, with unprecedented scope, velocity, and volume, cutting across every major field in today's world, the United Nations held a two-phase World Summit on the Information Society in 2003 and 2005. The aim was to bridge the global digital divide by making the Internet accessible in all countries, particularly in developing nations. Mexico became part of the United Nations Group of Governmental Experts (GEG) on Developments in the Field of Information and Telecommunications in the Context of International Security. Although there was initial progress in the talks, the group was unable to reach a consensus in 2017, primarily on how international law applies to the use of information and communications technologies by States. The multilateral talks have stopped.

In 2005, an international gathering in London, England initiated a process of global governmental bodies to exchange ideas and initiate actions on Critical Information Infrastructure Protection (CIIP) measures called the Meridian Process. In 2015, the Meridian Process merged with the Global Forum on Cyber Expertise (GFCE), made up of countries, international organizations, and private companies that exchange best practices and expertise on cyber capacity building. In 2016, Mexico was the host and Chair of the Meridian Process for the cooperation of global governmental bodies for Critical Information Infrastructure Protection (CIIP). In addition, that same year Mexico hosted the United Nations Internet Governance Forum (IGF) on public policy issues of the Internet and best practices.

Mexico has also worked closely with the Organization of American States (OAS) to organize national awareness and training events. In 2015, Mexico along with the Cyber Security Program of the Inter-American Committee against Terrorism (CICTE) of the Organization implemented a Cybersecurity Maturity Model tool to determine the state of affairs in cybersecurity presented to the Inter-American Development Bank in 2016. It also joined the Working Group on Cooperative and Confidence Building Measures in Cyberspace. It was present at the First Meeting of the Working Group on Cooperation and Confidence-Building Measures in Cyberspace in February 2018 in Washington, DC and continues to participate in the regional efforts to move forward in this area.

Mexico has now joined the group of Latin American countries that have presented cybersecurity strategies: Panama (2013), Trinidad and Tobago (2013), Jamaica (2015), Colombia (2011 & 2016), Paraguay, Chile, and Costa Rica (2017).

Mexico’s Cybersecurity Vision

The Government of Mexico announced its National Cybersecurity Strategy at the Third Annual Cyber Security Week in Mexico City on November 13, 2017. Mexico’s Strategy “recognizes the importance of information and communications technologies (ICTs) in the country’s political, social and economic development.” It outlines that “the risks and threats in Cyberspace can constitute a possible attack on human dignity, the integrity of people, the credibility, reputation and patrimony of companies and public institutions, and affect public security or even national security.”

1. The vision of the Strategy identifies the significance of Information and Communications Technologies (ICTs) as a main factor of political, social, and economic development where the population increasingly uses the Internet and where both public and private organizations use Cyberspace for their activities.

   As the economy grows, the Internet and ICTs drive innovation, and society becomes increasingly reliant on a digital infrastructure. In the cyber domain, a risk management analysis takes into account the dynamic nature of risk, thus contemplating threats, vulnerabilities, usage, probable impact, and where there is an acceptable level of risk. Security measures can act as a double-edged sword, as they are necessary in protecting social and economic activity that relies on Cyberspace, but they can also undermine these very activities. A careful evaluation and selection of appropriate security measures must be in place to protect and foster development in a digital environment.

2. The vision underlies the rising risks in the use of technologies and a growing number of cybercrimes, thus establishing a need for a general culture of cybersecurity in the country. It recognizes that criminal activities and malware development are moving at a faster pace than public policy or regulation. The Organization of American States published in 2014 that the inherent costs of digital crimes in the world was USD$113 billion and that cybercrime cost Mexico between USD$3-5 billion a year. The Inter-American Development Bank then provided a 2016 figure that shot up to USD$575 billion a year in the world, the equivalent of 0.5 percent of global GDP, and USD$90 billion for Latin America and the Caribbean. A national cybersecurity strategy was necessary to guide the efforts of all the stakeholders into future stages of digital penetration in Cyberspace.

3. The vision establishes a need for a general cybersecurity culture. According to the Internet Association of Mexico (AIMX), Internet users have gone from 40 million in 2012 to 65.5 million in 2016. The strategy establishes a series of objectives to protect individuals and businesses as usage rises, and with it the volume, speed, and sophistication of cyberattacks.

Mexico's Cyber Profile

Internet penetration in Mexico

60%

3 out of 4 use smartphone

How many people?

77.7 million mobile phone users

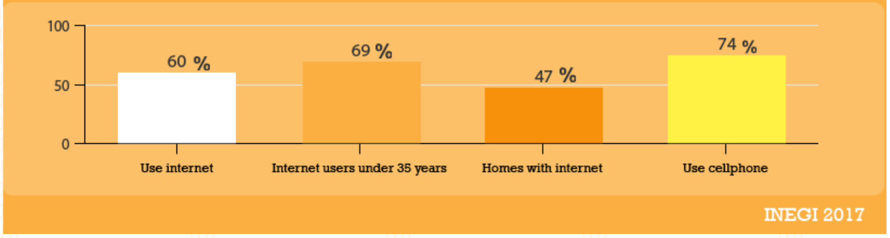
Who are they?

69% Internet users under 35 years of age

What profile?

9 out of 10 Mexicans with higher education (undergraduate and graduate) use the Internet in their daily lives

Internet Users (over 6 years old):



INEGI 2017

Mexico’s Cybersecurity Strategy: Design and Development

As with all nations around the world, keeping up with cybersecurity has been a challenge for Mexico. It has been active in addressing cybersecurity issues and has included them in several documents prior to launching the Strategy. These are:

- The National Development Plan 2013-2018
- The Program for National Security 2014-2018, and
- The Public Security National Program 2014-2018.

In addition, there have been several government initiatives to increase and improve cybersecurity. For example, the task of developing a National Strategy for Information Security fell under a Specialized Information Security Committee. The country’s Computer Incident Response Team (CERT-MX) is a member of the global Forum for Incident Response and Security Teams (FIRST), and it follows a Collaboration Protocol with other governmental agencies and is responsible for Critical National Infrastructure (CNI) protection. Government agencies adhere to the Administrative Manual of General Management of Information, Communications and Cyber Security Technologies (MAAGTICSI) on standards such as ISO 27001, ITIL, and Cobit. The Scientific Division of the Federal Police of Mexico investigates national cybercrimes and is the host institution of CERT-MX.

Stakeholders coordinate infrastructure security management and share information on CNI assets and vulnerabilities. The Mexican National Institute for Transparency Access to Information and the Protection of Personal Data (INAI) promotes personal data protection. It also assists in efforts for greater transparency and availability of information to the public while publishing reports and leading campaigns to raise citizen’s awareness of their rights as users of information and communication technology.

In 2013, the Guardian published information leaked by former National Security Agency (NSA) contractor Edward Snowden that pointed to an alleged NSA breach on the Government of Mexico’s email accounts. Sensitive and confidential information was exposed digitally before it was announced officially, as the hacking of government e-mails affected several government agencies, including the Presidency. Unclear whether this had a direct impact on policy decisions or not, one year later the Government of Mexico marked its Digital Agenda goals for cybersecurity and cyber defense within the Program for National Security 2014-2018. The objective of the Agenda is to “push forward the digitalization of Mexico through e-government, open sources, and the use of ICTs in the provision of health, education and financial services.”

Cyber defense, however, deals primarily with military capabilities and the digital revolution has presented an enormous challenge to traditional means of protecting national security. Cyberpower is dynamic, asymmetrical, multidimensional, disruptive, infinite, and 24/7. Furthermore, it is difficult to attribute to one source as it travels over several points of contact in Cyberspace. Due to the volume, velocity, scale, and variety, cyber conflict should have an active multi-layered approach, assisted by augmented intelligence and with a strong element of resiliency to learn from the intrusion, reconfigure, migrate, and retaliate, when necessary. It is not only a challenge for Mexico but is a challenge for international affairs and conflict in the 21st century overall.

Taking into consideration the role of stakeholders in securing Cyberspace in Mexico, the National Cybersecurity document points to a 2017 report on cybersecurity in Mexico presented by the National Chamber of the Electronics Industry, Telecommunications and Information Technologies (CANIETI) and other private sector associations. The report calls on establishing a National Cybersecurity Agency that would coordinate the strategy and establish a critical route for Internet governance, while generating certainty and trust in the new digital ecosystem. It underlines the importance of redefining a legal framework for cybersecurity that would guarantee the protection of personal data. It also outlines the protection of Critical Infrastructure emphasizing the importance of resilience understood within a risk management perspective to set up the mechanisms and protocols for the re-establishment or migration of the systems.

In October 2017, the Intergovernmental Agency for the Development of E-Government (CIDGE) proposed establishing a Sub-Committee for Cybersecurity under the Ministry of the Interior (Gobernación) through the Scientific Division of the Federal Police. Its task is to approve, disseminate, and coordinate the implementation of the Strategy and improve inter-agency cooperation and promote collaboration among all sectors of society. It will also act as a formal vehicle to the National Security Council.

The Role of the Organization of American States

In April 2017, at the request of the Government of Mexico, the Secretariat of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States through its Cyber Security Program presented a document with recommendations for the development of the National Cybersecurity Strategy. The information presented highlights the importance of inter-agency and multi-stakeholder cooperation.

The general recommendations made in the document are the following:

- Cybersecurity is not an end in itself but rather serves distinct higher-level purposes.
- The strategic framework should clearly state high-level objectives and explain why they are essential to the country (‘vision’).
- Anchor the strategy not just in national policy and law, but also in regional and international commitments and obligations.
- The highest level of government must support the Strategy.
- The Strategy should establish a clear institutional framework to ensure that responsibilities and modalities for implementation are clear and that institutions have the authority and resources to act.
- Some areas, such as the protection of critical infrastructure including critical information infrastructure protection (CIIP), may require a specific policy focus that

addresses the intersection between digital security and protection of critical infrastructure.

- Harmonization of cybercrime laws combined with initiatives to facilitate faster and more effective coordination between law enforcement agencies and the private sector is essential. These efforts should pursue goals in line with Mexico’s constitution and its international and regional obligations, in an environment of respect for fundamental rights and liberties of citizens.
- Mexico should find the appropriate legislative path that allows a common understanding of the application of federal and state cybercrime legislation.

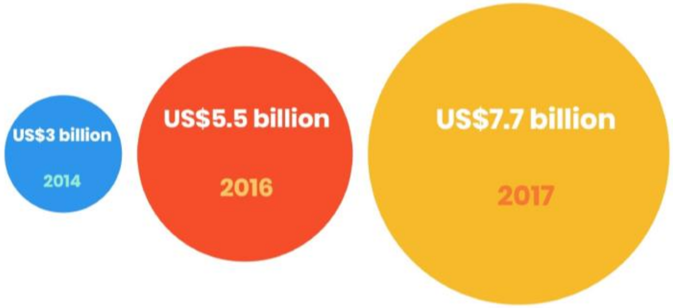
The State of Cybersecurity & Cyberfraud in Mexico

The Government of Mexico identifies the increase in use of Information and Communication Technologies (ICTs) in the daily activities of people, public and private organizations and recognizes its importance in the political, social and economic development of the country. It also highlights the inherent risks in using them. The trend points towards more people using more ICTs that result in an increase in vulnerabilities, risks, and threat.

It clearly lays out the cybercrime and cyberfraud scenario showing a large increase in Internet users in Mexico from 40 million in 2012 to 65.5 million in 2016. The rise of cyber incidents, according to the Scientific Division of the Federal Police in 2016, show a rise of 300 percent, from 20,000 in 2013 to 60,000 in 2016. False websites used for fraud have grown 11 percent tallying up 5,000 between 2015 and 2016. Transgressions by computer viruses have gone up 57 percent with 40,000 between 2015 and 2016. There has also been a substantial increase in cyberfraud, and figures from the National Commission for the Protection of Financial Service Users (CONDUSEF) reveal that the percentage and number of complaints in the first quarter of 2011 were 7 percent with 38,536 whereas by 2016 it was 42 percent with 639,857 grievances, averaging 193,000 a month. Most of the cyberfraud was committed through Internet transactions, primarily through e-Commerce, mobile banking, and individuals.

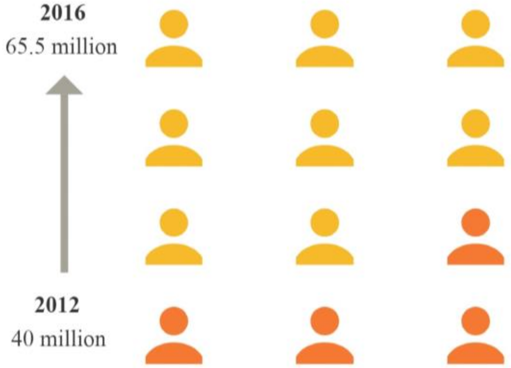
Cybercrime & Cyberfraud in Mexico

Cybercrime Cost 2014 - 2017



Symantec 2017

Increase in Internet Users



AIMX 2017

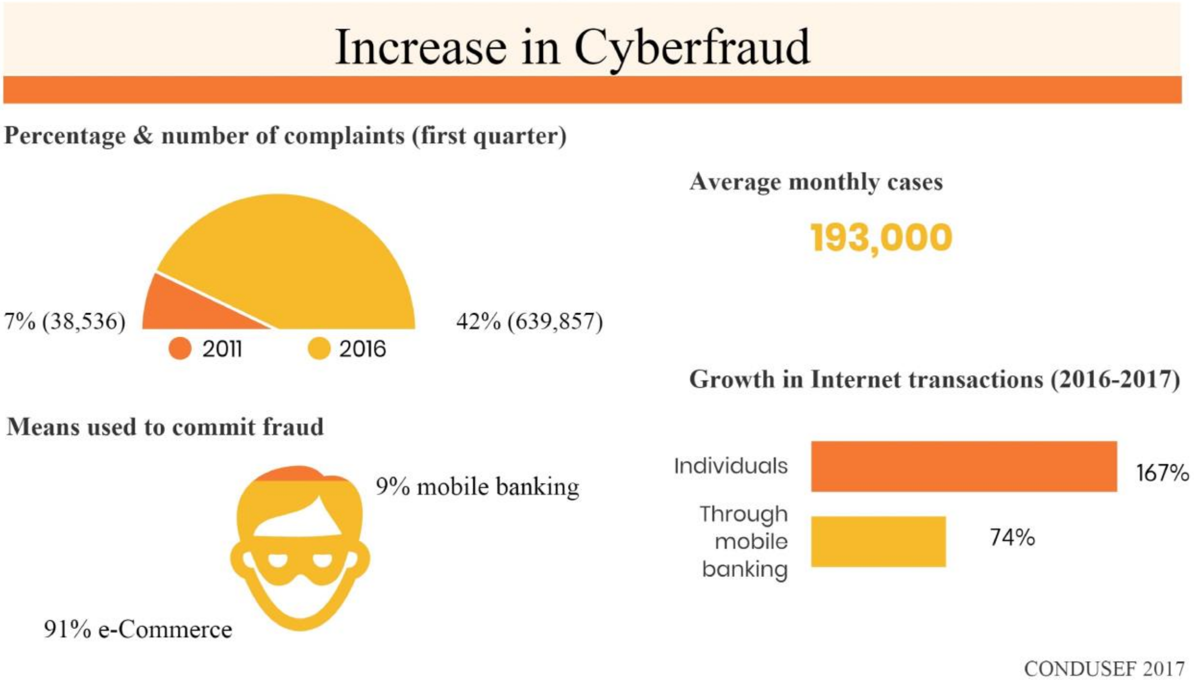
Increase in Cybercrime

Cyber incidents: 300%
(20,000 in 2013 / 60,000 in 2016)

False Websites used for fraud: 11%
(5,000 in 2015-2016)

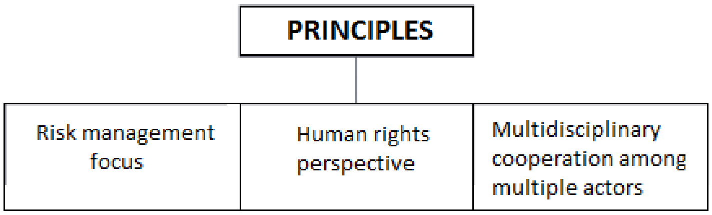
Transgressions by computer viruses: 57%
(40,000 in 2015-2016)

Scientific Division, Federal Police 2017



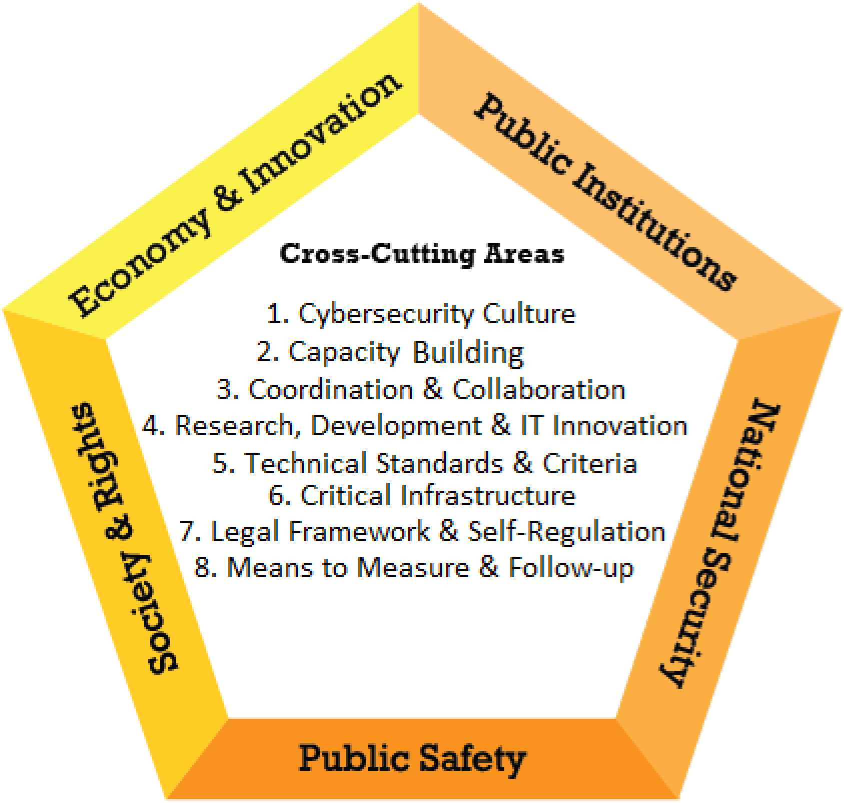
Mexico’s Strategy: The Three Principles and Five Objectives

The Strategy rests on three Governing Principles: a human rights perspective; a risk-management focus; and multidisciplinary cooperation among multiple actors. Human rights is an key topic for Mexico and focuses on maintaining a human rights perspective which includes freedom of expression, access to information, respect for privacy, the protection of personal data, health, education, and work. Risk management refers to the ability to deal with uncertain scenarios, preventive and corrective, to reduce the impact of ever evolving threats and risks in Cyberspace. Finally, the third principle deals with the collaboration of multiple actors and sectors of society based on Internet governance. The underlying theme here is a question of holistic and transversal development that opens the field for multidisciplinary teamwork.



The Strategy has five Strategic Objectives: society and rights; economy and innovation; public institutions; public safety; and national security. The first establishes the aim to create the conditions for a responsible, free, and trustworthy use of Cyberspace to promote a better quality of life that underpins, among other rights, freedom of expression, respect for private life, and the protection of personal data. The second of these proposes to strengthen cybersecurity mechanisms to protect the economy, support economic development, technological innovation, and a national cybersecurity industry. Protecting information and computer systems of public institutions is the third strategic objective and, as such, it seeks to do so in order to maximize their ability to provide uninterrupted and efficient services. In order to maintain public order and peace, the fourth objective sets forth to raise capacity building for the prevention and investigation of criminal conduct in Cyberspace. The fifth and last objective deals with National Security and aims at developing capacity building to prevent risks and threats in Cyberspace that can alter the independence, integrity, and national sovereignty.

STRATEGIC OBJECTIVES



Economy & Innovation

Public Institutions

National Security

Public Safety

Society & Rights

Cross-Cutting Areas

1. Cybersecurity Culture
2. Capacity Building
3. Coordination & Collaboration
4. Research, Development & IT Innovation
5. Technical Standards & Criteria
6. Critical Infrastructure
7. Legal Framework & Self-Regulation
8. Means to Measure & Follow-up

The Core of the Strategy: Eight Cross-Cutting Areas

In order to reach the Strategic Objectives set out in the National Security Strategy, there are eight Cross-Cutting Areas:

1. Cybersecurity Culture

These are the values, principles, and actions taken to raise awareness, education, and training that affect the way people interact in Cyberspace in a peaceful, trustworthy manner that is consistent with sustainable development. This will be achieved through public policy, strategies, programs, projects, actions, and initiatives that:

- Contribute to the promotion, fulfillment, and protection of individual rights and public and private organizations, with an emphasis on the protection of children and teenagers in Cyberspace.
- Favor the responsible use of ICTs; promote peaceful coexistence and the development of activities in Cyberspace.
- Motivate innovation, as well as the economy for a sustainable development.
- Strengthen the prevention of criminal risks and behavior that affect people and public and private organizations.
- Raise the level of trust and continuity in the services and in the digital public and private administration.
- Contribute towards risk prevention that can affect the information and operations critical infrastructure.

2. Capacity Building

These are actions directed at the generation and strengthening of organizational capacities, human capital, technological resources in cybersecurity, that allow for resources in risk management policy, threats in Cyberspace and national resilience. This will be met through public policy, strategies, programs, projects, actions, and initiatives that:

- Promote the development of human capital through cybersecurity specialists and professionals, professional leaders in cybersecurity as drivers of strategies and policies, research and development professionals for the cybersecurity industry and commerce, and professionals in research and prosecution of crimes committed through ICTs, as well as law enforcement.

- Set up the organization that will prevail in the private and public realm to position cybersecurity at a strategic level in public and private organizations, and establish mechanisms for participation of citizens in cybersecurity.
- Generate the technological infrastructure required for national technological development and gradual strengthening of cybersecurity in the country, and increase the technical capacities to identify and manage national cyber incidents.

3. Coordination & Collaboration

These are the coordinated efforts to consolidate a cybersecurity ecosystem and gain the necessary resilience to establish the preventive, proactive, and reactive mechanisms to bring trust and tranquility in the use of ICTs. This will be done by implementing the following actions:

- Strengthen international cooperation and collaboration.
- Identify the mechanisms of coordination and collaboration among the different national actors involved.
- Define and apply the cybersecurity governance model to share information and best practices.
- Establish protocols and communications channels to strengthen trust, reciprocity, and stimulate the social responsibility of all actors.

4. Research, Development & IT Innovation

These are the actions directed toward the mechanisms used to promote research, development, and innovation in the use of cybersecurity technology in favor of the development of human capital and technological innovation and to boost the cybersecurity home markets to develop its capacities and maturity of the national ecosystem. This will be done in order to:

- Establish the policies, programs, actions, and initiatives that detonate and consolidate the cybersecurity ecosystem to spark innovation in cybersecurity related ICTs.
- Promote scientific and technological innovation that propels the development of cybersecurity capabilities.
- Boost the national markets in cybersecurity that favor national technological autonomy and strengthen the national economy.

5. Technical Standards and Criteria

These are the actions that focus on the development, adoption, and strengthening of the standards, technical criteria, and the standardization in cybersecurity that allow for the approval and application of best practices and processes in the use and adoption of ICTs. The following is thus required:

- Establish the criteria, norms, and methodologies for the production, use, and adoption of hardware and software to strengthen the cybersecurity ecosystems and reduce the inherent risks and vulnerabilities of technology.
- Define the frameworks to strengthen cybersecurity in private and public organizations, academia, and society in general.
- Promote the participation of the academic, technical, and scientific community in developing and strengthening the standards and methodologies in cybersecurity.
- Identify and promote the use of international standards and best practices in cybersecurity.

6. Critical Infrastructure

These actions are required to establish the necessary mechanisms to reduce the probabilities of inherent risks and vulnerabilities in the use of ICTs for critical infrastructure management and to strengthen resilience to maintain stability and continuity of services should a cyber incident occur. This will be met through public policy, strategies, programs, projects, actions, and initiatives that:

- Establish policies and actions within the framework of the National Security Law and other national security instruments in collaboration with national security agencies.

7. Legal Framework & Self-Regulation

These are the actions and mechanisms to adapt the national legal framework to cybersecurity and self-regulation and to bring legal certainty to Internet users and society in general. To achieve this, it must go through public policy, strategies, programs, projects, actions, and initiatives that will:

- Train people on the digital ecosystem, Internet governance, and cybersecurity.

- Provide legal certainty to ensure that public and private institutions can cooperate and applying means to investigate, prevent, persecute, and sanction cybercriminals.
- Offer self-regulating mechanisms that promote trust within the law.
- Uphold the standardization of criminal codes and additional legislation in cybercrime and legal instruments.

8. Means to Measure & Follow-up

These are the policies and actions that promote and develop the approved measuring mechanisms that allow for a follow-up to the results obtained by the implementation of the National Cybersecurity Strategy and the impact of the social and economic development to the country to identify areas of opportunity and improvement. To achieve this, it must go through public policy, strategies, programs, projects, actions, and initiatives that will:

- Promote the collaboration of actors to draw-up the methodology that will allow for the construction of a national diagnosis on cybersecurity risks and threats.
- Establish centralized statistics related to the implementation and impact of cybersecurity and the Strategy in economic, political, and social spheres.
- Contribute to data gathering for improving and updating the National Cybersecurity Strategy.

Mexico and the United States in Cybersecurity

According to a 2018 study, "A Critical Juncture: Public Opinion in U.S.-Mexico Relations," the relationship between the two countries continues to be asymmetrical and is "at risk." NAFTA is also facing its most significant challenge for the first time since it went into effect in 1994. There is, however, continuity on security matters, intelligence sharing, and law enforcement cooperation, but since both sides decided to keep matters discreet with little publicity to avoid a nationalist whiplash in Mexico, it has backfired, as people on both sides are skeptical. Mexican opinion of the United States has hit a historic low with only 30 percent of Mexicans holding a favorable view of the United States and its president. Yet "the U.S. and Mexican governments now work closely together not only on economic issues but also public security, anti-money laundering, preventing terrorism, managing migration…the relationship largely continues full-steam ahead even as the new Trump administration in the United States has introduced challenging topics."

As Mexicans tend to vote based on national issues and not foreign policy, corruption and the economy weigh in more. It is difficult to say at this point if developing and implementing policies will provide for better cybersecurity without inhibiting cross-border supply chains. Another central issue is whether businesses feel confident in their international operations and in the safeguard of their intellectual property, while expecting the protection of standards and the prosecution of cybercrime.

Governments need to work together and with other stakeholders in a multidisciplinary and international manner to deal with an increase in digital attacks. In an effort to fight cybercrime in Latin America, Microsoft opened up an office in Colombia in 2016 when digital crimes were on the rise in this country. Soon afterwards, Mexico turned heads in 2017 due to the number and complexity of cyberattacks, and Microsoft kicked-off its Cybersecurity Engagement Center in Mexico City in February 2017.

Among other activities, the Center provides training to cybersecurity practitioners, focusing on government officials and the public sector. The goal is to reach a digital transformation that uses intelligence, data analysis, avant-garde digital forensics, and legal strategies to secure Cyberspace and relies on the Microsoft Cybercrime Center in Redmond, Washington and international support. In addition, the company signed a Government Security Program agreement with the Mexican Federal Police to strengthen IT security, share information and reinforce technological research. The Mexican Federal Police joined efforts with Google in 2016 in cybersecurity education.

Looking Ahead

On July 1, 2018, Mexicans will go to the polls to elect a new President along with voting in 128 federal senators, 500 federal deputies, nine state governors, mayors, and representatives of Congress. There are three strong contenders to the presidency: José Antonio Meade from the current ruling party, the PRI (Institutional Revolutionary Party), Andrés Manuel López Obrador from the new political party MORENA (Movement for National Regeneration), and Ricardo Anaya Cortes from the center-right PAN (National Action Party).

Ensuring a clean, fair, and transparent voting process is vital to maintaining trust in the electoral process that underpins national confidence in the country. Several scenarios can unfold in Mexico as the PRI administration sets forth the National Cybersecurity Strategy. International stories of electronic voter fraud and the use of the so-called “false news” to influence voter trends through social media have flooded the media. Should the Institutional Revolutionary Party win the 2018 elections with candidate José Antonio Meade, there may be a certain amount of momentum and continuity in pushing forward the Strategy.

Should the MORENA presidential candidate Andrés Manuel López Obrador move into Los Pinos, the Strategy may lose momentum as his policy proposals on security and education lean more towards a radical populist position. He has already called out voter fraud in 2006, claiming to have had his presidential turn taken away and taking over the core of downtown Mexico City to establish a rebel parallel government in protest. He ran and lost again in 2012.

Whatever the electoral results may be, Mexico’s National Cybersecurity Strategy is a step in the right direction toward guarding the country’s Critical Infrastructure, encouraging a cybersecurity ecosystem, and protecting national security. There is no stopping the force of the digital revolution, only moving in a bold, secure, and decisive manner to meet the challenges.

Which way is Mexico headed? Cyberspace is a multidimensional domain where technological innovation and human creativity meet endless possibilities. People and technology coming together to explore the boundaries of a digital transformation unprecedented in human history. Artificial intelligence is already at work in cars, drones, and home-assistants. Nanotechnology is pushing medical breakthroughs inside the human body, microchips and sensors are transforming the physical boundaries, and algorithms work out and sift through our daily activities using big data analytics. The way to go will depend on the permutations and combinations of future circumstances that we may not yet begin to conceive. One thing is certain, however, there is no standing still when it comes to living in the digital era. There is a long way to go from strategy to policy to protect infrastructure and e-services and to create an environment of economic prosperity. Nonetheless, the National Cybersecurity Strategy marks a path towards a stronger, more secure Mexico as a nation and as an active partner in the region and the world.

Bibliography

Altan Redes. (2017). *Red Compartida.* Retrieved from: http://altanredes.com/en/red-compartida/

Choucri, N. (2012). *Cyberpolitics in International Relations*. MIT Press.

Cybersecurity Ventures. (2017). *2017 Cybercrime Report*. Retrieved from: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Global Forum on Cyber Expertise. (2017). *About the GFCE*. Retrieved from: https://www.thegfce.com/about

Gobierno de México. (2017). *Estrategia Nacional de Ciberseguridad*. Retrieved from: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Gobierno de México. (2018). *Posición del Gobierno de México Sobre Informes Adicionales de Presuntas Actividades de la Agencia de Seguridad Nacional de Estados Unidos***.** Secretaría de Relaciones Exteriores, Embajada de México en Estados Unidos., Comunicados 2013. Retrieved from: https://embamex.sre.gob.mx/eua/index.php/es/comunicados/comunicados-2013/676-posicion-del-gobierno-de-mexico-sobre-informes-adicionales-de-presuntas-actividades-de-la-agencia-de-seguridad-nacional-de-estados-unidos

Goldsmith, J. (2011). *Cybersecurity Treaties: A Skeptical View.* Hoover Institution. Retrieved from: https://www.hoover.org/research/cybersecurity-treaties-skeptical-view

Glüsing, J. (2013). *NSA Accessed Mexican President's E-mail.* Retrieved from: http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html

Inter-American Development Bank. (2016). *Cybersecurity: Are We Prepared in Latin America and the Caribbean?* Retrieved from: https://publications.iadb.org/handle/11319/7449

International Telecommunications Union. (2017). *Global Cybersecurity Index 2017*. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Internet Association of Mexico. (2017). *Estudio Hábitos de los Internautas en México 2017.* Retrieved from: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/lang,es-es/?Itemid

McGuiness, Damien. (April 27, 2017). *How a Cyber Attack Transformed Estonia*. BBC News. Retrieved from: http://www.bbc.com/news/39655415

Meridian Process. (2017). *CIIP Good Practice Guides*. Retrieved from: https://www.meridianprocess.org/

Microsoft. (2017). *Microsoft Opens Cybersecurity Center to Protect Mexicans*. Retrieved from: https://news.microsoft.com/2017/02/24/microsoft-opens-cybersecurity-center-to-protect-mexicans/

Naegele, T. (January 17, 2018). *How AI Is Transforming Defense and Intelligence Technologies*. Govtech Works by General Dynamics IT. Retrieved from: https://www.govtechworks.com/how-ai-is-transforming-defense-and-intelligence-technologies/#gs.J7I4bfQ

National Chamber of the Electronics Industry. (2017). *Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado.* Retrieved from: http://www.canieti.org/Comunicacion/prensa/boletinesdeprensa/Presentaindustria.aspx

National Commission for the Protection of Financial Service Users. (2017). *Reclamaciones imputables a un posible fraude: 2011-2017 (primer trimestre).* Retrieved from: https://www.gob.mx/cms/uploads/attachment/file/240895/RECLAMACIONES_IMPUTABLES_A_UN_POSIBLE_FRAUDE_2011-2017_ver5.pdf

National Institute of Statistics and Geography. (2017). *Panorama general sobre el acceso a Internet y otras TIC en los hogares*. Retrieved from: http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Nal.pdf

Nye, J. (2017). *Deterrence and Persuasion in Cyberspace.* International Security, 41:3, pp. 44-71. Retrieved from: https://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00266

O'Connor, F. (November 2017). *NotPetya still Roils Company´s Finances, Costing Organizations $1.2 Billion in Revenue*. Cybereason. Retrieved from: https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue

Organization for Economic Cooperation and Development. (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.* Retrieved from: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Organization of American States. (2018). *Gestión del riesgo cibernético nacional*. Retrieved from: https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf

Organization of American States. (2017). *Recommendations for the Development of the National Cybersecurity Strategy, Technical Assistance Mission at the request of the Mexican Government.* Retrieved from: http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-049/17

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

Parraguez, L. (2017). *The State of Cybersecurity in Mexico: An Overview.* Mexico Institute, Woodrow Wilson Center. Retrieved from: https://www.wilsoncenter.org/publication/the-state-cybersecurity-mexico-overview

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

Reuters. (May 14, 2017). *Cyber Attack Hits 200,000 in at least 150 Countries: Europol*. Retrieved from: https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX

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

Statista. (2018). *Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025*. Retrieved from: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Symantec. (2018). *2017 Norton Cyber Security Insight Report Global Results*. Retrieved from: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

Tamkin, E. (April 27, 2017). *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?* Foreign Policy. Retrieved from: http://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

Trevino, M. (September 19, 2017). *Technology Can Reduce the Cognitive Overload in the C-Suite*. Information Week IT Network. Retrieved from: https://www.informationweek.com/strategic-cio/executive-insights-and-innovation/technology-can-reduce-the-cognitive-overload-in-the-c-suite/a/d-id/1329919

U.S. Government Department of Commerce. (2017). *International Trade Administration. The North American Leaders Summit*. Retrieved from https://www.trade.gov/nacp/nals.asp

Verizon. (2017). *Data Breach Digest: Perspective is Reality.* Retrieved from: http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf

Wilson, C., P. Paras, E. Enriquez. (November 2017). *A Critical Juncture: Public Opinion in U.S.-Mexico Relations*. Wilson Center Mexico Institute & Walsh School of Foreign Service. Retrieved from: https://www.wilsoncenter.org/publication/critical-juncture-public-opinion-us-mexico-relations

Wood, D. (January 10, 2018). *The Most Important 2018 Election for America May Be Mexico's*. The National Interest. Retrieved from: http://nationalinterest.org/feature/the-most-important-2018-election-america-may-be-mexicos-24013

World Economic Forum. (2016). *The Fourth Industrial Revolution*. Retrieved from: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Luisa Parraguez Kobek is a Fulbright Visiting Professor and Senior Researcher Scholar at the William J. Perry Center for Hemispheric Defense Studies, National Defense University in Washington DC & a Professor at Tecnológico de Monterrey, Mexico City Campus.

Special thanks to Fernando Barrios (graphic design), Abil Razo (infographics), Diorella Islas, Francisco Garcia Gonzalez, Mario Abrego, Adrian Trulin, Ursula Cuevas, Joav Pedraza, Roberto Dominguez, Marty Trevino, Jr., and Boris Saavedra.