MEXICO

Digital Threat Landscape: Civil Society & Media

Internews
Local voices. Global change.

SOCIALTIC
Digital technology for social change

Table of Contents

Background

In the world of digital security, Mexico has made a name for itself as the most prolific and one of the first reported customers of the Pegasus spyware, with civil society and media being a prime target. While Pegasus often makes the news, Mexican civil society and media organizations face less sophisticated digital attacks on multiple fronts. This report was prepared by Internews' Internet Freedom & Resilience team under a stream of work which strengthens civil society organizations (CSOs), journalists, and other human rights defenders (HRD) ability to detect, analyze, and build resilience to digital attacks through localized expertise in threat analysis and incident response. This report is intended to provide an overview of the digital threats faced by civil society and media organizations in Mexico and guidance for digital safety experts supporting this community. It is also intended to provide context for the cybersecurity industry which may need to analyze security incidents affecting Mexican civil society and media. We conclude with a discussion of mitigation measures that can be proposed by digital security experts to the organizations with whom they work, as well as for civil society and media organizations to implement.

This report was written in close collaboration with SocialTIC, a non-profit organization dedicated to research, training, support, and promotion of digital technology and information for social purposes. SocialTIC exists to securely empower change actors in Latin America by strengthening their analysis, social communication, and advocacy actions through the strategic use of digital technologies and data.

The threats, trends, and case studies highlighted in this report were identified through direct digital safety support for at-risk communities (provided by Internews and SocialTIC), desk research, and conversations with trusted members of the Internet Freedom community. This report aggregates data from incident response work and documents attack patterns specific to Mexico.

October 2023

Written and Edited: Martijn Grooten, Ashley Fowler, Marc Shaffer, and Skyler Sallick
Copyediting, Design, and Layout: Skyler Sallick

Digital Threat Landscape

Political Context, Civil Society, and the Media

The current government of Mexico under President Andrés Manuel López Obrador (often referred to as AMLO) is accused of undermining democracy and cracking down on media freedom and civil society. AMLO has stigmatized journalists in the press and bullies media outlets that go against official government narratives. Journalists face significant threats to their physical security, mostly from organized crime networks who work in collaboration with government officials. Almost 150 journalists have been murdered in Mexico since 2000, four of which occurred in 2023. Reporters Without Borders ranks Mexico 128th out of the 180 countries included in their press freedom index, which analyzes the political, economic, legislative, social, and security context of journalism in a country. Reporters Without Borders emphasizes that the physical threats in Mexico are among the highest in the world.[1] The struggles experienced by journalists are particularly severe for women and other marginalized communities as they often experience greater mental impacts and face more aggressive threats that take on a more personal nature.[2]

Although Mexican civil society remains active, they face significant hurdles to operate freely. AMLO's administration has not followed through on campaign promises to support human rights.[3] The administration is often in conflict with civil society; disregarding criticism and insulting opponents. In March 2022, legislators from MORENA, the ruling party, introduced a law that would "prohibit non-profit organizations from trying to influence or change laws either through lobbying or through strategic litigation if they receive funding, directly or indirectly, from foreign governments or corporations."[4] Amnesty International argues that there will be a chilling effect on civil society's ability to criticize the government if this law goes into effect. Similar laws exist in Nicaragua and Guatemala, and although El Salvador attempted to follow suit with its "foreign agent" law, human rights groups were successful in opposing the law's passage.[5]

Mexico's military has continued to gain power while remaining the least transparent arm of the government.

Mexico's military has continued to gain power while remaining the least transparent arm of the government. Notably, AMLO's administration transferred control of Mexico's civilian-led National Guard to the military in 2022. In 2021, the military took control of the development of and all future profits from the "Tren Maya," one of AMLO's signature development projects. The project intends to connect popular tourist destinations on the Yucatan coast such as Cancun and Tulum with the peninsula's interior and Caribbean coast via train. Many environmental and indigenous rights groups oppose the construction of this train as it has already caused damage to the Yucatan's ecosystem and historical sites. Rights groups have additionally accused the government of failing to gain public buy in and criticize the government transparency of the project. By transferring control of the project to the military, the administration further strengthens the armed forces while validating transparency concerns.[6]

Members of civil society, including those opposed to the removal of civilian control of the National Guard and the military takeover of the Tren Maya project, face violent retaliation from the military and organized criminal groups. The government has been accused of failing to investigate criminal abuses carried out by members of the armed forces. With a sense of impunity, criminals will target human rights advocates, often to the point where activists require physical security.[7]

Although the country has significantly improved the legislative rights of the LGBTQIA+ community, Mexico remains the country with the second highest rate of LGBTQIA+ related hate crimes in the region.

Mexico is home to several vulnerable communities that face discrimination and violence. Although antidiscrimination laws are in place, indigenous peoples and Afro-Mexicans remain underrepresented.[8] 77% of indigenous Mexicans live below the poverty line and states with higher proportions of indigenous peoples generally receive fewer resources and services.[9] Mexico's LGBTQIA+ community face a "progress paradox." Although the country has significantly improved the legislative rights of the LGBTQIA+ community, Mexico remains the country with the second highest rate of LGBTQIA+ related hate crimes in the region.[10] On paper, Mexico is a regional leader with respect to the LGBTQIA+ community. In practice, the country fails to protect the community's legislative rights and physical security.[11]

Cybersecurity in Mexico

Mexico has experienced significantly higher rates of malicious cyber activity in the past decade. The country has not avoided the recent global surge in the use of ransomware by cybercriminals, with threat actors deploying various families of banking malware to target users. Prominent targets of such cyberattacks include the oil provider Pemex and a local factory of the manufacturing giant Foxconn.[12]

While the Pemex and Foxconn attacks were opportunistic, organized cybercriminals are also active in the country. A group referred to by the security company Mandiant as "FIN13" conducted a more targeted financial campaign in the country.[13] Active since roughly 2016, "FIN13" focuses particularly on Mexico and targets large organizations in the financial, retail, and hospitality sectors through the use of off-the-shelf and custom-made malware. In addition, a recent publication by the security company SentinelOne reports that the kingpin of a global cybercrime operation targeting users of Spanish and Chilean banks resides in Mexico.[14]

A group of Romanian ATM skimmers has also been active in the country. According to local media reports, the group receives legal protection for their financially motivated cybercrimes from a top anti-corruption official in the country's Attorney General's office.[15]

In response to the prevalence of cybercrime, the Mexican government published a new "Ley de Ciberseguridad" (Cybersecurity Law) on April 25th, 2023 – their first attempt at a comprehensive law of this kind. The law contains four central approaches to cybersecurity: defending the digital space to safeguard national security, creating a new legal framework to address cyberattacks, annual penetration testing of public and private institutions, and the creation of an Agencia Nacional de Ciberseguridad (National Cybersecurity Agency). The National Cybersecurity

Agency will be controlled by Mexico's executive branch and is modeled on similar agencies in the European Union, United States, and Brazil.[16]

Human rights activists have intensely criticized the new law. Article19 México y Centroamérica, the local section of an international human rights organization focused on promoting free expression and freedom of information, has raised several concerns. Firstly, they note that the law militarizes cybersecurity by treating the defense of digital space as a national security issue.[17] Experts in Mexico's private sector agree that the law focuses too narrowly on cybersecurity as a national security matter without considering the reach of the issue across all aspects of life. There is concern that positioning cybersecurity under a national security framework could create legal cover for the widespread surveillance of digital activity in Mexico.[18] This narrow focus on cybersecurity as a national security issue provides avenues for the abuse of civil rights. Additionally, the types and definitions of cybercrime included in the law have the potential to criminalize legitimate conduct or make criminal activity overly difficult to prosecute. As an example, Article19 suggests that the criminalization of content that incites hostility can serve as justification for a crackdown on free expression. Article19 also notes that the law is poorly drafted, making implementation difficult while failing to address the abuses carried out by the Mexican government. [19]

The State of Cybersecurity of Civil Society and Media

Mexican civil society and media organizations currently face some of the most significant cybersecurity threats in the world. These organizations must not only combat standard financially motivated cyberattacks, but the Mexican government is currently the most prodigious user of advanced spyware software in the world.

NSO Group's Pegasus spyware has been used in Mexico against a wide range of targets including lawyers for the families of murdered women, journalists investigating criminal cartels, and the wife of a journalist killed by cartels.

Mexico is a target of the anonymous "Guacamaya" activist hacker, or hacktivist, group that has been active in various Latin American countries since the beginning of 2022. These hacks aren't merely relevant for their cyber activity, but also by what they revealed. In the case of Mexico, the "Guacamaya" hacktivist group revealed links between the military and criminal organizations, as well as the military's use of Pegasus spyware to target journalists, human rights defenders, and government officials.[20]

The use of Pegasus by Mexican officials is not new. The very first public report on the now notorious spyware was published in 2016 and named Mexican journalist Rafael Cabrera as one of the targets.[21] Since then, NSO Group's Pegasus spyware has been used in Mexico against a wide range of targets including lawyers for the families of murdered women, [22] journalists investigating criminal cartels,[23] and the wife of a journalist killed by cartels.[24] Of the 50,000 phone numbers uncovered in a 2021 investigation by Forbidden Stories and Amnesty International about potential phones targeted by Pegasus, about 15,000 were Mexican phone numbers – more than any other country.[25]

The initial findings of spyware use in Mexico led civil society organizations such as SocialTIC, R3D, and Article19 to withdraw from a spyware working group in 2017 at the Open Government Partnership, a multilateral organization promoting government transparency and reform. In their withdrawal, these CSOs cited a lack of trust in the Mexican government given its use of spyware. Following AMLO's election in early 2019, these organizations re-joined the working group based on his campaign promise of respect for human rights. However, allegations of ongoing Pegasus use by the government and the military have added additional complications.

In addition to Pegasus, Mexican civil society and media organizations have faced the use of Hacking Team,[26] Finfisher,[27] and QuaDream[28] spyware. Some media outlets and civil society organizations now perceive the prevalence of surveillance technology as the biggest threat to their work. Another prevalent risk is the frequency with which hacking results in the theft of personal and institutional accounts and the loss of information.

The pervasive use of spyware by Mexican authorities has an important effect on civil society and media organizations: the perception of being spied upon, even when that may not be the case. This fear pervades all aspects of their lives. Due to the fear of surveillance, unexplained events on accounts and devices such as lagging connectivity speeds or frequent device restarts cause these individuals to fear that spyware may have infected their device – increasing paranoia and stress when the explanation may be more mundane. Additionally, many members of civil society and the media face online harassment from those with opposing views. This harassment can involve 'doxing', the publication of personal information, which can lead to threats of physical violence and/or death. Women and gender minorities are a particular target of such harassment.

> ***Due to the fear of surveillance, unexplained events on accounts and devices such as lagging connectivity speeds or frequent device restarts cause these individuals to fear that spyware may have infected their device – increasing paranoia and stress when the explanation may be more mundane.***

The threats to civil society and the media in Mexico are significant, and these organizations require support from the cybersecurity community to ensure they can continue to carry out their necessary work.

Mitigation Measures

Account security is important for anyone in Mexico, but crucial for members of civil society in particular. **Two-factor authentication is a must** — and mitigates the use of weak and/or reused passwords. Though better than no two-factor authentication at all, SMS shouldn't be considered secure enough, especially for at risk users, as there is some evidence of SMS being intercepted through corrupt or hackable telecoms providers. Using an authentication app is better than SMS, and using a hardware token generally provides the best security, although this requires additional equipment.

Some messaging apps such as Telegram, WhatsApp, and Signal, require the use of a phone number to activate the account. Enabling two-factor authentication involves **adding a passcode** in addition to using SMS to access the account, providing security in cases of SMS compromise.

When this feature is enabled, the app will periodically ask the user to input their passcode to ensure the messages are not being accessed by someone besides the owner of the account. This prevents account takeover through SMS interception.

Advanced spyware such as Pegasus and Quadream commonly use zero-day vulnerabilities and, especially in the former case, zero-click infections. This kind of advanced spyware can infect a completely patched device without clicking a link or opening an attachment. As users cannot prevent this kind of infection, those at risk of such spyware should keep this in mind.

Potential targets are urged to **use disappearing messages** on messaging apps where messages are automatically deleted after a fixed amount of time as this can limit the damage of account compromise. Compartmentalization such as the **use of separate devices for work and personal use**, or even a **separate device for high-risk work**, also limits potential damage but comes with extra costs and inconveniences.

Endpoints, such as laptops and mobile phones, should be kept up to date by applying security patches to operating systems and other software whenever they become available. **Software should only be acquired from official sources**. In many cases, this requires payment. NGOs should not be shy to discuss this with funders, or to look for free alternatives such as open-source software and programs that provide software free of cost or at reduced prices to eligible NGOs.

Keeping devices up to date is very important, and for iPhones, **regularly rebooting the device** – ideally once a day– and **using Apple's Lockdown Mode** also mitigates the likelihood of attacks.

Much less is known about spyware targeting Android devices, though that does not mean Android users are less at risk. More expensive Android devices, including Google's Pixel devices, are more secure and usually have fixes for vulnerabilities available more quickly than cheaper Android devices. Regularly rebooting devices will likely mitigate damage as spyware is generally removed from devices after a reboot.[i] Rebooting an Android device may also remove evidence of a previous infection, which may be a concern for some users.

Case Studies

Doxing of an Anti-Trafficking Activist

A Mexican woman who provides human rights support and advocates for victims of human trafficking has long been the target of corrupt local governments and organized crime. Both groups oppose her work bringing to light their criminal activity and abuse of human rights they commit, which previously led her to leave the country for some time.

[i] This is the case with all known iPhone spyware and likely also for Android spyware, especially the kind that 'roots' the device.

In the autumn of 2022, she experienced a new harassment campaign. Her personal information was posted on a Mexican website similar to 4Chan that is commonly used for harassment. People on the site were urged to contact her for nude photographs and sexual services.

The woman reached out to SocialTIC, non-profit organization dedicated to research, training, support, and promotion of digital technology and information for social purposes, for help. The content was removed from the website and SocialTIC helped secure her online accounts and devices. SocialTIC performed a remote check on her devices to look for evidence of compromise. Luckily, none were found.

For at-risk communities, any form of harassment is impactful. However, the impact is often far worse for women and sexual minorities as it often involves harassment of a sexual nature.

In this case, the woman ceased her activities for several months as a result of the threats to her security, before eventually resuming them when the content had been removed. Doxing is incredibly impactful and can bring risks to personal safety.

The Tangled Web of Pegasus in Mexico

Pegasus was first discovered in Mexico on the phone of journalist Rafael Cabrera in 2016. In their book, *Pegasus*, investigative journalists Laurent Richard and Sandrine Rigaud reveal that the Mexican government first purchased Pegasus in 2011. The authors suggest that Mexico was NSO Group's first crucial customer, allowing them to become a successful business.

When he took office in 2018, Mexican president Andres Manuel Lopez Obrador ('AMLO') dissolved the federal police and reformed the country's intelligence agency.[29] Both institutions have previously used Pegasus to target individuals investigating the mass kidnapping and disappearance of 43 students in 2014.[30]

Despite his government's promise to the contrary, usage of Pegasus did not cease under AMLO.[31] In 2022, Citizen Lab, an interdisciplinary laboratory based at the University of Toronto, and R3D, a Mexican organization focused on human rights in the digital space, reported that Pegasus was successfully used against journalists, human rights defenders, and at least one opposition politician.[32] In 2023, SocialTIC – non-profit organization dedicated to research, training, support, and promotion of digital technology and information for social purposes – collaborated with R3D and other international partners to confirm Pegasus infections on the phones of two staff members at the Mexican human rights organization Centro Prodh.[33]

For many members of Mexican civil society, Pegasus feels like "business as usual." Although journalism and activism have always been dangerous occupations in Mexico, the pervasive use of spyware by government authorities has normalized such malicious digital threats.

However, in the May 2023 *New York Times* report that revealed Pegasus spyware on the phone of Alejandro Encinas did not feel like business as usual for many individuals in the country.[34] At the time, Alejandro was AMLO's Undersecretary for Human Rights and had been a long time AMLO ally, serving under AMLO during AMLO's term as Mexico City's mayor two decades earlier. Importantly, Encinas was one of the few people from within the government willing to criticize the military, which has continued to gain power under AMLO. In particular, he accused the military of involvement in the disappearance of 43 students in 2014.[35]

More than anywhere else in the world, spyware tools like Pegasus have become a favored tool for the country's military and government to target critics, whether journalists, activists, or members of their own government.

Further Reading

As seen in this report, civil society organizations and journalists often face unique, advanced threats, while lacking the resources to detect, analyze, and prevent them. An in-depth understanding of the threats facing civil society and media allows digital security practitioners to tailor their responses and better support the organizations they work with, leading to customized mitigation measures that are more effective and easier for civil society and media organizations to implement. For more information on the threats faced by civil society and journalists, Internews and their partners have authored the report "Global Trends in Digital Threats: Civil Society & Media," as well as Digital Threat Landscape Reports for Armenia, Brazil, Serbia, and Ukraine. These resources can be found on the Internews' Technology Resources webpage.

History of Mexico

The United Mexican States (Estados Unidos Mexicanos) is a federal presidential republic in North America, bordering the United States to the north and Guatemala and Belize to the south. Mexico is composed of 31 states and the capital, Mexico City. With a population of over 128 million, Mexico is the 10th most populous country in the world. Mexico is a member of the United Nations,[36] the G20,[37] the Organization for Economic Cooperation and Development (OECD),[38] the World Trade Organization,[39] the Asia-Pacific Economic Cooperation forum (APEC),[40] and the Organization of American States (OAS).[41]

Mexico was inhabited by several indigenous peoples before the Spanish conquered the land in the 16th century. After gaining its independence in the 19th century, Mexico underwent several political systems before the Institutional Revolutionary Party (PRI) consolidated power in the post-revolutionary period and began a de facto one-party rule that lasted until 2000. The current constitution of Mexico was adopted in 1917.[42]

Acknowledgements

Since 2021, Internews has worked with seven Threat Labs (*local organizations with the technical capacity and appropriate tools to analyze suspicious phishing and malware samples and then share information back to the community regarding attack trends, emerging threats, and countermeasures*) to respond to incidents affecting the digital security of civil society and media organizations around the world. The data collected through the incident response program helped shape mitigations and response approaches for at-risk communities and informed this report.

Internews would like to express our gratitude to the community of Threat Labs that worked with us on this project. They are committed to assisting those in need and ensuring that their partners in civil society and media organizations can complete their important work safely and effectively. In total, this project supported Threat Labs in responding to over 200 digital security incidents and publishing over 60 educational resources through their websites and social media platforms.

Special thanks to SocialTIC for providing the information to document and share these case studies and for reviewing and contributing valuable feedback to this report. The report would not have been possible without Paul Aguilar and Diego Morabito.

Endnotes

[1] "Mexico." Reporters Without Borders. Accessed September 2023. https://rsf.org/en/country/mexico.

[2] Hoosten, Jan-Albert. "Female journalists covering Mexican feminist protests face harsh police response." Committee to Protect Journalists. November 10, 2020. https://cpj.org/2020/11/female-journalists-covering-mexican-feminist-protests-face-harsh-police-response/.

[3] Sandin, Linnea and Sarah Baumunk. "Mexican Civil Society." Center for Strategic & International Studies. December 2018. https://www.csis.org/analysis/mexican-civil-society.

[4] "Mexico: Shelve regressive bill to curb civil society groups." Amnesty International. March 11, 2022. https://www.amnesty.org/en/latest/news/2022/03/mexico-shelve-regressive-bill-to-curb-civil-society-groups/.

[5] "Mexico: Shelve regressive bill to curb civil society groups," Amnesty International.

[6] "Freedom in the World 2023: Mexico." Freedom House. Accessed July 2023. https://freedomhouse.org/country/mexico/freedom-world/2023

[7] "Freedom in the World 2023: Mexico," Freedom House.

[8] "Freedom in the World 2023: Mexico," Freedom House.

[9] "Freedom in the World 2023: Mexico," Freedom House.

[10] Fistonich, Matt. "Progress Paradox for the LGBTQ+ Community in Mexico." Gay Nation. May 18, 2023. https://gaynation.co/progress-parodox-for-the-lgbtq-community-in-mexico/.

[11] Fistonich, "Progress Paradox for the LGBTQ+ Community in Mexico."

[12] Osborne, Charlie. "Mexico's Pemex oil provider says attempted hack 'neutralized'." *ZDNET*. November 12, 2019. https://www.zdnet.com/article/mexicos-pemex-oil-provider-says-attempted-ransomware-hack-neutralized/#ftag=RSSbaffb68.; Greig, Jonathan. "Foxconn: Mexico factory operations 'gradually returning to normal' after ransomware attack." *The Record.* June 1, 2022. https://therecord.media/foxconn-mexico-factory-operations-gradually-returning-to-normal-after-ransomware-attack.

[13] Ta, Van, Jake Nicastro, Rufus Brown, and Nick Richard. "FIN13: A Cybercriminal Threat Actor Focused on Mexico." Mandiant. Last modified August 8, 2022. https://www.mandiant.com/resources/blog/fin13-cybercriminal-mexico.

[14] Thill, Pol. "Neo_Net: The Kingpin of Spanish eCrime." SentinelOne. July 3, 2023. https://www.sentinelone.com/blog/neo_net-the-kingpin-of-spanish-ecrime/.

[15] "Report: ATM Skimmer Gang Had Protection from Mexican Attorney General's Office." KrebsonSecurity. May 26, 2020. https://krebsonsecurity.com/2020/05/report-atm-skimmer-gang-had-protection-from-mexican-attorney-generals-office/.

[16] Rivera, Santiago Fuentes. "Ley de Ciberseguridad en México: Conoce la nueva Ley." Delta Project. January 18, 2023. https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico.

[17] "Cybersecurity Law Initiative threatens human rights and promotes militarization." Article 19. April 27, 2023. https://articulo19.org/iniciativa-de-ley-de-ciberseguridad-amenaza-los-derechos-humanos-y-promueve-la-militarizacion/.

[18] Segundo, Luis Pablo. "México: Acusan de incoherente a Ley de Ciberseguridad." *DPL News*. July 27, 2023. https://dplnews.com/mexico-acusan-de-incoherente-a-ley-de-ciberseguridad/.

[19] Op cit.

[20] Greig, Jonathan. “Mexican president confirms ‘Guacamaya’ hack targeting regional militaries.” *The Record*. September 29, 2022. https://therecord.media/mexican-president-confirms-guacamaya-hack-targeting-regional-militaries.

[21] Marczak, Bill and John Scott-Railton. “The Million Dollar Dissident: NSO Group’s iPhone Zero-Days used against a UAE Human Rights Defender.” The Citizen Lab. August 24, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[22] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. “Reckless IV: Lawyers for Murdered Mexican Women’s Families Targeted with NSO Spyware.” The Citizen Lab. August 2, 2017. https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/.

[23] Scott-Railton, John, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. “Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague.” The Citizen Lab. November 27, 2018. https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/.

[24] Scott-Railton, John, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert. “Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group’s Spyware.” The Citizen Lab. March 20, 2019. https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/.

[25] “Mexico: Pegasus revelations prompt fresh calls for truth.” Article 19. July 20, 2021. https://www.article19.org/resources/mexico-pegasus-revelations-prompt-fresh-calls-for-truth/.

[26] Pérez, David Marcial. “Leaks reveal Mexican government’s spy contracts with cybersecurity firm.” *El País*. Last modified July 7, 2015. https://english.elpais.com/elpais/2015/07/07/inenglish/1436275149_259998.html.

[27] Carrieri, Matthew. “Cyber Stewards Network and Local Activists Investigate FinFisher in Mexico.” The Citizen Lab. November 8, 2013. https://citizenlab.ca/2013/11/cyber-steward-network-local-activists-investigate-surveillance-mexico/.

[28] Marczak, Bill, John Scott-Railton, Astrid Perry, Noura Al-Jizawi, Siena Anstis, Zoe Panday, Emma Lyon, Bahr Abdul Razzak, and Ron Deibert. “Sweet QuaDreams: A First Look at Spyware Vendor QuaDream’s Exploits, Victims, and Customers.” The Citizen Lab. April 11, 2023. https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.

[29] Kitroeff, Natalie and Ronen Bergman. “How Mexico Became the Biggest User of the World’s Most Notorious Spy Tool.” *The New York Times*. April 18, 2023. https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html.

[30] “Iguala mass kidnapping.” *Wikipedia*. Accessed July 2023. https://en.wikipedia.org/wiki/Iguala_mass_kidnapping.

[31] Solomon, Daina Beth. “Pegasus spyware attacks in Mexico continued under Lopez Obrador, report says.” Reuters, October 2, 2022. https://www.reuters.com/world/americas/pegasus-spyware-attacks-mexico-continued-under-lopez-obrador-report-2022-10-03/.

[32] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Paolo Nigro Herrero, and Ron Deibert. “New Pegasus Spyware Abuses Identified in Mexico.” The Citizen Lab. October 2, 2022. https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/.

[33] "Once again, Centro Prodh is attacked with Pegasus.” Centro Prodh. April 18, 2023. https://centroprodh.org.mx/2023/04/18/nuevamente-centro-prodh-es-atacado-con-pegasus/.

[34] Kitroeff, Natalie and Ronen Bergman. “He Was Investigating Mexico’s Military. Then the Spying Began.” *The New York Times*. May 22, 2023. https://www.nytimes.com/2023/05/22/world/americas/mexico-spying-pegasus-israel.html.

[35] Kitroeff, “He Was Investigating Mexico’s Military. Then the Spying Began.”

[36] “Member States.” United Nations. Accessed July 2023. https://www.un.org/en/about-us/member-states.

[37] "About G20.” Group of Twenty. Accessed July 2023. https://www.g20.org/en/about-g20/.

[38] “Member Countries’ Budget Contributions.” OECD. Accessed July 2023. https://www.oecd.org/about/budget/member-countries-budget-contributions.htm.

[39] "Members and Observers.” World Trade Organizations. Accessed July 2023. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.

[40] “Member Economies.” Asia-Pacific Economic Cooperation. Accessed July 2023. https://www.apec.org/about-us/about-apec/member-economies.

[41] “Member States.” OAS. Accessed July 2023. https://www.oas.org/en/member_states/default.asp.

[42] “Mexico country profile.” *BBC*. Last modified April 4, 2023. https://www.bbc.com/news/world-latin-america-18095241.