NOVEMBER 2021

The Development of the ICT Landscape in Mexico

Cybersecurity and Opportunities for Investment

Ryan C. Berg and Henry Ziemer

Executive Summary

Mexico's information and communications technology (ICT) sector has witnessed increased competition and investment since 2013's landmark regulatory reform, which created the Federal Institute of Telecommunications (IFT). However, to an extent under President Enrique Peña Nieto and especially since President Andrés Manuel López Obrador was inaugurated in 2018, the direction of the ICT sector has become heavily contested. The Mexican government has failed to create a national digital strategy or a clear roadmap for ICT public policy while at the same time constraining the IFT's regulatory agenda. This paper examines the current state of Mexico's ICT sector. First, the "Competitive North America" section assesses how to improve technological innovation, expand internet access, and promote competition. Second, the "Secure North America" section highlights how to improve cybersecurity within the region as digitalization increases.

In the "Competitive North America" section, this paper focuses on regulation of supply chains, innovation, and technology. Free trade agreements such as the North American Free Trade Agreement (NAFTA) and its successor, the United States-Mexico-Canada Agreement (USMCA), have contributed to Mexico's economic success and helped it become the United States' second-largest trade partner. However, the Covid-19 pandemic has drastically slowed Mexico's economic growth while also catalyzing the country's transition to a more digital world, economy, and workplace. This has elevated concerns over new ICT rollout and regulation. With several extra-hemispheric telecommunications suppliers increasingly eager to enter the Latin American market, strengthening supply chains and economic ties within the Western Hemisphere has become even more crucial.

One key obstacle to better regulation is the current López Obrador administration, which has actively pursued a strategy of weakening non-executive regulatory agencies, including the IFT. Besides implementing budget cuts to these agencies, President López Obrador has not replaced IFT commissioners who leave or retire. The Mexican Senate has little power to remedy the issue, as they only can approve candidates presented by the president, who has yet to submit any replacements for these positions.

Mexico's ICT future depends on growth in several key areas: physical capital, human capital, and technological innovation. The first, physical capital, involves addressing the critical issue of connecting people to the internet. There were **92.01 million** internet users in Mexico in January 2021 (71 percent of the population) but millions more remain without affordable or stable internet access. Second is human capital, which includes training workers in cybersecurity and promoting a broader digital mindset within companies. Third, to compete in an ever-more digital economy, Mexico needs technological innovation to grow and scale initiatives in cloud computing and data, especially in academia and the private sector. Future policies and strategies for Mexican ICT regulation must be data-driven if they are to bring about a more competitive North America.

The second section of this paper, "Secure North America," evaluates the current state of security and cybersecurity in Mexico's ICT sector and highlights the opportunities available to address these issues. Even as the sector becomes more competitive, Mexico's cybersecurity infrastructure and practices are simply not modern enough to ensure it is robust and secure. As it stands, Mexico's domestic criminal organizations and cartels are taking advantage of the inadequate cybersecurity infrastructure to further their illicit operations, simultaneously facilitating the entrance of foreign hackers into the Mexican ICT industry. Recently the perpetrators of a high-profile ATM hack were subsequently linked to both Venezuelan criminal enterprises and the Romanian mafia. Creating a strong ICT sector with well-developed cybersecurity infrastructure will not only benefit Mexico and its citizens, but it could also prove to be a crucial component of the relationship between the United States and Mexico and of North America's wellbeing and security.

The inclusion of a digital trade chapter with cybersecurity provisions in USMCA, as well as the U.S. Department of Defense's current cybersecurity cooperation with Mexico's Ministry of National Defense (SEDENA) and Navy (SEMAR), are two positive steps for the growth of cybersecurity policy in the region. However, the Mexican government's fiscal austerity and lack of a national digital agenda have inevitably downgraded cybersecurity to a national-level issue. Furthermore, Mexico's long-standing failure to prioritize digital skills within formal education makes it difficult to equip citizens or companies with the tools they need to prevent cyberattacks. As a result, individuals are more vulnerable to cyberattacks and companies are reluctant to adopt digital operations; only **48 percent** of Mexican companies believe that digital transformation is their top priority, even as the country continues to digitalize rapidly. As these current trends demonstrate, opportunities for innovation in cybersecurity are plentiful. This paper analyzes how partnerships between the public sector, private sector, and academia will be critical to creating a more secure North America.

Introduction

As Mexico continues to digitalize, strong development of its ICT sector will be crucial to its success. Partly due to the establishment of the IFT in 2013, Mexico has the **most advanced** telecommunications regulation in Latin America, according to the International Telecommunications Union's regulatory tracker.

However, even as the pandemic accelerated the pace of digital transformation, the government of Mexico has failed to create a national digital strategy or a clear roadmap for ICT public policy. Digital transformation, and the challenges and opportunities it entails, has not been a priority for the López Obrador government. Its focus on the sector is largely limited to the Internet para Todos ("Internet for All") program, which seeks to improve connectivity in rural areas; meanwhile, other necessary elements of a national digital strategy have been neglected. Moreover, the administration's budget cuts have obstructed ongoing digitalization and cybersecurity efforts that might have otherwise continued to expand.

Even though improvements to the competitiveness and security of the Mexican ICT sector are both necessary and in the overall best interest of the Mexican people, López Obrador's policies and his attempt to centralize regulatory oversight under his control are undermining private regulators. His administration has constrained the IFT, which has struggled to modify its inaugural 2013 agenda. From 2018 to 2019, the IFT's budget fell from 2 to 1.5 billion pesos ($73 million), hovering around the latter figure ever since. Overall the agency's budget has decreased by about 41.1 percent in real terms since 2014.

In this context, this paper will assess the ICT supply chain in North America and the investment climate in Mexico. It will then examine how this issue affects the development of secure digital connections in North America. Given the Mexican government's recent attempts to exert increased federal control over the ICT sector and transfer government resources to the López Obrador administration's preferred departments, it will also suggest next steps to improve technological innovation, expand internet access, promote competition, and improve security in Mexico. Lastly, it will offer policy recommendations for the Mexican government to foment a more attractive environment for foreign investors in the ICT sector and to engage a range of stakeholders including the United States and Canada on strengthening cybersecurity measures.

Part I: Competitive North America

THE IMPORTANCE OF SUPPLY CHAINS, INNOVATION, AND TECHNOLOGY

Increasing the competitiveness of Mexican supply chains, joint production platforms, and technology is crucial both from a U.S. foreign-policy perspective and from a domestic standpoint within Mexico, where more digitalization will lead to further economic development for its citizens. Mexico's rapid digitalization efforts are exemplified by a threefold increase in mobile-broadband internet penetration between 2013 and 2018.

Mexico has benefited from three decades of economic integration with the United States and Canada through NAFTA and now USMCA. Free trade, combined with Mexico's geographical proximity and the rapid growth of its ICT sector over the past decade, has made Mexico a vital link in the North American regional economy. Today, Mexico is the second-largest trade partner of the United States and receives 12 percent of total U.S. export sales of telecommunications goods, making it the United States' second-largest export destination (after Hong Kong) in this category. Whereas the success of NAFTA lay in the manufacturing sector in general and the automotive industry in particular, the future success of the USMCA will be digital.

However, the ongoing Covid-19 pandemic has sent tremors through Mexico's economy, resulting in an 8.5 percent contraction in GDP in 2020. The government's policy of austerity meant that Mexico spent little to keep suffering businesses afloat during the pandemic, causing an estimated one million small- and medium-sized businesses to close their doors. The pandemic also reinforced the importance of digital growth and internet access even as it led to a slowdown of investment into Mexico's ICT sector. Despite the large percentage of Mexicans who continue to work in person (and informally), the accelerated shift toward virtual work, learning, and commerce since March 2020 means that Mexico's digital economy will be a critical part of the country's medium- to long-term economic growth.

Whereas the success of NAFTA lay in the manufacturing sector in general and the automotive industry in particular, the future success of the USMCA will be digital.

Currently, the Mexican telecommunications landscape is dominated by América Móvil and its subsidiaries. The company has a 62 percent market share in terms of wireless internet lines, and its market cap is roughly 13 times higher than the next largest Mexican competitor, Megacable Holdings. While key reforms in 2013 and 2014 improved the competitiveness of Mexico's ICT sector, América Móvil has not seen a significant reduction in its control of the market even though new companies have emerged and expanded their operations.

Another major development has been the expansion of Chinese companies into Mexico's ICT sector. While Mexico remains one of the lowest recipients of Chinese investment in Latin America, telecom giant Huawei has made several overtures to both the Peña Nieto and López Obrador governments. In 2014, for instance, Huawei concluded a $1.5 billion deal to construct ICT infrastructure in the state of Queretaro. Following the 2018 elections, President López Obrador signaled a greater openness to investment from non-U.S. carriers, especially Chinese-backed enterprises. Huawei's global campaign during this period prompted the Trump administration to launch its Clean Network initiative to combat Beijing's aggressive intrusions on citizens' privacy and companies' most sensitive information.

The Clean Network initiative consists of six main objectives: clean carrier, clean store, clean apps, clean cloud, clean cable, and a clean 5G path. Broadly, the initiative underscores the importance of strengthening supply-chain security and economic ties in the digital realm. While over 50 countries joined the Clean Network, it made little headway in Latin America, where just three countries signed on, two of which later backed out. For its part, Mexico has never been part of the Clean Network, although U.S. skepticism toward Chinese ICT providers has led the country to try to confine their operations to southern Mexico, away from the U.S. border. However, the nature of digital infrastructure means it is difficult to enforce such limitations in practice, prompting renewed dialogues within the Biden-Harris administration over how to better secure Mexico's ICT supply chains.

MEXICO'S REGULATORY AGENCY: THE FEDERAL INSTITUTE OF TELECOMMUNICATIONS

The IFT became Mexico's regulatory agency in the ICT sector after the 2013 reforms, enacted during the Peña Nieto administration. This reform replaced Cofetel, which was facing a wide range of constraints as Mexico's telecommunications regulatory agency. These constraints included the politically motivated selection of commissioners, a lack of autonomy from the executive branch, a lack of legal authority to regulate the entire sector, weak sanctioning authority, and weak implementation of regulatory rules. It is ironic that Cofetel's replacement, the IFT, now suffers similar constraints under the López Obrador administration.

Under its current structure, the IFT is an independent agency, both financially and legally under the Mexican constitution. Commissioners are selected through a three-step process designed to maximize appointees' technical knowledge and abilities. First, a technical evaluation committee works with universities to select three to five candidates and sends this list to the president. The president chooses one, who is then proposed to the Senate for confirmation.

Since its creation in 2013, the IFT has helped reduce market concentration, benefiting the consumer population and creating a competitive ICT environment in Mexico. It has done so through several

important reforms, especially regarding antitrust regulations. The IFT can declare firms either preponderant in a particular sector or "with substantial market power" in the provision of a particular service, then issue regulations that apply only to those firms. For instance, the agency mandated that América Móvil and multimedia giant Televisa allow all telecom firms operating in Mexico to negotiate agreements for use of their infrastructure. Furthermore, if the firms could not agree on a price for such access, the IFT was empowered to step in and set one itself. In 2018, the IFT also found América Móvil in violation of antitrust laws and slapped the company with a $5.4 million fine.

Mexico's regulatory push has made strides in improving customer-service standards and promoting foreign investment in Mexican telecommunications. In 2015, the IFT forced telephone companies to stop charging long-distance rates for any calls within Mexico and enhanced contract protections for customers, particularly by preventing phone contracts from being modified without notification and requiring that customers be compensated for outages or erroneous charges. The same legislation that established the IFT also took heed of international recommendations to allow fully foreign-owned firms to operate in the Mexican telephone and internet industries, opening the country up to a wide range of new investment opportunities.

Despite the success of the IFT's regulation efforts since 2013, the López Obrador administration has undermined the independent body since taking office in December 2018. First, he claims that the agency is not truly autonomous, but rather serves the agenda of "neoliberal" elite interests, a critique he has leveled against other regulatory bodies. Next, he claims that the commissioners have too high a salary. In Mexico, there is a popular perception that government officials earn more money than they should; López Obrador seeks to counter this image by cutting the salaries of top public servants such as those in the IFT. He has publicly supported the idea of bringing the independent agency under the umbrella of the Ministry of Communications and Transportation to cut costs.

As it stands, the López Obrador administration could deal a fatal blow to the independence of the IFT in two ways. First, continued budget cuts to the agency would easily undermine the agency's mandate. Second, President López Obrador could continue not replacing the IFT commissioners that are leaving until there are not enough commissioners left to form an operating regulatory body. Currently, the IFT has only four of seven commissioners; by March 2023, only three will remain. For its operations to continue uninterrupted—which requires having at least four commissioners—the López Obrador administration must present candidates to the Senate for approval, which currently seems unlikely.

CURRENT TRENDS IN THE MEXICAN ICT SECTOR

Today Mexico sits at a crossroads when it comes to the future of ICT. The country is caught between an increasingly online population eager to unlock the benefits of digital transformations and a suite of institutional barricades that hamper desperately needed progress. Covid-19 has exacerbated both trends, making digital work and commerce more attractive while simultaneously slowing the pace of investment into Mexico's ICT sector. Nevertheless, Mexico could significantly benefit from growing internet and telecommunications access, with one report from the AlphaBeta consultancy group estimating that a new digital strategy could lead the Mexican economy to grow by $316 billion by 2030.

Today Mexico sits at a crossroads when it comes to the future of ICT. The country is caught between an increasingly online population eager to unlock the benefits of digital transformations and a suite of institutional barricades that hamper desperately needed progress.

Mexico as a whole has embraced the importance of internet access for all its citizens. As of January 2021, there were more than 92 million internet users in Mexico, representing about 71 percent of the population.

This number has risen by 4 percent since 2020 and is a significant jump from just 43.5 percent of the population with internet access in 2013. President López Obrador's ambitious Internet para Todos campaign pledged to deliver online connections to 100 percent of Mexicans by the year 2023. His goals are shared by major companies such as Facebook and Google, which have donated to help build free public Wi-Fi sites throughout the country. However, significant hurdles remain in rural areas, where nearly 20 percent of Mexico's population lives and where internet and mobile penetration is significantly lower.

Throughout 2020 and beyond, pandemic-related lockdowns created newfound demand for e-commerce in Mexico and the Western Hemisphere more broadly. According to one analysis, queries for online shopping in Mexico grew by 37 percent, a trend in keeping with an overall rise in e-commerce throughout Latin America. Retailers have recognized that this trend is likely to persist even as government-mandated lockdowns cease. The Argentinian firm MercadoLibre has already announced plans to invest $1.1 billion in increasing warehouse and workforce capacity within Mexico to meet this growing demand for online shopping options. Such investments are likely just the beginning, as more companies begin to recognize the untapped potential of digitally integrated warehouse-to-doorstep services.

However, the pandemic and ensuing global economic crisis have also slowed down investments in the ICT sector. Foreign direct investment in Mexico dropped by 15 percent between 2019 and 2020, and the country fell six places in the World Bank's Doing Business rankings over concerns surrounding fiscal austerity and GDP contractions. Low levels of investment have also contributed to rising prices, which have rendered telecommunications products and services outside the budget range of many customers, further hampering efforts to extend access throughout the country. The lack of a robust regulatory framework compounds these issues, and without a strategy for identifying and encouraging investment in crucial sectors, Mexico's digital economy will be seriously limited in its growth potential.

A more pervasive and long-standing challenge for ICT in Mexico is the influence of monopolistic entities that obstruct needed reforms. Companies in this sector, especially América Móvil, have traditionally exercised considerable regulatory and procurement leverage, not only by making campaign contributions to elected officials but also by placing loyalists in ICT-related cabinet positions. Thus, while the IFT has made strides toward breaking down monopolistic practices, the cost to entry for many smaller firms remains unsustainably high in the face of deeply entrenched and well-connected actors.

Additionally, corruption within government procurement in the ICT sector at the federal, state, and municipal levels continues to be a barrier for U.S. firms in Mexico. According to the Organization for Economic Cooperation and Development, Mexico has struggled to implement anti-bribery measures, especially regarding bribes paid by foreign companies. Firms not bound by the U.S. Foreign Corrupt Practices Act do not need to be as scrupulous, giving them a market-entry advantage. This dimension is especially important when it comes to Chinese corporations, some of the United States' main competitors in the Mexican ICT space.

Embedded monopolies and endemic corruption have combined to produce a worrying trend of ICT business failures. In 2020, Grupo Telefónica, a Spanish multinational corporation, announced it would leave the Mexican telecommunications market. In June 2021, Altan Redes, a major Mexican telecom company, filed for bankruptcy. The exit of these companies increases the dominance of América Móvil over the Mexican ICT sector and slows the development of infrastructure needed to make internet and mobile services accessible to more users. These challenges mirror the dilemma regulators have faced since 2013: how to choose between levying special telecom taxes that decrease demand, issuing high-spectrum rights that reduce the cost of goods sold, and eliminating state and municipal roadblocks to infrastructure development.

DETERRENTS TO MEXICO BECOMING A DIGITAL SPRINTER

One of the most glaring impediments to Mexico's digital growth is the lack of a national digital strategy. The López Obrador administration is the first in decades not to issue a public policy strategy for ICT. This makes it difficult for public regulators such as the IFT, as well as relevant government ministries, to harmonize their efforts with that of private-sector actors. Strategic confusion in turn leads to counterproductive or overlapping policies, which further complicate efforts to grow the ICT sector sustainably.

Mexico has also introduced large budget cuts to the ICT sector as part of López Obrador's push to cut out digital actors entirely. The president has repeatedly floated combining the IFT with other regulatory bodies, namely the Institute for Access to Information (INAI) and Federal Commission for Economic Competition (COFECE). He has framed these proposals as a cost-saving measure and insists that personnel will remain employed by the new agency after restructuring. However, his desire to downsize will inevitably reduce know-how regarding cybersecurity and tech transformation within the government, and many professional offices have already been terminated.

Mexico also has no policy to improve education and literacy on fundamental ICT subjects. Such measures are vital for ensuring that Mexico's future workforce possesses the tools and skills to function in an increasingly digital environment. This is driven in part by unequal access to the internet in schools, a divide exacerbated by the pandemic. Yet the federal administration has not issued any public policies to resolve the gap in schools' digital connectivity or the education system's insufficient training in digital skills.

The lack of high-level leadership and strategizing on ICT is one of the primary obstacles to Mexico's digital development. Without strong commitments from the López Obrador administration, it will be difficult to create the market conditions to see the key investments in infrastructure and human capital Mexico needs to fully capitalize on its growing internet-using population.

OPPORTUNITIES FOR POLICY DEVELOPMENTS

Mexico's ICT future depends on the formation of a wide coalition of public and private actors with energetic leadership from the government. The current administration can take the lead by drafting a national digital strategy. A useful framework for outlining this strategy comes from Google's 2020 report on "digital sprinters," which identifies the three pillars of physical capital, human capital, and technological innovation as essential for countries to make the most of ICT opportunities.

Physical capital, a fundamental necessity for connecting people to the internet, can be promoted by encouraging greater foreign investment in Mexico's ICT sector. President López Obrador should view his Internet para Todos program as highly compatible with private-sector firms. Human capital includes promoting worker training in cybersecurity and enacting policies to enforce proper digital hygiene within companies. Finally, policymakers should recognize that future technological innovation will be driven by advances in growing and scaling up initiatives in cloud computing and data. Encouraging a competitive, market-driven environment within Mexico will be instrumental to supporting innovation in these areas, as will expanded government support for students pursuing technical careers in the country.

One underutilized resource in Mexico's ICT sector is academia, including technical education centers. There are numerous higher-education establishments, such as the Mexico Autonomous Institute of Technology (ITAM) and National Polytechnic Institute of Mexico, that would make strong partners in this respect. Not only are universities incubators for future technical and engineering leaders, they also possess a wealth of knowledge the government can turn to when developing sound policy. For instance, Mexico's National Institute of Statistics and Geography collects extensive data on the use of internet

and telecommunications, which would help both the government and educational institutions design better policies for improving access. A national strategy for ICT should therefore recognize that the list of relevant actors extends beyond government agencies and corporations to educators and students. Including academia in such a strategy will mean Mexico can better utilize all the resources at its disposal to accelerate its digital transformation.

Much of the value to be created in both Mexico and North America will be the result of changes in the digital and information technology sphere. Mexico has the tools at its disposal to harness these trends, but using them to their full effect will require sufficient willpower. Bolstering, rather than undermining, the IFT—and engaging with actors across the public-private spectrum—will pay dividends down the line through increased competitiveness and expanded internet access for Mexican society.

Part II: Secure North America

THE IMPORTANCE OF CYBERSECURITY IN MEXICO'S ICT SECTOR

Although the digital sector provides new avenues for economic growth, these opportunities come with their own risks. Given the level of risk it faces, Mexico does not possess the cybersecurity infrastructure and practices that are necessary for a secure and robust ICT sector. In the first quarter of 2020, the country suffered an estimated 800 million attempted cyberattacks, making it the fourth-largest cybercrime target in the Western Hemisphere, after the United States, Canada, and Brazil. Meanwhile, the cost of cybercrime and cyber fraud to the Mexican economy has been reported to be as high as $7.7 billion a year.

Moreover, the lack of a cybersecurity paradigm in Mexico creates challenges for regional efforts to protect critical infrastructure and joint interests. Integrated electrical grids, which are expanding across the U.S.-Mexico border, are especially vulnerable targets. Meanwhile election tampering by hostile actors using digital methods has been reported throughout North America. As cyberspace grows in importance as an area for geopolitical competition, regional dialogues and coordinated policy will become essential for Mexico to protect its critical infrastructure.

The growing importance of digital tools for everyday life in Mexico will likely only exacerbate these threats. For instance, 91 percent of cyber fraud is related to e-commerce, with the rise in mobile banking presenting a lucrative target for hackers. Thus, as Mexico continues to expand internet access, the threats from malicious actors will multiply accordingly, especially in the absence of a nationwide campaign to address digital security issues.

> *Given the level of risk it faces, Mexico does not possess the cybersecurity infrastructure and practices that are necessary for a secure and robust ICT sector.*

Mexico, to its credit, adopted a National Cybersecurity Strategy in 2017. Based on the principles of human rights, risk management, and multidisciplinary cooperation, it was ambitious in scope. However, this framework has been criticized for its failure to suggest actionable steps for centralizing the government's response to cyber threats—and the change in government in 2018 did not help. President López Obrador has been decidedly less focused on cyber issues than his predecessor, delaying putting the national strategy into practice. For instance, Mexico currently has no dedicated cybersecurity agency like the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Cybercrime investigations are typically entrusted to the Scientific Division of the National Guard (formerly of the Federal Police), specifically the Center of

Expertise in Technological Response (CERT-MX). Yet the interagency nature of such attacks demands a whole-of-government approach, which Mexico has been slow to adopt.

Insecurity in the digital realm will pose an increasingly difficult challenge for Mexican ICT companies, especially when it comes to obtaining foreign partnerships. Outside investors will be reluctant to consider Mexico a reliable partner if companies remain vulnerable to hacks. The same can be said for government actors, who will be reluctant to share secret or potentially compromising information with their Mexican counterparts unless they adopt stricter cybersecurity measures. Creating a strong ICT sector with well-developed cybersecurity infrastructure is therefore vital to the bilateral relationship between the United States and Mexico, as well as broader North American interests in securing critical infrastructure.

CURRENT CYBERSECURITY TRENDS

Mexico's cybersecurity progress is marked by five main developments. Some, especially in the realm of cooperation with the United States, are cause for optimism; others illustrate the major obstacles that Mexico still needs to surmount. At a glance, the five developments are the inclusion of a "digital trade" chapter in USMCA, increased U.S.-Mexico cybersecurity cooperation, the prioritization of fiscal austerity over digital transformation, attempts to address data-privacy issues, and the continued lack of a digital mindset.

1. USMCA's Digital Trade Chapter

The USMCA is one of the most forward-thinking multilateral trade agreements in terms of ICT provisions. Most notably, the agreement contains a chapter specifically pertaining to the digital economy, including how to encourage safe digital trade between the member countries. This chapter introduced provisions for digital intellectual-property protection, as well as bans on customs duties for digital goods. Crucially, the agreement took a firm stance against data localization, a form of digital protectionism that requires foreign companies to store data collected from a country within physical infrastructure inside that country. These provisions help lay the groundwork for combating financial crimes and upholding copyright protections in cyberspace.

Article 19.15 of the digital trade chapter deals specifically with cybersecurity. This section calls on the signatories to bolster their national defenses against cyber threats and to increase bilateral and trilateral coordination on cybersecurity. Furthermore, Article 19.8 introduces obligations to protect the personal information of users, issuing a set of recommendations modeled on the Asia-Pacific Economic Cooperation (APEC) privacy framework. These provisions include data minimization and security policies, as well as a requirement that individuals be notified promptly of a personal data breach and be given appropriate means for redress within their country of residence. Combined, these articles help the region set an agenda to secure cross-border data flows against malicious actors.

These provisions promise to make the signatory countries much more attractive destinations for ICT-sector investment. Better safeguards on both intellectual property and liability protections will help companies become more resilient in the face of cyberattacks. Furthermore, by baking cybersecurity into its framework, USMCA sets a precedent for future coordination between parties on other cyber issues.

2. U.S.-Mexico Cybersecurity Cooperation

Increased security cooperation between the United States and Mexico can be mutually beneficial to common and North America-wide cybersecurity infrastructure and practices. This is already a priority in the U.S. defense establishment, which has increasingly focused on cybersecurity as a major national-security priority. The Department of Defense (DOD) has also made developing Mexico's cybersecurity capacity a strategic priority, working with the Mexican Ministries of National Defense (SEDENA) and the Navy (SEMAR).

Although the bulk of Mexico's cybersecurity focus is currently centered within the National Guard, this military-to-military cooperation is essential to strengthening Mexico's national-defense capacity.

The connection between cybersecurity and more conventional national-security issues has sharpened in recent years as criminal groups in Mexico have expanded into the digital sphere. In one prominent case, the Bandidos Revolution Team targeted Mexican banks and ATMs, stealing between $2.5 and $5 million a month throughout 2018. Members of this group had ties to criminal enterprises stretching from Venezuela to Romania. Cartels have also integrated dark-web communications networks and cryptocurrencies into their trafficking operations as nearly untraceable methods for acquiring synthetic drug precursors and selling them in the United States. Finally, a recent report by the Wilson Center identified major weaknesses in Mexico's ability to protect critical infrastructure from cyberattacks. This includes state oil giant Pemex, which suffered a serious ransomware attack in 2019, as well as the National Electoral Institute, which was the target of nearly three million cyberattacks in 2018. As Mexico's critical digital infrastructure becomes more integrated with the rest of North America, its weak cyber defenses could threaten the region as a whole.

Current work by the DOD and Mexican military in the country's ICT space focuses on protecting information networks and systems for domain awareness and control. Overall security cooperation between the two countries, while whittled down during the Peña Nieto administration, has particularly suffered over the past three years of the López Obrador administration, and Mexico's relatively low national cyber-defense capacity has meant cooperation remains limited. Nevertheless, there are signs of a renewed dialogue, and U.S. secretary of defense Lloyd Austin has so far been proactive in reaching out to counterparts at SEDENA and SEMAR. The United States will nevertheless need to proceed with caution on DOD-headed initiatives, as President López Obrador has indicated his opposition to an overly militarized relationship with the United States.

Future moves should be carefully calibrated to help rebuild a sense of trust between the two countries and ensure that Mexico views cybersecurity cooperation as a mutually beneficial issue that fits into a larger geostrategic framework for North America as well. For example, the U.S. Department of Homeland Security and CISA could open talks with Mexico about creating a national cyber-defense agency. While budgetary and bureaucratic constraints under the López Obrador administration pose significant challenges, pushing for the creation of such an agency would be a worthwhile allocation of U.S. efforts, however unlikely the agency is to come to fruition. Both organizations could draw on their extensive backgrounds in countering cyber threats to help the new Mexican agency start on the right footing. CISA in particular has produced several documents—such as its Supply Chain Risks Analysis and Framework for Resiliency Against Threats—to help ICT-sector organizations in the United States better understand the risks and vulnerabilities of cyber threats. A new Mexican government agency focused on these challenges could produce similar items for domestic companies. Alternatively, CISA could cooperate with existing agencies such as CERT-MX to help protect ICT networks across North America.

3. Fiscal Austerity and Digital Transformation

While USMCA and certain defense-sector developments look promising for the development of a budding U.S.-Mexico cybersecurity paradigm, the Mexican government has largely deprioritized the issue in policymaking. President López Obrador's commitment to fiscal austerity is hampering investment flows into necessary cybersecurity infrastructure and tools for technological transformation. As mentioned above, budget cuts to the IFT are already eliminating entire digital profiles. This includes professional offices such as the undersecretary of communications, who was responsible for coordinating satellite

systems and the national Red Compartida ("shared network") 4G project. President López Obrador's proposed merger of three regulatory agencies will likely erode available ICT expertise even further.

Contrary to the government's claims that cutting positions will produce a leaner, more efficient government, removing experienced ICT personnel will expose Mexico to additional cyber threats. Secure digital infrastructure relies upon having experienced workers who are conscious of possible vulnerabilities and able to provide advice to other branches of government. The potential merger also signals to foreign investors that there is little high-level commitment to USMCA's cybersecurity provisions, undermining the boost in confidence the agreement created. Decreased funding for digital transformation will in turn have long-term implications for Mexico's cybersecurity, as it may delay vital security updates to ICT infrastructure, creating more opportunities for cybercriminals.

4. The Data-Privacy and Cybersecurity Gap

Mexico's efforts to legislate new digital protections have also struggled to balance individual rights and security interests. Indeed, the Peña Nieto administration was criticized for its use of spyware to monitor journalists, civil society members, and opposition leaders. In an attempt to increase data security against cyber threats, Mexico passed an amendment to the Federal Telecommunications and Broadcasting Law in April 2021. This amendment ordered telecommunications carriers, such as América Móvil and AT&T, to collect customers' biometric, fingerprint, and personal data and file it with the IFT, effectively creating a national registry of mobile telephone users. While the bill was intended to curb kidnapping and telephone extortion, it has been criticized for violating the privacy rights of Mexican citizens; this led the bill to be passed narrowly, with 54 votes in favor, 49 against, and 10 abstentions.

While critics rightly point out the bill's personal-privacy implications, another significant obstacle is the cost of the registry's infrastructure and operations. Indeed, this has been the main reason the law is currently falling short of its original intentions. Mexico faces a tradeoff in operating such an extensive and sensitive database. If it prioritizes low operating costs—or is forced to by budgetary restrictions—it will likely compromise on security measures, potentially leading to major security breaches by the criminal enterprises the bill sought to curtail. Indeed, this was the same rationale behind the repeal of Mexico's former National Registry of Telecommunications Users in 2011 after hackers listed its content on the black market.

However, good security does not necessarily mean the registry will be put to good use either. Officials may point to the need to protect data from bad actors to justify limiting transparency, thus allowing a massive government data collection program to run with few checks from other branches or civil society. This would surely breach international and domestic standards of proportionality and accountability when it comes to collecting citizens' personal information. In the process, the registry would merely shift from being a target for criminal exploitation to an avenue for governmental abuse.

Other relevant cybersecurity and data protection laws have also fallen short. For instance, while the Federal Law on the Protection of Personal Data Held by Private Parties states that data processors must immediately report data breaches, this requirement is not properly enforced, and organizations often do not comply. Companies believe that reporting a breach will be seen as an indication that they are less secure than their competitors. This reaction also belies the need for improved corporate and workforce outreach regarding cybersecurity issues.

Finally, Mexico's struggle to promote digital literacy at all educational levels is rapidly creating new vulnerabilities. While Mexico's National Cybersecurity Strategy notes a "culture of cybersecurity" as one of its objectives, there appears to have been little outreach to relevant ministries—such as those

of education or labor—to devise a policy to promote this. Advancing public knowledge of safe internet practices is essential for Mexico to scale its cybersecurity response to meet growing levels of online crime and fraud. The majority of cyberattacks in Mexico are not highly sophisticated and can be prevented with effective digital hygiene. Without training in this area, however, Mexican citizens are liable to fall victim to phishing, simple malware, digital identity theft, and other forms of cybercrime.

5. Lack of a Digital Mindset

Mexico's struggle to educate citizens on cyber threats speaks to a deeper challenge in convincing Mexican companies—particularly small and medium-sized enterprises (SMEs)—to adopt a fully digital mindset. Put differently, Mexican private-sector companies by and large continue to view ICT as only one aspect of their work, rather than a vehicle for transforming workforce dynamics. Without this digital mindset, a large percentage of Mexican SMEs continue to neglect cybersecurity.

This failure to appreciate digital transformation can be seen in the walling off of digital expertise in many companies. For instance, when asked about digital issues, many Mexican executives will refer the question to their chief information officer (CIO). While that position certainly should possess specialized knowledge of ICT issues, broader concerns about cybercrime, fraud, and digital intellectual property theft should not be the purview of a company's CIO or IT department alone.

Failure to adopt a digital mindset can have damaging effects on the competitiveness of SMEs. Mid-sized companies often struggle to increase sales via e-commerce because they do not focus on improving cybersecurity infrastructure or trust in their digital platforms. In Mexico, 14.3 percent of online purchases are not completed because the consumer is suspicious of fraud, economically impacting the SMEs providing these services and locking out a crucial category of businesses from one of Mexico's most rapidly growing sectors.

Given the dire straits in which many SMEs have found themselves as a result of the pandemic, digital vulnerabilities compound their troubles. By not devoting infrastructure and human capital to cybersecurity now, these firms will find it even harder to digitize in the future.

OPPORTUNITIES FOR CYBERSECURITY INNOVATION

The cybersecurity challenges faced by Mexico's public and private sector are deeply embedded. Yet the forecast is not entirely bleak, and calibrated policy responses can have an outsized impact in raising awareness of cyber threats and taking actionable steps toward mitigating them. Such policies will pay dividends in the form of reduced loss through theft, espionage, and damage to digital infrastructure.

First, Mexico should immediately expand digital training and cybersecurity education. Cybersecurity games and tools for children can help foster online safety and start creating healthy digital citizens from an early age. For instance, picoCTF, a competition run by Carnegie Mellon University, presents students with a set of cybersecurity challenges to work through in their specific country environment. Launching these initiatives early sets up a pipeline of cybersecurity know-how and talent. Early education on digital issues should be paired with a reinvigorated effort to encourage workforce training about safe online practices. These training sessions can also help workers develop new digital skills, which will help them compete in a rapidly digitizing economy.

Partnerships with academia can also be reestablished to bring in a wider array of expertise. Before 2013, the National Association of Universities and Institutions of Higher Education (ANUIES) had organized a National Computer Security Network (RENASEC). This network was responsible for collating information

on cyber threats and running diagnostic studies of the vulnerabilities university internet systems faced. The national network has since been disbanded, fragmenting into a series of less effective regional partnerships between institutions. However, in 2017 ANUIES formed a specialized ICT committee to centralize discussion on cybersecurity issues. Because universities pose lucrative targets for cyber criminals—owing to the sensitivity of the data they possess on students, faculty, and their finances—ANUIES is understandably eager to strengthen universities' cyber defenses. The association's experience in operating RENASEC could also allow it to share expertise with the Mexican government and private sector.

Mexico should also continue advancing its Program for the Development of the Software Industry (PROSOFT). This initiative promotes the creation of industrial innovation centers that provide training, develop human capital, and encourage the adoption of new technologies for digital security. Such innovation is crucial for Mexico—not only to better protect against new forms of cyber threats, but also to further its progress toward becoming a digital sprinter. Given President López Obrador's revitalization of PROSOFT in 2019, there is an opportunity to use this existing program to ensure that resources are dedicated to increasing digitalization efforts in line with new cybersecurity infrastructure and practices.

Finally, Mexico can consult the accumulated knowledge of other countries and international organizations. Especially in developing ICT supply chains, relevant frameworks from the International Standards Organization (ISO) can provide valuable guidance. For instance, ISO 28000 and 28001 outline the critical requirements for supply-chain security and how to fully implement these protections. Meanwhile, ISO/IEC 16085 describes how to safely manage the life cycle of software given that aging systems present increased security risks. Policymakers can consult these documents to gain a common understanding of what benchmarks and indicators are important for ICT supply-chain security. In turn, having shared standards helps coordinate efforts across government agencies as well as with other countries, especially key trade partners such as the United States and Canada.

POLICY RECOMMENDATIONS

Much of the world's economic growth over the next decade, and certainly North America's, will be driven by innovations in the digital and ICT sectors. To realize its full potential, Mexico needs to recognize this trend and act quickly to encourage digital advancements and business integration. At the moment, Mexico's approach to its digital sector is somewhat haphazard. Promising developments—including greater internet connectivity, a modern digital trade agreement, and a competent autonomous regulator—are running up against disunity within the government. The lack of a comprehensive national digital strategy, coupled with pandemic-induced stimulus austerity and economic shocks, has put Mexico on the back foot regarding digital transformation and cybersecurity in particular. Thus, even as the government in Mexico City pushes to make internet accessible to all citizens, it has ignored broader structural challenges that prevent individuals and companies from making the most of new digital opportunities.

Three main courses of action will allow Mexico to make the most of its digital future. The first should be developing and disseminating a new national digital strategy. Although Mexico possessed one from 2013 to 2018, the López Obrador administration has yet to produce its own document on the subject. An updated strategy could be centered around an expanded vision of Internet para Todos, one that recognizes the need for public-private partnerships and more secure digital connections. Such a document would help present a holistic view of Mexico's challenges and opportunities in the ICT sector.

Another important reform would be the creation of Mexico's own, standalone, civilian-run cybersecurity agency. This move would put the country on more solid ground for combating the diverse nature of cyber threats, which range from criminal to terroristic to hostile nation in nature. Rather than assigning the

bulk of cyberattack investigations to a subsection of a single division of the National Guard, having an independent agency could more effectively draw on resources from across a range of government and private actors. Furthermore, it could take a more proactive stance, as CISA in the United States has already, in developing recommendations and guidelines about cybersecurity. Finally, this agency would open new opportunities for collaboration with its North American counterparts, who could lend their expertise to ensure the agency is able to ramp up quickly after being established.

Finally, Mexico will need to consciously engage private and civil-society actors to speed the pace of its digital transformation. Greater dynamism and foreign investment will play a key role in making digital connections more accessible. Meanwhile, academia could provide invaluable partners to help officials understand the economic and security implications of the ICT sector. While such partnerships should be given ample space in any national digital strategy, Mexico can also work toward these goals in the short term. In the private sector, Mexico could offer targeted assistance to small and mid-sized ICT companies as it begins its slow economic recovery from the Covid-19 pandemic. Although such measures will be difficult given President López Obrador's penchant for fiscal austerity, the digital sector is likely to lead the way in post-pandemic growth, meaning early support can serve as an impetus for future investment. Among universities, CERT-MX or a new cybersecurity agency could sponsor hackathons to tackle different types of cyber threats and establish partnerships with academic and research institutions. If the government can enlist broader swathes of Mexican society in its efforts, it will likely find many untapped or underutilized resources to accelerate the digital transformation.

Finally, Mexico will need to consciously engage private and civil-society actors to speed the pace of its digital transformation. Greater dynamism and foreign investment will play a key role in making digital connections more accessible.

Conclusion

Accessible, reliable, and secure internet connections are crucial to the lives and livelihoods of millions of Mexican citizens. These developments mirror a global trend wherein the ICT sector has become increasingly relevant not just for macroeconomic projections but also for daily life. However, Mexico should recognize that sound digital policy cannot be achieved with an atomized approach. It requires far-reaching cooperation with allies, private entities, various government agencies, and more. It is therefore essential for Mexico to adopt a more strategic outlook to capitalize on its progress in the ICT realm. ■

Ryan C. Berg *is a senior fellow with the Americas Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Henry Ziemer*** *is an intern with the CSIS Americas Program.*

This report is made possible by general support to CSIS.