CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

MAY 2024

Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO

Joe Devanny and Russell Buchan

Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO

Joe Devanny and Russell Buchan

Carnegie does not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Contents

Introduction

Mexico published its first National Cybersecurity Strategy (ENCS) in 2017.[1] Since then, its cyber policy has suffered from a lack of political prioritization during the presidency of Andrés Manuel López Obrador (AMLO), who was elected the following year. Absent reinvigorated presidential interest from his successor—who takes office in October 2024, after the election in June—there is little prospect that the ENCS will be comprehensively implemented or that significant progress will be made in addressing cyber threats.

This paper examines the political, legal, public policy, and diplomatic aspects of Mexico's cyber policy, which has stalled under AMLO. The country faces significant cybersecurity challenges, and the neglected ENCS still offers a plausible starting point for what it needs to do. With AMLO constitutionally limited to one term, it will be up to the winner of the 2024 presidental election to rejuvenate the national approach to cyber. Mexico can achieve progress through more active presidential coordination, greater institutionalization of cybersecurity, and more investment in education and skills and in developing Mexico's cybersecurity culture and system.

The fact that cyber policy under AMLO has not kept pace with the threats the country faces is particularly unfortunate. In recent years, Mexico has suffered from the same sharp rise in cyber crime, such as ransomware attacks, that other states have experienced. This does not appear to have stimulated a response commensurate with the threat by the federal government.[2] Indeed, AMLO's spending controls have included the cancellation of funds to improve cybersecurity.[3] Pervasive corruption and human rights abuses are significant problems in the domestic security system—including with regard to cyber, most notably allegations about the use of commercial spyware to surveil journalists and critics of the government.[4]

The rising tide of cyber crime—in particular the Guacamaya hacktivist group's 2022 hacking of the Ministry of National Defense and leaking sensitive documents to the media suggesting misconduct by the armed forces[5]—shows the breadth and scale of Mexico's problem. However, the development of the ENCS in 2017 under then president Enrique Peña Nieto suggests that, with better coordination and leadership, the country could yet improve its resilience and cybersecurity capacity.[6]

At the same time, Mexico's cyber diplomacy has changed little under AMLO. The country continues to be an active and constructive participant in multilateral and bilateral initiatives aimed at creating a free, open, peaceful, and secure internet, such as the UN Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security and the United Nations (UN) negotiations for a new cyber crime treaty. This has been a positive factor but it also shows the gap between the shortcomings of Mexico's domestic cyber policies and the aspirations of its cyber diplomacy.

The proximity of the United States and Mexico's interdependency with it in addressing shared security challenges means their relationship is likely of paramount importance for the provision of cybersecurity assistance and capacity building to Mexico. The two countries have collaborated on various relevant bilateral, minilateral, and multilateral initiatives in recent years. The implementation of the United States-Mexico-Canada Agreement (USMCA) is a high point, and it has an ambitious chapter on digital trade. However, the difficulties in relations with Washington under AMLO (which may or may not subside depending on the outcomes of the presidential elections in Mexico, in June 2024, and the United States, in November 2024) have created opportunities for other states to deliver capacity-building assistance in cyber to Mexico. This need not be limited to the federal level and could include increasing engagement with specific federal states or sectors in the country.

A lack of national strategic coordination and cyber expertise are two shortcomings in Mexico's approach to cybersecurity. These are two possible areas for other countries to target in future cooperation. The United States and the United Kingdom, for example, have strong experience when it comes to greater institutionalization, rolling out education and training initiatives, and cultivating a vibrant cybersecurity system including corporate and nonprofit actors, which can be blueprints for an integrated approach to capacity-building in Mexico.[7]

Cybersecurity in Mexico

Mexico has a growing and increasingly technologically sophisticated economy, but it lacks the capacity to make steady improvement in cybersecurity. Corruption and political abuses—such as the alleged use of commercial spyware against critics of the government—are major obstacles to formulating and implementing an effective national cyber policy.[8] According to one estimate, Mexico has the highest rate of cyber crime in Latin America.[9] This is a plausible assessment given the size of its economy (the fifteenth-largest in the world[10]) and the degree of internet penetration in the country (which currently stands at 83.2 percent, although there is a sharp digital divide between urban and rural areas, with just over 15 percent of rural households online).[11] In 2021, the cyber threat intelligence company Mandiant estimated that Mexico accounted for the second-highest percentage (17 percent) of online advertisements regarding ransomware data theft in Latin America, which is one proxy metric for the magnitude of the cyber crime problem.[12]

Mexico generally is placed somewhere in the middle of the global cyber capability rankings. For example, in the most recent Global Cybersecurity Index produced by the International Telecommunications Union index (2020), Mexico was fifty-second, with only the United States (first), Canada (eighth), and Brazil (eighteenth) ranked higher in the Americas.[13] Mexico does not appear in the Belfer Centre's most recent (2022) "Top 30" Cyber Power Index, with Brazil as the only state in Latin America to merit a ranking.[14]

Regionally, however, Mexico is near the top of cyber capability rankings. For instance, a 2020 study placed the country in Latin America's second tier with regard to implementation across the Organization of American States (OAS) of the internationally respected Oxford Cybersecurity Capacity Maturity Model for Nations and in the first tier for "cyber power" given the size of its economy and the fact that it has had to contend with significant security threats posed by sophisticated transnational organized crime groups.[15] This assessment juxtaposes the potential for Mexico to achieve greater capability with its patchy level of governmental coordination and its poor track record in policy reform, institutional capacity building, and improving resilience.[16]

Notwithstanding the legitimate concerns about how much weight should be afforded to such rankings, they give a sense of Mexico's global position and regional status. Despite its domestic challenges, it compares favorably with the rest of Latin America.

The National Cybersecurity Bill

Mexico has not adopted a national cybersecurity law. Instead, legal provisions on cybersecurity are dispersed across laws in different sectors, such as finance, telecommunications, labor, consumer protection, and intellectual property. In April 2023, Congress introduced the long-awaited National Cybersecurity Bill.[17] With ninety-two articles and eight transitory articles, this is a detailed and wide-ranging piece of legislation that would establish a comprehensive cybersecurity regime. Some of its most important provisions include:

- Developing specific legal protections for digital rights (for example, digital inclusion, net neutrality, and online consumer protection)

- Requiring private companies to collaborate with the government to address cybersecurity matters

- Creating an executive-controlled National Cybersecurity Agency to coordinate cybersecurity efforts, including monitoring networks, responding to incidents, and undertaking countermeasures to combat malicious cyber activity

- Empowering the Directorate General of Cyber Investigations and Technological Operations to request the takedown of internet websites and data considered harmful to the public

- Introducing specialized prosecutors and judges for cybersecurity

- Establishing a database of individuals, groups, and organizations of malicious cyber actors

The bill proposes to radically transform the regulation of Mexico's cybersecurity system. It would give significant powers to law-enforcement agencies to counter cyber threats. There are legitimate concerns about potential government overreach in cyberspace, given recent revelations concerning cyber surveillance activities, and these apply to the bill.[18]

The approach of the presidential election may have reduced the political appetite to push forward quickly with the bill. This could again be a case of politics undermining the possibility of progress in cybersecurity policy.[19] Fresh proposals were made in March 2024 to revise the draft bill, provoking concerns about its impact on surveillance legislation and the role of the armed forces in domestic cyber operations.[20] Should the revised version of the bill be enacted, its subsequent implementation could meet the same fate as the 2017 ENCS, whose first implementation year was also an election one.

Politics and Cyber Policy

AMLO has largely ignored the ENCS, as some analysts had anticipated before he was elected.[21] It was in its first implementation phase when he entered office, and was essentially a high-level, structured overview of the key actors, objectives, and principles underpinning a strategic approach to cybersecurity. The ENCS designates five strategic priority areas: society and rights, economy and innovation, public institutions, public safety, and national security. Three principles underpin it: protecting human rights, risk management, and implementing a coordinated approach within government and between government and other sectors and stakeholders. It also outlines eight workstreams: creating a cybersecurity culture; building capacity; coordination and collaboration; research, development, and innovation; technical standards; critical infrastructure; legal framework; and metrics.[22]

The ENCS is not perfect. Critics have argued that it focuses more on protecting digital rights than reducing cyber threats; lacks depth of analysis of contemporary cyber crime; and lacks clarity about how different institutions can coordinate to achieve progress.[23] But most commentators agreed that its adoption was a step in the right direction, taken at the same time as several other states in the region were also producing their strategies.

More than six years have passed since the adoption of the ENCS. Given rapid developments in technology and the threat landscape, the ENCS is at risk of becoming outdated. The impending change of administration provides a good opportunity to refresh it. Whether or not the next president orders the development of a new strategy, if the political will exists the ENCS has laid the building blocks for a more structured, coordinated, and actively led approach to improving the institutionalization of cybersecurity and to investing in capability, education, skills, and the national cybersecurity system.

Implementation is another matter, however. The state's ability to effectively implement a cyber policy is undermined by pervasive corruption, the strength of organized crime groups, and—paradoxically—the disruption to administrative continuity caused by periodic institutional reforms to address these two issues.[24] There are also concerns about abuses of commercial spyware by the domestic security and national defense forces, before and during AMLO's presidency.[25] This creates obvious challenges for cyber capacity-building and external actors should make their assistance subject to strict conditions, put in place safeguards before it is provided, and establish effective monitoring and oversight mechanisms during and after its provision. As with other areas of capacity building, this assistance should be aligned with wider, structural reforms.

The lack of momentum under AMLO does not mean that nothing has been achieved. For example, some progress has been made in coordinating cyber incident management processes[26] and in curating a national register of cyber incidents.[27] A wider National Digital Strategy 2021–2022 was published in 2021, which focuses more on the importance of digital technology for sustainable development than on elaborating new policies or governance frameworks for cybersecurity.[28] National legislators have worked toward the development of a national cybersecurity law.[29] Mexico also assumed the pro-tempore secretariat of the Ibero-American Forum of Cyber Defense in 2021–2022.[30]

Notwithstanding these continuing efforts, recent analyses of Mexico's cybersecurity governance have noted a list of consequential obstacles. These include: poor coordination at the federal level;[31] lack of public trust in the executive; a deficit of education, skills, and resources to invest in national capability; and insufficient regulatory and oversight arrangements.[32] These are not exclusive to the field of cybersecurity, and AMLO has been criticized for adopting a generally authoritarian and populist approach to the presidency, hollowing out institutions and reducing checks on presidential power.[33] The point should not, perhaps, be taken too far. Two senior OAS cybersecurity officials have argued that all states in the region have faced persistent challenges with coordination and implementing effective cyber capacity-building.[34]

Mexico's Cyber Diplomacy

There has been more continuity under AMLO in Mexico's approach to cyber diplomacy, where it is a constructive—but also a cautious—actor. The president has displayed only a few clear interests in foreign policy, such as the importance of asserting Mexico's sovereignty, qualified pursuit of Chinese investment in infrastructure, and echoing Mexico's historical doctrine of nonintervention when it comes to Venezuela as well as Russia's invasion of Ukraine.[35] This approach to foreign policy is unlikely to make AMLO (or the next administration) approve Mexico's participation in any coordinated public attribution of malicious state behavior in cyberspace. It has been consistent with his administration's multilateral and multistakeholder approach to cyber diplomacy in the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security and the OEWG, with the Secretariat of Foreign Affairs constructively participating in both processes. Mexico has been a keen advocate of the multistakeholder approach to cyber governance, welcoming the participation in cyber diplomacy of the country's nongovernmental actors from civil society, academia, and the private sector.[36] At the UN level, Mexico has played an active role in the negotiations on the cyber crime treaty,[37] suggesting amendments to the draft text and attempting to mediate between conflicting parties.[38]

Mexico is also an observer to the Council of Europe's Convention on Cybercrime (the Budapest Convention) and has reportedly used it as an exemplar when incorporating cyber crime in its penal code and National Security Law.[39] It has, however, refused to sign the Budapest Convention—a decision generally attributed to concerns over its implications for national sovereignty and the burden of implementation. This concern has also been evident in Mexico's statements during the UN cyber crime treaty committee meetings.[40]

The USMCA, which replaced the North American Free Trade Agreement, was signed the day before AMLO took office in December 2018. His administration has overseen the implementation of the agreement, which came into force in 2020. The agreement addresses cybersecurity and includes a detailed and ambitious chapter on developing and integrating digital markets in North America and creating the conditions necessary for digital trade to thrive. For example, it prohibits potential barriers to trade (such as the imposition of customs duties on digital transactions) and ensures that data can be transferred across borders, including personal data. The USMCA also seeks to create a free, open, peaceful, secure, and reliable cyber ecosystem in North America by protecting consumer rights online and by requiring Canada, Mexico, and the United States to invest in their cybersecurity response capabilities, to strengthen their collaboration in identifying and countering malicious cyber threats and in adopting a risk-based approach to addressing these, and to cooperate among themselves and internationally to promote the development of digital trade.[41] According to the Office of the United States Trade Representative, the USMCA "contains the strongest disciplines on digital trade of any international agreement"[42] and lays the foundation for North America to become a world leader in the digital economy.

In October 2021, Mexico was among the countries that the United States brought together to discuss the global security threat posed by ransomware and that established the Counter Ransomware Initiative (CRI).[43] State participation in the CRI has grown year on year, and the CRI held annual meetings in 2022 and 2023. The CRI aims to combat ransomware by: building resilience, developing effective relationships between the public and private sectors and across civil society, deepening interstate cooperation aimed at disrupting attacks (such as sharing intelligence and conducting joint cyber training exercises), pursuing malicious actors and holding them responsible, preventing the financing of such actors, and recovering illicit gains acquired.[44] At its 2022 meeting, the CRI established the International Counter Ransomware Task Force to develop tools to counter attacks, share intelligence, and exchange best practices.[45] And at its 2023 meeting, the CRI focused on "developing capabilities to disrupt attackers and the infrastructure they use to conduct their attacks, improving cybersecurity through sharing information, and fighting back against ransomware actors."[46]

In August 2022, Mexico and the United States established a Working Group on Cyber Issues to advance bilateral cooperation on cybersecurity and to promote their "shared commitment to an open, interoperable, secure, and reliable internet and a stable cyberspace."[47] During the group's first meeting, the two sides committed themselves to improving coordination among bilateral cooperation initiatives focused on cybersecurity, to strengthening technical coordination mechanisms for addressing cyber threats, to exchanging cyber threat intelligence for investigating cyber crimes, to continuing bilateral cyber training initiatives, and to engaging in multilateral and multistakeholder cybersecurity processes.[48] The United States and Mexico stated that "cyber issues have become a priority" in their bilateral relationship and the group will build on their existing collaboration on cybersecurity, such as the inclusion of cybersecurity in the High-Level Security Dialogue and High-Level Economic Dialogue.

Mexico supports the norms of responsible state behavior in cyberspace and, more broadly, the application of international law and human rights in cyberspace—consistent with its foreign policy agenda that highlights the importance of the rule of law and protecting human rights.[49] Yet, unlike many other states, including those in Latin America such as Brazil and Costa Rica, it has not published a national statement setting out how international law applies to cyberspace, notwithstanding the fact that the 2021 UN Group of Governmental Experts invited states to contribute such statements to a compendium accompanying its final report.

Mexico's cyber diplomacy is consistent with its positions on matters of peace, international security, sovereignty and nonintervention, and the importance of technology in international development. In this respect, there has been much continuity with the foreign policies of AMLO's predecessors.[50] This is unsurprising, given the relatively technocratic nature of cyber diplomacy and in light of the structural and strategic factors that have long shaped Mexico's foreign policy.[51] At the same time, this consistent line in cyber diplomacy has been somewhat undermined by a long-running capacity constraint on Mexico's wider diplomacy, which has been worsened under AMLO. The Secretariat of Foreign Affairs' limited budget and the need to focus resources on the Mexico-United States bilateral relationship and consular issues for Mexican citizens in the United States limits the ability to pursue a more global agenda.[52] Thus there are severe constraints on what the country can hope to accomplish, absent greater prioritization and resources, neither of which appears imminent or likely.

Mexico recognizes the importance to itself of efforts to address digital exclusion and to use technology to drive economic development. It has benefited from bilateral and regional capacity building,[53] including through the OAS, which assisted in the development of the ENCS.[54] It has also benefited from private-sector capacity building, such as Microsoft's creation of a Cybersecurity Engagement Centre in the country in 2017.[55] Microsoft also extended its TechSpark engagement program to Mexico, the only country other than the United States to benefit from it.[56] This is just one example of how Mexico benefits from its uniquely close economic relationship with the United States.

Prospects for External Engagement

Mexico is the second-largest trading partner of the United States, and there are over forty million U.S. citizens of Mexican heritage living there.[57] Their relationship extends from trade to security, and includes cross-border challenges—most significantly the trafficking of illegal arms and narcotics, and the migration crisis—that can only be solved by working together.[58] Cybersecurity is one such challenge, reflected in their Working Group on Cyber Issues. However, not least given the difficulties in relations at present,[59] there are opportunities for other states to provide practical assistance in cyber capacity building in different areas.

Donors and providers of assistance need to coordinate among themselves and to deconflict their efforts, but this would be easier if the government addressed Mexico's cyber capacity-building requirements in a more coordinated and well-structured manner. Assistance also need not be limited to the federal government, and there could be more engagement with individual Mexican states or sectors after identifying where governmental, corporate, and wider nongovernmental assistance can be most effectively used. That Mexico's national policy is not yet comprehensively integrated is not a reason for external actors to delay or dismiss opportunities to engage with different institutional actors at the federal, state, or even city levels. In doing so, they should draw on the emerging body of global knowledge about which capacity-building interventions are most successful. They should also commission research into the applicability of wider lessons for effective capacity-building interventions in Mexico. Wherever possible, formal evaluation of lessons learned should be a feature of their interventions.[60]

National strategic coordination and weakness in education and skills could be two areas for the United States and other external actors to target for cooperation. There are already private-sector initiatives, such as Microsoft's abovementioned efforts.[61] Their effectiveness should be studied, with the findings disseminated and widely used to shape future interventions.[62] The U.S. government has strong experience in institutionalization and education/ training initiatives, as well as a vibrant cybersecurity system (including corporate and nonprofit actors) that can contribute to developing a whole-of-society approach to capacity building in Mexico. But context is key and interventions need to be tailored to the country's requirements and constraints. Effective collaboration and partnership between donors, providers, and recipients is also crucial.[63]

Conclusion

AMLO's term in office has been a missed opportunity to continue the progress made under previous administrations. Instead of fully implementing the ENCS, cyber policy has stalled. The timing has been particularly unfortunate given the recent global wave of cyber crime, which has badly hit Mexico.

Cyber-related incidents, such as the Guacamaya revelations, have been downplayed, rather than used as an opportunity to kick-start progress. Moreover, recent allegations about the use of commercial spyware in ways that would seem to violate human rights underline the relatively weak mechanisms of accountability and oversight regarding the defense and security forces. The combination of these important drawbacks and Mexico's relatively constructive role in global cyber diplomacy suggests there is a "say/do gap" between domestic practice and statements about responsible state behavior in cyberspace globally.

Mexico's cybersecurity challenges are real and not easy to fix. The challenge of doing so is exacerbated by the fact that the country must address other significant security threats, most notably the strength of organized crime. But the ENCS still offers a plausible starting point for what needs to be done. The new president who will be elected in 2024 will need to press the reset button on cyber policy. The next administration should re-prioritize an actively led, coordinated national approach that pursues further institutionalization and invests effectively in improving education, skills, and the national cybersecurity culture and system. The United States and other external actors—state and nonstate—will continue to have roles to play in supporting such efforts.

About the Authors

Joe Devanny is lecturer in the Department of War Studies at King's College London. He was a 2022–2023 British Academy Innovation Fellow at the U.K. Foreign, Commonwealth and Development Office. He writes here in a personal capacity. Follow him on X (Twitter): @josephdevanny.

Russell Buchan is professor of international law at the University of Reading. He was a 2022–2023 British Academy Innovation Fellow at the UK Foreign, Commonwealth and Development Office. He writes here in a personal capacity. Follow him on X (Twitter): @russellbuchan.

Notes

[1] Government of Mexico, *Estrategia Nacional de Ciberseguridad (ENCS)*, https://intranet.inaes.gob.mx/pdf/CiberSeguridad/Estrategia_Nacional_Ciberseguridad.pdf.

[2] Marco A. Mares, "Ciberseguridad, ¿en el olvido?," *El Economista*, May 9, 2023, https://www.eleconomista.com.mx/opinion/Ciberseguridad-en-el-olvido-20230509-0133.html.

[3] Jeffrey E. Zinsmeister, "A Call to Action: Strengthening Judicial Cybersecurity Across the Americas to Protect the Rule of Law," Global Americans, November 17, 2023, https://theglobalamericans.org/2023/11/a-call-to-action-strengthening-judicial-cybersecurity-across-the-americas-to-protect-the-rule-of-law/.

[4] Natalie Kitroeff and Ronen Bergman, "How Mexico Became the Biggest User of the World's Most Notorious Spy Tool," *New York Times*, April 18, 2023, https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html#:~:text=A percent20New percent20York percent20Times percent20investigation,the percent20world percent27s percent20most percent20infamous percent20spyware.

[5] "Massive Leak of Military Docs Reveals Mexico Armed Cartels, Surveiled Journalists and Zapatistas," Democracy Now!, October 12, 2022, https://www.democracynow.org/2022/10/12/mexico_military_drug_cartels_ayotzinapa_ministry.

[6] As this paper explains, the national strategy has not been a pathway to inevitable success. For the Peña Nieto administration's mixed record of improving cybersecurity, see: Eduardo Guerrero, "Towards a Transformation of Mexico's Security Strategy," *The RUSI Journal* 158 (2013), 6-12: https://www.tandfonline.com/doi/pdf/10.1080/03071847.2013.807579; Carlos Solar, "Cybersecurity and cyber defence in the emerging democracies," *Journal of Cyber Policy* 5 (2020), 392-412: https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1820546; Carolyn Gallaher, "Mexico, the Failed State Debate, and the Mérida Fix," *The Geographical Journal* 182 (2016), 331–41: https://rgs-ibg.onlinelibrary.wiley.com/doi/abs/10.1111/geoj.12166; and Eric Farnsworth, "Mexican Standoff," *The National Interest* 146 (November/December 2016), 61-67: https://www.jstor.org/stable/26557352.

[7] Brazil is a recent case of a country drawing explicitly from the United Kingdom's example in drafting a cyber policy. See Joe Devanny and Russell Buchan, "Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress Is Possible," Carnegie Endowment for International Peace, August 8, 2023, 5-6, https://carnegieendowment.org/files/Devanny_Buchan_Brazil_Cyber.pdf.

8 Saul Mauricio Rodriguez-Hernandez and Nicolas Velasquez, “Mexico and cybersecurity: policies, challenges, and concerns” in *Routledge Companion to Global Cyber-Security Strategy*, ed. Scott N. Romaniuk and Mary Manjikian (Abingdon: Routledge, 2021), 489.

9 Juan Manuel Aguilar Antonio, “Panorama de nacional de ciberdelitos: ¿qué sabemos al respecto en México?,” *Praxis Legal* (2022), 67: https://www.academia.edu/77712787/Panorama_de_nacional_de_ciberdelitos_qué_sabemos_al_respecto

10 Overview of the Mexican Economy, https://embamex.sre.gob.mx/filipinas/index.php/negocios-y-comercio/overviewmexicaneconomy.

11 https://datareportal.com/reports/digital-2024-mexi-co#:~:text=There%20were%20107.3%20million%20internet%20users%20in%20Mexico%20in%20January,January%202023%20and%20January%202024; Chafic Nassif, “Ericsson Signs Collaborative Alliance With Mexico’s Federal Telecommunications Institute,” Ericsson (April 25, 2023), https://www.ericsson.com/en/blog/4/2023/ericsson-signs-collaborative-alliance-with-mexicos-federal-telecommunications-institute.

12 Juan Carlos Garcia Caparros, “Top Cyber Threats to Latin America and the Caribbean,” *Mandiant*, 24 May 24, 2021, https://www.mandiant.com/resources/blog/top-cyber-threats-to-latin-america-and-the-caribbean

13 International Telecommunications Union, *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity*, 2020: 25: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

14 Belfer Centre, *National Cyber Power Index 2022*, September 2022, https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf.

15 Alex Crowther, “The 5x5: The state of cybersecurity in Latin America,” Atlantic Council, December 9, 2021, https://www.atlanticcouncil.org/commentary/the-5x5-the-state-of-cybersecurity-in-latin-america/

16 The five dimensions of the Oxford model are a way of conceptualizing the problem areas to be addressed: cybersecurity policy and strategy; cybersecurity culture and society; building cybersecurity knowledge and capabilities; legal and regulatory frameworks; and standards and technology. If enacted and implemented successfully, the draft bill could improve Mexico’s performance across these dimensions, but the evidence of AMLO’s term suggests that strong presidential buy-in is essential for progress, even if a good framework exists on paper. See “The CMM,” *Global Cybersecurity Capacity Centre*, https://gcscc.ox.ac.uk/the-cmm.

17 http://gaceta.diputados.gob.mx/PDF/65/2023/abr/20230425-II-2.pdf.

18 Ana Luisa Gutiérrez, “Las propuestas de ley de ciberseguridad buscan vulnerar derechos,” *Expansion*, November 16, 2023, https://expansion.mx/tecnologia/2023/11/16/propuestas-de-ley-ciberseguridad-buscan-vulnerar-derechos.

19 Cristal Bautista, “Diferencias sectoriales frenan ley de ciberseguridad en México,” *Milenio*, August 12, 2023, https://www.milenio.com/negocios/diferencias-sectoriales-frenan-ley-ciberseguridad-mexico.; “The pros and cons of Mexico’s cybersecurity bill,” BnAmericas, September 7, 2023, https://www.bnamericas.com/en/news/the-pros-and-cons-of-mexicos-cybersecurity-bill; Melisa Osores, “Las leyes de ciberseguridad son importantes, pero tienen que aplicarse,” *Computer Weekly*, October 19, 2023, https://www.computerweekly.com/es/noticias/366556340/Las-leyes-de-ciberseguridad-son-importantes-pero-tienen-que-aplicarse.

20 Jose Soto Galindo, “Los Peligros de la Ley de Ciberseguridad,” *El Economista*, March 3, 2024, https://www.eleconomista.com.mx/opinion/Los-peligros-de-la-ley-de-ciberseguridad-20240303-0014.html; Surya Palacios, “Morena quiere militarizar el ciberespacio,” *AltoNivel*, March 6, 2024, https://www.altonivel.com.mx/actualidad/morena-quiere-militarizar-el-ciberespacio/

21 Luisa Parraguez, “Quo Vadis? Mexico’s National Cybersecurity Strategy,” Wilson Center, May 2018, 19, https://www.wilsoncenter.org/sites/default/files/media/documents/publication/quo_vadis_mexicos_cybersecurity_strategy.pdf.

22 See Parraguez, *Quo Vadis?*, 11-14. See also: Government of Mexico, *Estrategia Nacional de Ciberseguridad*, https://intranet.inaes.gob.mx/pdf/CiberSeguridad/Estrategia_Nacional_Ciberseguridad.pdf.

23 Juan Manuel Aguilar Antonio, ‘Panorama de nacional de ciberdelitos.”

[24] Saul Mauricio Rodriguez-Hernandez and Nicolas Velasquez, "Mexico and cybersecurity: policies, challenges, and concerns," in *Routledge Companion to Global Cyber-Security Strategy*, ed. Scott N. Romaniuk and Mary Manjikian (Abingdon: Routledge, 2021), 489.

[25] According to the *New York Times*, Mexico is "the most prolific user of the world's most infamous spyware." Natalie Kitroeff and Ronen Bergman, "How Mexico Became the Biggest User of the World's Most Notorious Spy Tool," *New York Times*, April 18, 2023, https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html.

[26] National Guard Computer Emergency Response Team-Mexico (Guardia Nacional CERT-MX), "Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos," June 19, 2023, https://www.gob.mx/gncertmx/articulos/protocolo-283239.

[27] Government of Mexico, "Alista SSPC Registro Nacional de Incidentes Cibernéticos," December 6, 2021, https://www.gob.mx/sspc/prensa/alista-sspc-registro-nacional-de-incidentes-ciberneticos.

[28] Government of Mexico, *Estrategia Digital Nacional 2021-2022*, https://sidof.segob.gob.mx/notas/5628886.

[29] Rodrigo Riquelme, "Cámara de Diputados turna a comisiones iniciativa de ley de ciberseguridad," *El Economista*, June 7, 2023, https://www.eleconomista.com.mx/tecnologia/Camara-de-Diputados-turna-a-comisiones-iniciativa-de-ley-de-ciberseguridad-20230607-0045.html.

[30] Government of Mexico, "MARINA se fortalece en materia de Seguridad en el Ciberespacio, al recibir la Secretaría Pro-Tempore del Foro Iberoamericano de Ciberdefensa," January 14, 2021, https://www.gob.mx/semar/prensa/marina-se-fortalece-en-materia-de-seguridad-en-el-ciberespacio-al-recibir-la-secretaria-pro-tempore-del-foro-iberoamericano-de-ciberdefensa.

[31] Ryan C. Berg and Henry Ziemer, "The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment," Center for Strategic and International Studies, November 19, 2021, https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment.

[32] Carlos Solar, *Cybersecurity Governance in Latin America: States, Threats, And Alliances* (Albany, NY: State University of New York Press, 2023).

[33] Denise Dresser, "Mexico's Dying Democracy: AMLO and the Toll of Authoritarian Populism," *Foreign Affairs*, November 1, 2022, https://www.foreignaffairs.com/mexico/mexico-dying-democracy-amlo-toll-authoritarian-populism-denise-dresser

[34] Belisario Contreras and Kerry-Anne Barrett, "Challenges in Building Regional Capacities in Cybersecurity: A regional organisational reflection," in *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen (Abingdon: Routledge, 2020), 214-217.

[35] Greg Weeks, "AMLO's cautious foreign policy," *Global Americans*, February 15, 2019, https://theglobalamericans.org/2019/02/amlos-cautious-foreign-policy/; Olga Pellicer, "Why Mexico Is a Quiet Presence on the World Stage," *Americas Quarterly*, April 25, 2023, https://www.americasquarterly.org/article/why-mexico-is-a-quiet-presence-on-the-world-stage/.

[36] Government of Mexico, 'Contribution of the Government of Mexico for consideration by the Ad Hoc Committee at its second substantive session."

[37] Katitza Rodriguez and Meri Baghdasaryan, "UN Committee To Begin Negotiating New Cybercrime Treaty Amid Disagreement Among States Over Its Scope," Electronic Frontier Foundation, February 15, 2022, https://www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among

[38] Elements of the Government of Mexico for the United Nations ad hoc Committee to elaborate a comprehensive international Convention on countering the use of information and communications technologies for criminal purposes, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/MEX-Initial_Position_to_UN_Cybercrime_Convention.pdf.

[39] Bruna Martins dos Santos, "Budapest Convention on Cybercrime in Latin America: A brief analysis of adherence and implementation in Argentina, Brazil, Chile, Colombia and Mexico," Derechos Digitales, 2022, https://www.derechosdigitales.org/wp-content/uploads/ENG-Ciberdelincuencia-2022.pdf

40 See Government of Mexico, "Contribution of the Government of Mexico for consideration by the Ad Hoc Committee at its second substantive session," UN Office on Drugs and Crime, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Mexico_Contribution.pdf.

41 "The USMCA and Digital Trade in North America," Brookings, February 24, 2022, https://www.brookings.edu/articles/usmca-forward-building-a-more-competitive-inclusive-and-sustainable-north-american-economy-digital/.

42 "United States-Mexico-Canada Modernizing NAFTA into a 21st Century Trade Agreement," https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing.

43 "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021," White House, October 14, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

44 "The Second International Counter Ransomware Initiative Summit," White House, November 1, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/.

45 "The Second International Counter Ransomware Initiative Summit". See also "Global Task Force to Fight Ransomware Commences Operations," Australian Government, Department of Home Affairs, January 23, 2023, https://www.homeaffairs.gov.au/news-media/archive/article?itemId=1013.

46 "International Counter Ransomware Initiative 2023 Joint Statement," White House, November 1, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/.

47 US Department of State, "Joint Statement on U.S.-Mexico Working Group on Cyber Issues," August 18, 2022, https://www.state.gov/joint-statement-on-u-s-mexico-working-group-on-cyber-issues/.

48 Ibid.

49 Pablo Arrocha Olabuenaga and Juan Ramón de la Fuente, "Mexico's Priorities as an Elected Member to the Security Council for 2021-2022," *Just Security*, July 7, 2020, https://www.justsecurity.org/71241/mexicos-priorities-as-an-elected-member-to-the-security-council-for-2021-2022/.

50 Hernán F. Gómez Bruera, "To be or not to be: Has Mexico got what it takes to be an emerging power?," *South African Journal of International Affairs 22* (2015) 227-248: https://www.tandfonline.com/doi/abs/10.1080/10220461.2015.1053978.

51 For deeper insight into the longer-term challenges for and trends in Mexico's foreign policy and diplomacy, see Ingrid Berlanga Vasile, "Challenges of Contemporary Diplomacy for Mexico," *The Fletcher Forum of World Affairs* 43 (2019), 63–81: https://www.jstor.org/stable/45289828; Günther Maihold, "Mexico: A Leader in Search of like-Minded Peers," *International Journal* 71 (2016), 545–62: https://journals.sagepub.com/doi/abs/10.1177/0020702016687336; and Ana Covarrubias and Jorge A. Schiavon, "In Search of International Influence: Mexico as an Entrepreneurial Power," *International Journal* 73 (2018), 535–53: https://journals.sagepub.com/doi/10.1177/0020702018811901.

52 Jorge A. Schiavon and Bruno Figueroa, "Foreign Policy Capacities, State Foreign Services, and International Influence: Brazil versus Mexico," *Diplomacy & Statecraft* 30 (2019), 816-828: https://www.tandfonline.com/doi/full/10.1080/09592296.2019.1673560.

53 The Cybil Portal, curated by the Global Forum on Cyber Expertise, lists twenty-two such cyber capacity-building projects in Mexico, making the country one of the largest recipients of such assistance in Latin America. See https://cybilportal.org. See also the UN Institute for Disarmament Research (UNIDIR) Cyber Policy Portal, https://cyberpolicyportal.org/states/mexico.

54 For an overview of the OAS's role in supporting the development of national cybersecurity strategies in Latin America see: Organisation of American States and Global Partners Digital, *National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions* (2022), https://www.oas.org/en/sms/cicte/docs/National-Cybersecurity-Strategies-Lessons-learned-and-reflections-ENG.pdf.

[55] "Microsoft opens cybersecurity center to protect Mexicans," Microsoft, February 24, 2017, https://news.microsoft.com/2017/02/24/microsoft-opens-cybersecurity-center-to-protect-mexicans/.

[56] The Microsoft TechSpark Program, https://www.microsoft.com/en-us/corporate-responsibility/techspark.

[57] Office of the United States Trade Representative, "Countries & Regions" (no date), https://ustr.gov/countries-regions; U.S. Department of State, "200th Anniversary of U.S.-Mexico Bilateral Relations," December 12, 2022, https://www.state.gov/200th-anniversary-of-u-s-mexico-bilateral-relations/.

[58] U.S. Department of State, "Remarks at the U.S.-Mexico High-Level Security Dialogue," October 13, 2022, https://www.state.gov/remarks-at-the-u-s-mexico-high-level-security-dialogue/.

[59] Duncan Wood and Alexandra Helfgott, "Seeking Process and Predictability: An Evaluation of U.S.-Mexico Relations Under President Biden," Wilson Center, January 24, 2022, https://www.wilsoncenter.org/article/seeking-process-and-predictability-evaluation-us-mexico-relations-under-president-biden; Natalie Kitroeff and Michael D. Shear, "After Rocky Start, Biden Builds Rapport With Mexico's President," *New York Times*, January 23, 2023, https://www.nytimes.com/2023/01/10/world/americas/biden-amlo-mexico-relationship.html.

[60] There is evidence of emerging professionalisation and reflective practice in cyber capacity-building over the last decade, but much work remains to be done in developing an evidence base for understanding the factors behind effective interventions. See: Patryk Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy," *Global Policy* 7 (2016), 83-92: https://onlinelibrary.wiley.com/doi/abs/10.1111/1758-5899.12298; Rob Collett and Nayia Barmpaliou, "International Cyber Capacity Building: Global Trends and Scenarios," Luxembourg: EU Institute for Security Studies, 2021. https://en-cyber.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/all-units/RCRL/Copies%20References%20Documents/international%20cyber%20capacity%20building-QN0121158ENN.pdf; Belisario Contreras and Kerry-Anne Barrett, "Challenges in Building Regional Capacities in Cybersecurity: A regional organisational reflection," in *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen (Abingdon: Routledge, 2020), 214-217; Anthony J. S. Craig, Richard A. I. Johnson, Max Gallop, "Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies," *Journal of Cyber Policy* (2023), 1-24: https://www.tandfonline.com/doi/abs/10.1080/23738871.2023.2178318; and Sadie Creese, William H. Dutton, Patricia Esteve-González, "The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions," *Personal and Ubiquitous Computing* 25 (2021), 941-955: https://pubmed.ncbi.nlm.nih.gov/33994905/.

[61] "Microsoft opens cybersecurity center to protect Mexicans," Microsoft, February 24, 2017, https://news.microsoft.com/2017/02/24/microsoft-opens-cybersecurity-center-to-protect-mexicans/; Kate Behncken, "Closing the cybersecurity skills gap—Microsoft expands efforts to 23 countries," Microsoft, March 23, 2022, https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/.

[62] There is an increasing literature on what makes for effective capacity building interventions in different sectors. See: Tim Maurer and Arthur Nelson, "International Strategy to Better Protect the Financial System Against Cyber Threats," Carnegie Endowment for International Peace, November 18, 2020, 127-139: https://carnegie-production-assets.s3.amazonaws.com/static/files/Maurer_Nelson_FinCyber_final1.pdf.

[63] On 'collaborative transformation' through cyber capacity building, see: Cesar Moline Rodriguez and Carlos Leonardo Garcia, "Cyber Capacity Building Collaborative Transformation: Good practice from the Dominican Republic," EU CyberNet, February 3, 2022, https://www.eucybernet.eu/publication/cyber-capacity-building-collaborative-transformation-good-practice-from-the-dominican-republic-1/.

Carnegie Endowment for International Peace

In a complex, changing, and increasingly contested world, the Carnegie Endowment generates strategic ideas, supports diplomacy, and trains the next generation of international scholar-practitioners to help countries and institutions take on the most difficult global problems and advance peace. With a global network of more than 170 scholars across twenty countries, Carnegie is renowned for its independent analysis of major global problems and understanding of regional contexts.

Technology and International Affairs Program

The Technology and International Affairs Program develops insights to address the governance challenges and large-scale risks of new technologies. Our experts identify actionable best practices and incentives for industry and government leaders on artificial intelligence, cyber threats, cloud security, countering influence operations, reducing the risk of biotechnologies, and ensuring global digital inclusion.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org