Exercise Background Material

Mexico
Country Profile

Points of Contact: Rebecca Beigel, Julia Schuetze | Stiftung Neue Verantwortung e. V.
Beisheim Center | Berliner Freiheit 2 | 10785 Berlin

This document is exercise-specific information material and was developed for the purpose of a cybersecurity policy exercise only.

Disclaimer:

The research only represents a country's cybersecurity policy to a limited extent and is not an in-depth or complete analysis or assessment of current policy. In order to adapt the exercises to specific countries, it is important to understand the broader strokes of cybersecurity policies of other countries. Our team, therefore, researches publicly available information on cybersecurity policies of countries to adapt the exercises to country-specific needs. The research is shared with participants as background material in preparation for the exercise. Therefore, the documents have a timestamp and consider policy up until the date of publication. In the interests of non-profitability, we decided to make the background research publicly available. If you are using these materials, please include the disclaimer. Please also do not hesitate to contact us. The country profile was published in March 2022.

Points of Contact:

Rebecca Beigel

Project Manager for International Cybersecurity Policy

rbeigel@stiftung-nv.de

+49 (0)30 40 36 76 98 3

Julia Schuetze

Junior Project Director for International Cybersecurity Policy

jschuetze@stiftung-nv.de

+49 (0)30 81 45 03 78 82

Research support by:

Lina Siebenhaar

Student Assistent for International Cybersecurity Policy

lsiebenhaar@stiftung-nv.de

This document is exercise-specific information material and was developed for the purpose of a cybersecurity policy exercise only.

Table of Contents

Political System and Socio-Political Background

Key Facts

Political System

Socio-Political Context

Mexico‘s Cybersecurity Policy

Vulnerability and Threat Landscape

Key Documents

Legal Framework

Cybersecurity Architecture - Selected Institutions

Bilateral and Multilateral Cooperation

This document is exercise-specific information material and was developed for the purpose of a cybersecurity policy exercise only.

Political System and Socio-Political Background

Key Facts

- Official country name: United Mexican States[1]
- Capital: The Federal District (Mexico City)[2]
- Population: 126,014,024 in 2020[3]
- Official languages: Spanish, in addition, the government recognizes over 66 Indian languages[4]
- Currency: Mexican Peso[5]

Political System

Mexico is a federal republic consisting of 32 states[6]; its government system is presidential.[7] Constitutionally, powers are divided between the executive, legislative, and judicial branches.[8] The current head of state and head of government of Mexico is President Andrés Manuel López Obrador, affiliated with the National Regeneration Movement (Movimiento Regeneración Nacional, MORENA). He was elected as president in 2018.[9] Among others, the president can, for example, select a cabinet and Supreme Court justices. The legislative branch consists of the upper house, the Senate, and a lower house, the Chamber of Deputies.[10] The judicial branch is based on the Supreme Court of Justice of the Nation.[11]

Socio-Political Context

Mexico is considered one of the 15 largest economies in the world. It is the second-largest economy in Latin America, according to data by the World Bank.[12] Despite its economic wealth, based e.g., on natural resources and trade, it “has underperformed in terms of growth, inclusion, and poverty reduction compared to similar countries”[13] in the last three decades. Recently, the economy was heavily influenced by the COVID 19-pandemic, which led to a temporary contraction of 8.3 percent in 2020. Although the economy has been recovering since then, the pandemic emphasized national challenges such as poverty and inequality.[14] Mexico’s poverty rate reached a threshold of nearly 44 percent at the end of 2020.[15] The Organisation for Economic Co-operation and Development (OECD), in which Mexico has been a member since 1994, assesses that “inequality is higher than in most advanced economies”.[16]

In 2020, Mexico's internet penetration rate was approximately 72 percent[17]. Economic inequality and poverty are the main cause for a digital divide[18] that is evident, for example, between "rural and urban populations"[19]. Smartphones constitute the primary means to access the internet (96 percent).[20] Accordingly, the World Economic Forum's Global Competitiveness Report of 2019 assesses a level of 77.5 mobile per 100 people.[21] In terms of the adoption of internet communication technologies, Mexico ranks 74th out of 141 countries in the report.[22]

Internet freedom and freedom of the media remain constrained in Mexico. Freedom House analyzed that "manipulation of content, coordinated attacks against journalists, and violence, threats, and cyberattacks against other users"[23] are among the country's challenges. It, therefore, labeled Mexico's internet freedom as "partly free" in 2021. This decision is also based on recent governmental choices, such as changes in legislation and institutions, and shrinking spaces for critical voices online.[24] According to Reporters Without Borders, Mexico further "continues to be one of the world's most dangerous and deadliest countries for the media."[25] Journalists are regularly threatened, abducted, or murdered. Mexico, therefore, ranks only 143 out of 179 countries in the 2021 World Press Freedom Index.[26]

Mexico’s Cybersecurity Policy

Vulnerability and Threat Landscape

According to the FBI’s Internet Crime Report 2020, Mexico ranks 9th in the list of most targeted countries by malicious cyber activities globally.[27] The country experienced a number of cyber incidents that received public attention in recent years. These incidents targeted different sectors.

In June 2018, for example, a presumed Distributed Denial of Service incident affected a Mexican campaign website just days before the general elections. The incident targeted the website of Mexico’s political opposition party, National Action Party (Partido Acción Nacional, PAN), while the presidential candidates were debating on national television. Before the incident, documents criticizing the leading candidate Andres Manuel Lopez Obrador, who later won the elections, were published on the website.[28] Mexico’s ministries are not spared either. In February 2020, for example, Mexico’s economy ministry was affected by a cyber operation. According to a statement, the ministry noticed malicious cyber activities on its email and archive servers, emphasizing, however, that no sensitive information was compromised.[29]

In November 2019, the state-owned Mexican oil and gas company Pemex fell victim to an (assumed) DoppelPaymer ransomware incident. The threat actors demanded $5 million in bitcoin from the company.[30] According to news reports by Reuters, the incident “forced the company to shut down computers across Mexico, freezing systems such as payments.”[31] Later, the company declared that the incident was “neutralized” in a timely matter”[32] and that it affected only 5 percent of its computers[33]. It further highlighted that operations and production were unaffected. Pemex did not pay the ransom but faced high costs to clean its systems.[34]

In recent years, Mexico’s financial system also repeatedly faced cyber threats. In 2019, an OAS report revealed that 43 percent of the country’s large financial institutions were affected by cyber incidents throughout the year.[35] The Mexican central bank, Banco de México, published data that cyber operations against finance institutions went from one to four per trimester in 2019, targeting a range of services, such as ATMs or electronic transfers.[36] In April 2018, the Banco de México revealed that malicious actors targeted the real-time payment transfers of three banks in Mexico. Although the attempts were unsuccessful, all three banks were forced to use contingency plans.[37]

In December 2021, Japan’s largest auto parts manufacturer Denso, belonging to the Toyota Motor Corp, was hit by a ransomware incident. While domestic systems were spared and business operations abroad functioned regularly, the ransomware affected a Mexican plant with a breach of about “20 computers used in the plant and connected to an old network”[38]. A group of malicious actors, Rook, claimed responsibility, announcing it had stolen big amounts of data. The Mexican facility could resume its businesses in early January 2022, and important information for business operations could be secured. However, it "remains possible that the personal information of the workers at the Mexican plant was among the data stolen"[39]. Later, the data was partly disclosed.[40]

Key Documents

Several key documents shape the national cybersecurity policy landscape in Mexico, among them the National Cybersecurity Strategy, the National Digital Strategy 2021 - 2024, and the Homologated National Protocol for the Management of Cyber Incidents. The implementation of some of these key documents is proving difficult. According to analysts, the Mexican administration has not made cybersecurity a priority for the past few years, resulting, for example, in delays in the implementation of the National Cybersecurity Strategy.[41]

Mexico's cybersecurity policy is particularly influenced by the **National Cybersecurity Strategy** (Estrategia Nacional de Ciberseguridad, ENCS)[1], adopted in 2017.[42] According to the ENCS, the guiding principles during the development were a human rights perspective, a risk-management approach, and multidisciplinary and multi-stakeholder collaboration. The strategy's main objective is to enable private and governmental actors to take advantage of information and communications technologies (ICTs) "in a responsible manner and contribute to the sustainable development of Mexico".[43] This goal is translated into several strategic objectives[44]:

- Society and Rights: Enable the population to use and benefit from new technologies and cyberspace in a safe manner and with respect for their fundamental rights.
- Economy and Innovation: Develop Mexico's cybersecurity industry and improve cybersecurity to strengthen the resilience of the Mexican industry as a whole.
- Public Institutions: Protection of public digital infrastructures to ensure their functioning at all times.
- Public Security: Strengthen the investigation and prosecution of cybercrime to ensure security in the digital space.
- National Security: Build capacities to counter cyber threats that could, for example, affect national sovereignty or independence.

To further these strategic objectives, the ENCS defines eight crosscutting pillars. According to the ENCS, these eight pillars are:[45]

- Cybersecurity Culture: Cybersecurity culture is considered as a set of values, principles,

[1] Disclaimer on translation: The Spanish names of stakeholders, organizations, and (legal) documents were translated to English for better readability. Partly, these English names are not official translations. The official Spanish names are provided right after the English version, together with the respective abbreviations.

and actions defined in terms of awareness, education, and training carried out by all stakeholders that will boost innovation, strengthen the responsible use of digital technologies and reduce the risks of cybercrime. This is achieved, for example, by promoting safe and responsible behavior in cyberspace.

- Capacity Development: By strengthening the organizational capacities, human capital, and technological resources in cybersecurity, the Mexican society as a whole will enhance its resilience to cyber threats. To this end, Mexico, for example, invests in the training of its cybersecurity specialists and identifies opportunities for citizen participation in cybersecurity matters.
- Coordination and Collaboration: Mexico strengthens the exchange and confidence-building between all actors in the field of cybersecurity, including academia, civil society, and private organizations, on the national and international level. This is done, for example, by establishing appropriate protocols and communication channels.
- Research, Development and Innovation in ICT: Mexico increases support for research and development of cybersecurity technologies to strengthen the national cybersecurity market, stimulates innovation and develops cybersecurity skills among the workforce.
- Standards and Technical Criteria: To reduce the inherent risk of ICT, such as low-quality hard- and software, Mexico establishes criteria, standards, methodologies, and best practices that strengthen the cybersecurity capacities of organizations and products. For example, Mexico plans to promote international standards and best practices that are considered useful and effective
- Critical Infrastructures[2]: This includes the minimization of the exposure of critical infrastructures to cybersecurity risks and vulnerabilities and the strengthening of their resilience.
- Legal Framework and Self-Regulation: Mexico develops the capacities of all stakeholders to participate in the legal harmonization and strengthen the trust between actors to facilitate the prosecution of cybercrimes and the elaboration of self-regulation procedures. For example, Mexico plans to improve the understanding of cybersecurity and digitization issues among stakeholders in all relevant government, civil society, and private entities.
- Measurement and Monitoring: To measure the degree of implementation of the strategy and its impact on society, policies and actions are developed. In addition, potentials for improvement of the strategy are identified.

[2] The National Cybersecurity Strategy (please see “Key Documents”) provides the definition of Critical Information Infrastructure as follows: “the essential information infrastructures considered strategic that are related to the provision of goods and essential public services and whose disturbance could compromise National Security in terms of applicable law.” Among the 16 critical infrastructure sectors identified in the Homologated National Protocol for the Management of Cyber Incidents (please see “Key Documents”) are, for example, communications, emergency services, energy or public health.

The current administration also addresses cybersecurity in its **National Digital Strategy 2021 - 2024** (Estrategia Digital Nacional 2021 - 2024). The strategy was published in September 2021 by the Coordinator of the National Digital Strategy of the Office of the President of the Republic (Coordinador de Estrategia Digital Nacional de la Oficina de la Presidencia de la República).[46] It lists five main principles the government will concentrate on, among them the Principle of Information Security (Principio de Seguridad de la información). The main aim is to promote a culture of cybersecurity and promote public trust in governmental digital services. Planned measures to achieve this objective include elaborating a protocol to harmonize incident response or strengthening of cooperation among government institutions in the field of incident detection. This protocol has now been drafted and is presented in the next paragraph.

The **Homologated National Protocol for the Management of Cyber Incidents** (Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos), published in October 2021, aims to improve the security of government and academic institutions as well as private organizations.[47] It establishes a framework for recommended and responsible behavior before, during, and after cyber incidents that are aligned with international best practices.[48] In addition, the protocol defines the procedures for cooperation between the aforementioned entities and the National Cyber Incident Response Center (Centro Nacional de Respuesta a Incidentes Cibernéticos, CERT-MX).[49]

In addition to the documents mentioned, Mexican institutions, such as the Central Bank[50] and the Federal Institute of Telecommunications[51], publish institution-specific cybersecurity and digitization strategies that reflect their respective visions and goals. As these are not applied on the national level, they are explained in more detail in the chapter Cybersecurity Architecture - Selected Institutions below.

Legal Frameworks

Mexican legislation on information security and cybercrime is largely based on existing laws that are applied to the new circumstances and environment.[52] Although certain international cybersecurity regulations apply in Mexico, such as Mexico's commitment to strengthening its cybersecurity defense capabilities by entering into the United States-Mexico-Canada Agreement (please see “Bilateral and Multilateral Cooperation” below), the following section focuses solely on legal frameworks.[53]

Enacted in June 2014, the **Federal Telecommunications and Broadcasting Law (Ley Federal de Telecomunicaciones y Radiodifusión)**[54] introduced regulations for various types of telecommunications technologies and infrastructure, including the Internet. It obliges Internet Service Providers to comply with data protection regulations and sets an objective that all citizens should be able to gain access to the Internet. In addition, the law expands the regulatory power of the Federal Institute of Telecommunications (Instituto Federal de Telecomunicaciones, IFT), which can thus independently set rules for internet providers.

The **Federal Penal Code (Código Penal Federal)**[55] compiles Mexico's criminal law and also applies to offenses against cybersecurity and cybercrime. The Chapter, "Illicit Access to Computer Systems and Equipment"[56] (Acceso Ilícito a Sistemas y Equipos de Informática), criminalizes all modification and destruction of data on computer systems that are protected by security mechanisms. The penalties depend on the kind of computer system that was affected, with the most severe ones applying to access of state IT infrastructure, according to Article 211 of the Code.

Other forms of cybercrime are not directly addressed by the Criminal Code, but are covered by other offenses. Phishing can, for example, be prosecuted as a form of fraud under Article 386.[57]

The **General / Federal Law on the Protection of Personal Data held by Private Parties (Ley General de protección de datos personales en posesión de sujetos obligados)**[58], enacted in 2017, regulates the management and protection of personal data. It contains guidelines and rules that Data Controllers and Data Processors have to follow to guarantee the protection and integrity of the stored information. According to Article 33, they have to conduct risk analysis, taking into account existing vulnerabilities and threats and updating them regularly.

There have been several attempts by members of Mexico's legislative bodies to create specific cybersecurity laws in the past.[59] The latest law proposal was made in 2021 by Senator Jesús Lucía Trasviña Waldenrath, affiliated with Morena. Among other objectives, the proposed legislation would create a National Cybersecurity Agency (Agencia Nacional de Ciberseguridad) as well as a National Cybersecurity Commission (Comisión Nacional de Ciberseguridad) and amend the Federal Penal Code (Código Penal Federal) to define specific cybercrimes.[60] It has not yet been passed.[61]

Cybersecurity Architecture - Selected Institutions

Cybersecurity in Mexico is shaped by different national key actors, including the following government institutions, among others.

The **Secretariat of Infrastructure, Communications and Transportation** (Secretaría de Infraestructura, Comunicaciones y Transportes, SICT), is a first-level government agency, equivalent to a ministry, headed by the Secretary (Secretario) who is directly appointed by the President.[62] It is responsible for the development and implementation of policies concerning digitalization and ICTs. Its stated goal is to promote safe, efficient, and competitive transport and communication systems.[63] In collaboration with the Organization of American States, it published a study in 2019 in which it identified cybersecurity as a major problem for the accessibility of the Internet for all citizens, which is declared one of the central goals of the government, as the multitude of cybersecurity incidents undermines confidence in ICTs.[64] To address this issue, SICT is taking steps to promote the Mexican citizens' digital literacy and cybersecurity knowledge, such as publishing a guide on cybersecurity in telework[65] or developing a cybersecurity simulator, an interactive application through which users are made aware of the dangers of new technologies.[66]

Following an internal restructuring in 2020, the Undersecretariat for Communications and Technological Development (Subsecretaría de Comunicaciones y Desarrollo Tecnológico), a subdivision of the Secretariat previously responsible for most cybersecurity issues, was dissolved. Now, various departments within the Secretariat are responsible for the field.[67]

The **General Scientific Directorate of the National Guard** (Dirección General Científica de la Guardia Nacional) oversees several subunits that are tasked with the investigation and prevention of cybercrime, such as the National Cyber Incident Response Center (Centro Nacional de Respuesta a Incidentes Cibernéticos, CERT-MX) or the Center for Cyber Crime against Minors (Centro de Delitos Cibernéticos contra Menores, CENADEM).[68]

The **Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX)**[3] is charged with a multitude of tasks relating to cybersecurity. It assists critical infrastructure providers in a cyber incident and supports the Public Prosecutor's Office (Ministerio Público) with digital forensic investigations and technical analysis.[69]

Furthermore, the CERT-MX contributes to raising awareness for cybersecurity issues in the Mexican population. It issues alerts if new cyber threats are detected and its experts participate in awareness-raising measures, like the National Cyber Fraud Campaign.[70]

The CERT-MX serves as the primary point of contact for national and international incidents.[71] It is under the authority of the General Scientific Directorate of the National Guard (Dirección General Científica de la Guardia Nacional).[72]

Furthermore, the CERT-MX is part of the global Forum of Incident Response and Security Teams (FIRST).[73] This forum aims at facilitating the cooperation between different CERTs and other emergency response teams from different sectors and countries.[74]

The **Federal Institute of Telecommunications (Instituto Federal de Telecomunicaciones, IFT)** was created in 2013 by an amendment to the Constitution to regulate, promote and supervise the development of radio and telecommunications in Mexico.[75] The IFT is intended to be a financially and legally independent institution. The agency's governing body is the plenary, made up of seven commissioners that are first selected by a technical committee and the President and then confirmed by the Senate.[76] Under the current administration, several posts of commissioners are left vacant and the budget of the Institute was reduced.[77]

[3] The CERT-MX is currently referred to under different names, such as "Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional" (Gobierno de México: Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional. https://www.gob.mx/gncertmx?tab=¿Qué%20es%20CERT-MX?), "Centro de Respuesta a Incidentes Cibernéticos de Mexico" (FIRST: CERT-MX Team Information. https://www.first.org/members/teams/cert-mx) or "Centro Nacional de Respuesta a Incidentes Cibernéticos" (Secretaria de seguridad y protección ciudadana (2021): Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. https://bit.ly/3I0tV53).

With the emergence of new ICTs, the IFT enforced its activities in the field of cybersecurity. In December 2020, it published the Strategy IFT 2021-2025 (Estrategia IFT 2021-2025) for planning and streamlining the Institute's actions. In this document, the IFT identifies five goals and several strategies to achieve each goal. One goal, for example, is to promote the adoption of digital technologies and the development of the digital ecosystem. To achieve this goal, the IFT proposes to strengthen cybersecurity through a variety of measures, such as sharing targeted recommendations and best practices for using new technologies.[78]

The **National Institute for Transparency, Access to Information and Personal Data Protection** (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI) aims to guarantee access to public information and ensure the right to the protection of personal data.[79] The INAI focuses on raising awareness for cybersecurity issues among companies that handle personal data[80] and promoting a cybersecurity and data-sensitive culture among the general public.[81]

The Mexican central bank, **Banco de México,** was established in 1925. Its main purpose today is to preserve the value of Mexico's currency in the long term in order to improve Mexicans' well-being.[82] Its autonomy in the exercise of its functions and its administration is guaranteed by Article 28 of the Mexican Constitution.[83] Its governance structure consists of a board of five Governors, appointed by the President and approved by the Senate.[84] The Banco de México recognizes the relevance of cybersecurity issues, as financial institutions are particularly exposed to cyber risk due to their high degree of automation, process complexity and the amount of financial resources they manage.[85] For the internal regulation of cybersecurity, the Bank elaborated a Cybersecurity Strategy in 2021 (Estrategia de Ciberseguridad del Banco de México).[86] With respect to the larger banking sector, the Banco de México participated in the elaboration of the Principles for Strengthening Cybersecurity for the Stability of the Mexican Financial System (Principios para el Fortalecimiento de la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano), which a large majority of the Mexican financial sector pledged to respect.[87] The principles include[88] :

- Committing to cooperation and information sharing among financial institutions regarding cyber threats;
- Updating cyber defense methodologies and policies regularly;
- Educating end users and employees about responsible behavior in cyberspace.[89]

Bilateral and Multilateral Cooperation

Mexico is a member of the United Nations (UN), International Telecommunication Union (ITU), and the Organization of American States (OAS). These international organizations deal with and discuss cybersecurity-related topics.

Mexico was one of four U.S. countries that sent an expert to participate in the **Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security** (GGE), established by the General Assembly Resolution 73/266 and operating from 2019 to 2021.[90] Moreover, Mexico, as a member of the **United Nations** (UN), participates in the **Open-ended working group on developments in the field of information and telecommunications in the context of international security** (OEWG) by commenting on drafts of reports[91] or by publishing its own proposals.[92] In a joint proposal with Australia, Mexico, for example, calls for a regular survey on progress made by states in implementing the 2015 GGE report.[93]

Mexico has been a member of the **International Telecommunication Union** (ITU) since 1908 and is one of nine countries representing the Americas in the ITU Council.[94] The ITU aims to strengthen international cooperation, enhance the security of and confidence in ICTs, and provide necessary information to member states.[95]

Mexico is a member of the **Organization of American States** (OAS) that addresses cybersecurity as a part of its programs and in the specialized **Inter-American Committee against Terrorism** (CICTE).[96] The international organization has set up a Cybersecurity Program that focuses on "policy development, capacity development (including training and cyber exercises), research and outreach."[97] In the context of this program, Mexico received OAS assistance to develop its first National Cybersecurity Strategy in 2017.[98] Furthermore, cyber threats were addressed in multiple resolutions of the aforementioned CICTE.[99] The Plenary of the Committee adopted the Declaration Strengthening Cyber-Security in the Americas in 2012, underlining the necessity for all member states to develop their national cybersecurity capacities, for example, by strengthening their national incident response and by developing coherent cybersecurity strategies.[100] In 2015, the Declaration called Protection of Critical Infrastructure from Emerging Threats was passed, emphasizing the importance of critical infrastructure and the need to protect it from cyber threats.[101]

Mexico currently has the status of observer for the **Convention on Cybercrime (Budapest Convention)** and was formally invited to accede to the Convention.[102] The Convention aims to harmonize cybersecurity and cybercrime legislation and strengthen international cooperation in this field.[103] The Senate has expressed on several occasions, most recently in 2020, that it "respectfully urges the Ministry of Foreign Affairs to take the necessary actions so that the Mexican State adheres to the provisions of the Convention on Cybercrime of the Council of Europe and its additional protocol."[104]

Mexico joined the **Global Forum on Cyber Expertise** (GFCE) in 2015 and is a member of the Working Group on Policy & Strategy.[105] The GFCE is an organization with members that range from countries to intergovernmental and international organizations to private companies. Its goal is to build and exchange practical knowledge amongst these actors. The membership gives Mexico access to high-level and multi-stakeholder discussions on cybersecurity issues and allows it to profit from the clearinghouse function of the GFCE.[106]

Mexico's cooperation with the European Union takes multiple forms. Mexico was formally defined as a strategic partner in cybersecurity matters.[107] In 2021 the **high-level dialogue on justice and security** specifically addressed the fight against cybercrime, along with other security concerns, as an important step toward deepening cooperation between the two parties.[108] Furthermore, Mexico participated in a scenario-based discussion on addressing international security related to cyberspace, organized by the European External Action Service.[109]

In 2018, the Mexican President signed the **Agreement between the United States of America, the United Mexican States, and Canada** (USMCA) that entered into force in July 2021.[110] The trade agreement includes rules for digital trade (chapter 19) and provides new regulations for cybersecurity. The signing states agree in Article 19.15 to enhance their respective national cybersecurity incident response capabilities and reinforce cooperation in cyber defense.[111]

In regard to bilateral cooperation, the U.S.-Mexico partnership is particularly important for cybersecurity. To strengthen diplomatic ties and further cooperation between the two countries, Mexico and the United States developed the **U.S.-Mexico Bicentennial Framework for Security, Public Health, and Safe Communities**. One of the cooperation areas identified in the framework is cyberspace, to address threats faced by both countries.[112] In a joint statement on **U.S.-Mexico High-Level Security Dialogue** (HLSD), both countries underlined the importance of bilateral cooperation for cybersecurity and "commit to convening our bilateral cyber working group by 2022, with the goal of promoting international security and stability in cyberspace, sharing information, exploring ways to protect critical infrastructure, a focus on preventing and addressing cybercrime."[113]

At the **German-Mexican Dialogue on Quality Infrastructures**, Mexico and Germany have launched a so-called Work Plan 2021. Regarding cybersecurity, the plan identifies cybersecurity of supply chains as an important element for the success of economic cooperation.[114] Currently, a multidisciplinary team is developing a roadmap to facilitate the implementation of international cybersecurity standards.[115]

Sources

1 Secretaría de Relaciones Exteriores (2016): Basic Information about Mexico. https://embamex.sre.gob.mx/nigeria/index.php/en/information-about-mexico/mexico-facts

2 Secretaría de Relaciones Exteriores (2016): Basic Information about Mexico. https://embamex.sre.gob.mx/nigeria/index.php/en/information-about-mexico/mexico-facts

3 INEGI (2020): Población total. https://www.inegi.org.mx/temas/estructura/

4 Secretaría de Relaciones Exteriores (2016): Basic Information about Mexico. https://embamex.sre.gob.mx/nigeria/index.php/en/information-about-mexico/mexico-facts

5 Banco de México: History. https://www.banxico.org.mx/getting-to-know-banco-de-mexico/history-hierarchical-history-.html

6 Encyclopaedia Britannica (2022): Government and society. https://www.britannica.com/place/Mexico/Government-and-society

7 Instituto National Electoral: The Mexican Electoral System.

https://portalanterior.ine.mx/archivos3/portal/historico/contenido/The_Mexican_Electoral_System/

8 morena: HISTORIA DE MORENA. https://morena.si/nuestra-historia/

9 Encyclopaedia Britannica: Andrés Manuel López Obrador. https://www.britannica.com/biography/Andres-Manuel-Lopez-Obrador

Gobierno de México: México Presidencia de la República. https://www.gob.mx/presidencia/

10 Secretaría de Relaciones Exteriores: Government, political parties and laws. https://embamex.sre.gob.mx/nigeria/index.php/en/information-about-mexico/mexican-federal-government

Encyclopaedia Britannica (2022): Government and society. https://www.britannica.com/place/Mexico/Government-and-society

11 Instituto National Electoral: The Mexican Electoral System. https://portalanterior.ine.mx/archivos3/portal/historico/contenido/The_Mexican_Electoral_System/

Secretaría de Relaciones Exteriores: Government, political parties and laws. https://embamex.sre.gob.mx/nigeria/index.php/en/information-about-mexico/mexican-federal-government

12 The World Bank (2021): The World Bank In Mexico. https://www.worldbank.org/en/country/mexico/overview#1

13 The World Bank (2021): The World Bank In Mexico. https://www.worldbank.org/en/country/mexico/overview#1

14 OECD (2021): Mexico. https://www.oecd.org/economy/growth/Mexico-country-note-going-for-growth-2021.pdf

The World Bank (2021): The World Bank In Mexico. https://www.worldbank.org/en/country/mexico/overview#1

15 El Consejo Nacional de Evaluacion de la Politica de Desarrollo Social (2021): CONEVAL PRESENTA LAS ESTIMACIONES DE POBREZA MULTIDIMENSIONAL 2018 y 2020 https://bit.ly/33vwDAz

16 OECD: Our global reach. https://www.oecd.org/about/members-and-partners/

17 INEGI (2021): EN MÉXICO HAY 84.1MILLONES DE USUARIOS DE INTERNET Y 88.2MILLONES DE USUARIOS DE TELÉFONOS CELULARES: ENDUTIH 2020. (https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf

18 Mecinas Montiel (2016): THE DIGITAL DIVIDE IN MEXICO: A MIRROR OF POVERTY. https://www.elsevier.es/en-revista-mexican-law-review-123-articulo-the-digital-divide-in-mexico-S1870057816300464

19 Freedom House (2020): Mexico. https://freedomhouse.org/country/mexico/freedom-net/2020

20 INEGI and ift (2021): EN MÉXICO HAY 84.1MILLONES DE USUARIOS DE INTERNET Y 88.2 MILLONES DE USUARIOS DE TELÉFONOS CELULARES: ENDUTIH 2020. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf

21 Schwab, World Economic Forum (2019): The GlobalCompetitiveness Report. https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

22 Schwab, World Economic Forum (2019): The GlobalCompetitiveness Report. https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

23 Freedom House (2020): Mexico. https://freedomhouse.org/country/mexico/freedom-net/2020

24 Freedom House (2021): Mexico. https://freedomhouse.org/country/mexico/freedom-net/2021

25 Reporters Without Borders (2021): Mexico. https://rsf.org/en/mexico

26 Reporters Without Borders (2021): Mexico. https://rsf.org/en/mexico

27 ControlRisks (2021): Mexico Cyber Threat Outlook Report. https://www.controlrisks.com/our-thinking/insights/reports/mexico-cyber-threat-outlook-report

Federal Bureau of Investigation (2020): Internet Crime Report 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

28 Reuters (2018): A cyberattack took down a Mexican campaign website 2 weeks before the election. https://bit.ly/3LGKo0o

29 Barrera (2020): Mexico's economy ministry hit by cyber attack. https://www.reuters.com/article/us-mexico-economy-cyberattack-idUSKCN20J0BI

Secretaría de Economía (2020): Controla Secretaría de Economía ataque informático. https://www.gob.mx/se/articulos/controla-secretaria-de-economia-ataque-informatico?idiom=es

30 Barrera and Satter (2019): Hackers demand $5 million from Mexico's Pemex in cyberattack. https://www.reuters.com/article/us-mexico-pemex-idUSKBN1XN03A

CISOMAG (2019): Hackers Demand US$ 5 Million in Ransom from Mexico's Pemex. https://cisomag.eccouncil.org/hackers-demand-us-5-million-in-ransom-from-mexicos-pemex/

31 Barrera and Satter (2019): Hackers demand $5 million from Mexico's Pemex in cyberattack. https://www.reuters.com/article/us-mexico-pemex-idUSKBN1XN03A

32 Reuters (2019): Mexico's Pemex says operations normal after cyber attack. https://www.reuters.com/article/us-mexico-pemex-cyber-idUSKBN1XM07U

33 Pemex (2019): Pemex opera con normalidad. https://www.pemex.com/saladeprensa/boletines_nacionales/Paginas/2019-47_nacional.aspx

Reuters (2019): Mexico's Pemex says operations normal after cyber attack. https://www.reuters.com/article/us-mexico-pemex-cyber-idUSKBN1XM07U

34 Barrera and Satter (2019): Hackers demand $5 million from Mexico's Pemex in cyberattack. https://www.reuters.com/article/us-mexico-pemex-idUSKBN1XN03A

Pemex (2019): Pemex opera con normalidad. https://www.pemex.com/saladeprensa/boletines_nacionales/Paginas/2019-47_nacional.aspx

35 OAS (2019): OAS Report Reveals 43% of Large Financial Institutions in Mexico Suffered Cyber Incidents in the Last Year. https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-052/19

36 Banco de México (2019): Reporte de Estabilidad Financiera. https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/%7B04E197EE-B6FC-7BA1-72A0-32D3E6C9BF28%7D.pdf

Martínez (2020): Cyberattacks against Mexican banks are on the rise. https://bit.ly/350uRYt

37 Schwartz (2018): Hackers Target 3 Mexican Banks' Real-Time Transfers. https://www.bankinfosecurity.com/hackers-target-3-mexican-banks-real-time-transfers-a-10927

38 THE ASAHI SHIMBUN (2022): Auto parts maker Denso targeted in ransomware cyberattack. https://www.asahi.com/ajw/articles/14521880

39 THE ASAHI SHIMBUN (2022): Auto parts maker Denso targeted in ransomware cyberattack. https://www.asahi.com/ajw/articles/14521880

40 THE ASAHI SHIMBUN (2022): Auto parts maker Denso targeted in ransomware cyberattack. https://www.asahi.com/ajw/articles/14521880

41 Berg and Ziemer (2021): The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment. https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment

42 Gobierno de México (2017): National Cybersecurity Strategy. https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf

43 Gobierno de México (2017): National Cybersecurity Strategy. https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf

44 Gobierno de México (2017): National Cybersecurity Strategy. https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf

45 Gobierno de México (2017): National Cybersecurity Strategy. https://www.gob.mx/cms/uploads/attachment/file/399655/ENCS.ENG.final.pdf

46 Secretaría de Gobernación (2021): ACUERDO por el que se expide la Estrategia Digital Nacional 2021-2024. http://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021

47 Presidencia de la República Coordinación de Estrategia Digital Nacional and Secretaría de Seguridad y Protección Ciudadana Guardia Nacional (2021): Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. https://bit.ly/3gqDiyP

48 Seguridad y Defensa (2020): GN trabaja en Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. https://bit.ly/3AZVNUd

49 Secretaría de Seguridad y Protección Ciudadana Guardia Nacional (2021): Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos. https://bit.ly/3gqDiyP

50 Banco de México (2021):Estrategia de Ciberseguridad del Banco de México. https://bit.ly/3LfbiMI

51 Instituto Federal De Telecomunicaciones (2020): ESTRATEGIA IFT 2021-2025. http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/estrategia20202025acc.pdf

52 Ciberseguridad: México. https://ciberseguridad.com/

53 United States Trade Representative: Chapter 19 Digital Trade. https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

54 CÁMARA DE DIPUTADOS DEL H.CONGRESO DE LA UNIÓN (2014): LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN. https://bit.ly/3oFOr3j

55 Justia México (2020): Código Penal Federal Libro Segundo Título Noveno - Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática Capitulo II - Acceso Ilícito a Sistemas y Equipos de Informática. https://bit.ly/3owgWjL

56 Justia México (2020): Código Penal Federal Libro Segundo Título Noveno - Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática Capitulo II - Acceso Ilícito a Sistemas y Equipos de Informática. https://bit.ly/3owgWjL

57 Creel García-Cuéllar Aiza y Enriquez SC (2020): Cybersecurity in Mexico. https://www.lexology.com/library/detail.aspx?g=60c54f8c-7cce-4dac-89b8-79dfb217e054

58 CÁMARA DE DIPUTADOS DEL H.CONGRESO DE LA UNIÓN (2017): LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

59 Covarrubias (2021): Análisis de la iniciativa que expide la Ley General de Ciberseguridad, presentada el 25/03/2021. https://bit.ly/3Jkrbzs

60 Senado de la República LXIV Legislatura (2021): INICIATIVA DE LA SENADORA JESÚS LUCÍA TRASVIÑA WALDENRATH, CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD Y SE DEROGAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL. Inic_Morena_Sen_Trasvina_Ciberseguridad_Penal.pdf

61 Gaceta del Senado (2021): Iniciativas. https://www.senado.gob.mx/64/gaceta_del_senado/documento/116270

62 Gobierno de México: Gobierno. https://www.gob.mx/gobierno

63 Secretaría De Infraestructura, Comunicaciones y Transportes : Acciones y Programas. https://www.gob.mx/sct#2353

64 Secretaría de Comunicaciones y Transportes (2019): Publican estudio sobre hábitos de los usuarios en ciberseguridad en telecomunicaciones y radiodifusión. https://bit.ly/3HxiMbN

65 Secretaría de Comunicaciones y Transportes (2020): La SCT presenta una Guía de Ciberseguridad en apoyo al teletrabajo. https://bit.ly/3HAoU2L

66 Ochoa (2019): Ciberseguridad, un tema de todos: SCT y OEA. https://www.itmasters-mag.com/noticias-analisis/ciberseguridad-un-tema-de-todos-sct-y-oea/

67 Secretaría de Comunicaciones y Transportes (2020): La Secretaría de Comunicaciones y Transportes informa. https://bit.ly/3HxWxT3

68 Borredá and Valadés (2021): Comisario Jacobo Bello Joya: “La Guardia Cibernética protege las infraestructuras críticas mexicanas”. https://bit.ly/3GwAkmZ

69 Gobierno de México (2021): Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional. https://www.gob.mx/gncertmx?tab=¿Qué%20es%20CERT-MX?

70 Guardia Nacional CERT-MX (2022): 05 ENE 2022 - Recomendaciones para evitar un fraude cibernético 12:00 - 13:30 hrs. https://www.gob.mx/gncertmx/articulos/116663

71 Gobierno de México (2021): Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional. https://www.gob.mx/gncertmx?tab=¿Qué%20es%20CERT-MX?

72 Secretaría de Seguridad y Protección Ciudadana (2020): La Guardia Nacional ocupa un nuevo espacio de seguridad en beneficio de los usuarios de internet: Alfonso Durazo. https://bit.ly/3gtt7cK

73 FIRST: CERT-MX.https://www.first.org/members/teams/cert-mx

74 FIRST: FIRST Vision and Mission Statement. https://www.first.org/about/mission

75 Instituto Federal De Telecomunicationes: Conócenos Línea de tiempo. http://www.ift.org.mx/conocenos/acerca-del-instituto/historia

76 Instituto Federal De Telecomunicationes: Conócenos Pleno. http://www.ift.org.mx/conocenos/pleno/integrantes-del-pleno

77 Berg and Ziemer, Center for Strategic & International Studies (2021): The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment. https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment

78 Instituto Federal De Telecomunicaciones (2020): ESTRATEGIA IFT 2021-2025. http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/estrategia20202025acc.pdf

79 INAI: ¿Qué es el INAI?. https://home.inai.org.mx/?page_id=1626

80 https://home.inai.org.mx/wp-content/uploads/Recomendaciones_Manejo_IS_DP.pdf (S. 49)

81 INAI (2020): 10 Recomendaciones. https://bit.ly/3urTZCd

82 Banco de México: Mission and vision. https://www.banxico.org.mx/getting-to-know-banco-de-mexico/mission-and-vision-objetives-.html

83 Constitute Project (2021): Mexico’s Constitution of 1917 with Amendments through 2015 https://bit.ly/3oTHX0z.

84 Banco de México: Junta de Gobierno. https://bit.ly/3gpqn05

85 Banco de México: Ciberseguridad. https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html

86 Banco de México (2021):Estrategia de Ciberseguridad del Banco de México. https://bit.ly/3LfbiMI

87 Secretaría de Hacienda y Crédito Público, Comisión Nacional Bancaria Y De Valores: Foro C1ber Segur1dad. https://www.gob.mx/cms/uploads/attachment/file/274782/Resumen-Ciberseguridad.pdf

88 Secretaría de Hacienda y Crédito Público (2017): 5 medidas de fortalecimiento de la ciberseguridad para la estabilidad del Sistema Financiero Mexicano. https://bit.ly/3gsZrfP

89 Secretaría de Hacienda y Crédito Público (2017): 5 medidas de fortalecimiento de la ciberseguridad para la estabilidad del Sistema Financiero Mexicano. https://bit.ly/3gsZrfP

90 United Nations Office for Disarmament Affairs (2021): Group of Governmental Experts. https://www.un.org/disarmament/group-of-governmental-experts/

91 UNODA (2020): Preliminary comments of Mexico to the initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2020/04/mexico-inputs-pre-draft-oewg.pdf

92 UNODA: Proposal of Mexico for a Follow-Up Implementation Mechanism. https://bit.ly/3ouS2B4

93 UNODA (2020): Mexico-Australia Proposal for OWEG Report Text. https://bit.ly/3gSP9pB

94 ITU (2019): ITU Council Membership. https://www.itu.int/en/council/Pages/members.aspx

95 ITU: ITU Cybersecurity Activities. https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

96 OAS (2021): Member State: Mexico. https://www.oas.org/en/member_states/member_state.asp?sCode=MEX

97 OAS (2021): Cybersecurity Program. https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

98 OAS (2017): Mexico Presented National Cyber Security Strategy Developed with OAS Support. https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-082/17

99 OAS: Cyber Security. https://www.oas.org/en/topics/cyber_security.asp

100 INTER-AMERICAN COMMITTEE AGAINST TERRORISM (2012): DECLARATION STRENGTHENING CYBER-SECURITY IN THE AMERICAS. https://ccdcoe.org/uploads/2018/11/OAS-120307-DeclarationCSAmericas.pdf

101 INTER-AMERICAN COMMITTEE AGAINST TERRORISM (2015): DECLARATION PROTECTION OF CRITICAL INFRASTRUCTURE FROM EMERGING THREATS. https://bit.ly/3sjTI1r

102 Inter-American Development Bank (2020): CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE Reporte Ciberseguridad 2020. https://bit.ly/3rw97wv

103 Council of Europe (2021): Acceding to the Budapest Convention on Cybercrime: Benefits. https://rm.coe.int/cyber-buda-benefits-june2021a-en/1680a2ddb0

104 Gaceta del Senado (2020): Gaceta: LXIV/3PPO-7/111988. https://www.senado.gob.mx/64/gaceta_del_senado/documento/111988

105 GFCE: Member Profile Page Mexico. https://thegfce.org/member/mexico/

106 GFCE: About the GFCE. https://thegfce.org/about-the-gfce/

107 http://aei.pitt.edu/94368/1/EPS-EU-cyber-partners_RENARD_AM.pdf

108 Secretaría de Relaciones Exteriores (2021): Mexico and the European Union deepen their collaboration on security and justice. https://bit.ly/3gSycvm

109 EEAS (2021): Cyberspace: Strengthening cooperation in promoting security and stability. https://bit.ly/3oZGXbA

Presidencia de la República EPN (2018): Mexico, the United States and Canada Sign USMCA.

https://www.gob.mx/epn/prensa/mexico-the-united-states-and-canada-sign-usmca-183674

110 Presidencia de la República EPN (2018): Mexico, the United States and Canada Sign USMCA.

https://www.gob.mx/epn/prensa/mexico-the-united-states-and-canada-sign-usmca-183674

111 United States Trade Representative: Chapter 19 Digital Trade. https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

112 U.S. Department of State (2022): Summary of the Action Plan for U.S.-Mexico Bicentennial Framework for Security, Public Health, and Safe Communities. https://bit.ly/3sjTKX7

113 U.S. Mission to Mexico (2021): Joint Statement: U.S.-Mexico High-Level Security Dialogue. https://mx.usembassy.gov/joint-statement-u-s-mexico-high-level-security-dialogue/

114 GPQI (2020): German-Mexican QI Dialogue: Defining the Work Plan 2021. https://bit.ly/3sN4CwX

115 GPQI (2021): Work Plan 2022 of the German-Mexican QI Dialogue signed. https://www.gpqi.org/news_en-details/work-plan-2022-of-the-german-mexican-qi-dialogue-signed.html