BRAZIL

Digital Threat Landscape: Civil Society & Media

Internews
Local voices. Global change.

maria
[lab]

Table of Contents

Background

In Brazil, cybercrime is a significant issue impacting all facets of society, with many cybercriminals operating from the country. Though civil society is subject to many digital threats, more advanced attacks are less common than in some other countries, such as Mexico. While targeted threats are less common, they still occur, and civil society should be proactive in protecting against threats to their digital security.

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 in Brazil and guidance for digital safety experts supporting this community. It also provides context for the cybersecurity industry which may need to analyze security incidents affecting Brazilian civil society and journalists. We conclude with a discussion of mitigation measures that can be proposed by digital security experts to the people and organizations with whom they work, as well as for civil society organizations to implement.

This report was written in close collaboration with MariaLab, an independent non-profit association, operating at the intersection of politics, gender, and technology. MariaLab works to value self-care in digital media and take technology to feminist spaces and feminism to technology spaces. MariaLab builds safe virtual and physical environments, with social, ethnic, or economic dimensions – understanding that only in this way can learning be built through exchange and accumulation of knowledge among all.

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 MariaLab), 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 Brazil.

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

Brazil is a democratic country with competitive elections, as seen during the 2022 presidential election that saw former president Luiz Inácio Lula da Silva (known simply as Lula) resume his role. As the far right gains popularity and far right politicians take positions in the government, however, Brazil is experiencing democratic backsliding, following a global trend.[1] The Economist's Democracy Index categorizes Brazil as a 'flawed democracy', scoring 6.78 out of 10, with a score similar to other countries in the Americas including Argentina and Colombia and falling in the same category as the United States.[2] The country is rated as "Free" in Freedom House's 2023 Freedom in the World Report, scoring 72 out of 100,[3] in comparison to 79 in 2017.[4] The most significant change was a decrease of six points in civil liberties.

Vulnerable communities in Brazil face significant threats to their security. Afro-Brazilians, Brazilians whose ancestry is predominantly from Sub-Saharan Africa; women; and the LGBTQ+ community face even more intense threats. Despite many in authority projecting an idealized version of racial equality, Afro-Brazilians have suffered discrimination for centuries, and it is only in recent years that efforts have been made to acknowledge and rectify the disparities.[5] Women also face significant threats to their safety, as demonstrated by a 2022 report by the Brazilian Security Forum that violence against women of all kinds has been increasing.[6] The LGBTQ+ community is also at risk, and those living at the intersection of these identities suffer the most, with Brazil being one of the most dangerous countries in the world for Black trans women.[7]

According to Freedom House, civil society is generally able to operate freely in Brazil, but members of non-governmental organizations, journalists, and other civil society actors face harassment and violence, which has increased in recent years. Large corporations can exert significant pressure through widespread corruption, impacting the ability of activists to operate freely.[8] These corporations and the government use threats of defamation to control the media, and under former president Bolsonaro, pro-government social media accounts frequently doxed journalists. Women journalists are targeted by online violence at higher rates, but due to a proportionally small presence at high level positions in media organizations, these issues are not taken seriously.[9]

Women journalists are targeted by online violence at higher rates, but due to a proportionally small presence at high level positions in media organizations, these issues are not taken seriously.

Several activists and journalists in Brazil have had to pay for their activism with their lives. Brazilian indigenist Bruno Pereira and British journalist Dom Philips were murdered while traveling to the country's second largest indigenous area;[10] three environmental activists from the same family were found dead in Pará state;[11] and an official of the then opposition Workers' Party (PT) was shot dead by a Bolsonaro supporter.[12] Even politicians have been murdered for their work promoting human rights, most notably the assassination of Marielle Franco. Franco, a Black lesbian from the favelas, was a city councilor in Rio de Janeiro. She was likely murdered due to

Several activists and journalists in Brazil have had to pay for their activism with their lives.

her activism on behalf of these marginalized communities.[13] Under Bolsonaro, investigators and government officials did not prioritize this murder, and the case remains unresolved. With the election of Lula, Franco's family is now hoping for resolution.[14]

Cybersecurity in Brazil

As people, organizations, and companies move more of their operations online, digital threats, especially financially motivated cybercrime, have increasingly detrimental effects. Cybercrime in Brazil has long been an issue, with many actors openly advertising their activities on Facebook and Instagram. Threat actors generally use tools and tactics like banking malware and phishing to make money, frequently targeting the popular "Boleto" payment method with phishing attacks.[15] Recent examples of banking malware also include the Grandoreiro,[16] PixBankBot,[17] and GeoMetrix[18] malware campaigns.

Brazil has experienced many data breaches in which personal information has been leaked, including from government departments. In 2018, a misconfigured server exposed the taxpayer IDs of more than half of the population, and in 2020, the personal data of 16 million COVID-19 patients was exposed online.[19] As the first case study found in Appendix B shows, threat actors will often use leaked personal data in other attacks.

Cybercriminals will frequently hack email and social media accounts to extort funds from the account owners. In 2023, Rest of World reported that many resort to paying 'ethical hackers' to regain access to their Instagram accounts.[20] "Hacking" in this context largely consists of navigating the complicated Instagram customer support process, highlighting usability flaws in Meta's standard procedures.

Despite the prevalence of cybercrime, Brazil only adopted a national cybersecurity strategy in February 2020.[21] Since 2005, the Brazilian government has addressed cybersecurity issues as an aspect of national defense, leading to militarized cyberdefense; since 2008, cyberdefense has fallen under the purview of the armed forces. Between 2012 and 2016, Brazil hosted several significant international events, including the 2014 FIFA World Cup and the 2016 Olympic Games. These events led to increased scrutiny and placed intense pressure on the government to shore up its cyberdefense. The measures adopted, however, fell short of addressing the rise in cybercrime. Some experts have characterized the government policy in this period as a "mirage."[22]

At the end of Michael Temer's term as president, the government published its first national cybersecurity strategy, the first concrete step towards improvement. In 2022, Brazil acceded to the Convention on Cybercrime,[i] facilitating the sharing of electronic evidence of cybercrime with

[i] The Convention on Cybercrime, or the Budapest Convention, is a Council of Europe initiative described as a "**framework that permits hundreds of practitioners from Parties to share experience and create relationships that facilitate cooperation** in specific cases, including in emergency situations, beyond the specific provisions foreseen in this Convention."[i]

other members.[23] This agreement serves as one of the primary international mechanisms for this type of sharing.[24]

With the increased focus on cybersecurity legislation, the balance between cybersecurity and the protection of the digital rights of citizens has been the subject of significant debate. CSOs and other advocates have pointed to an increase in surveillance and a weakening of privacy online.[25] The Brazilian government is currently debating a proposed Fake News Law, formally known as Bill 2630,[26] which would require internet companies to "find and report illegal material, instead of leaving it to the courts."[27] Failing to comply will lead to significant fines.[28] The law faces significant opposition from tech companies, including Google and Meta, while civil society appears divided on the bill. Supporters of the bill argue that it serves as a necessary measure to counteract the increase in illegal activity online. Critics argue, however, that the bill was too hastily created in the wake of the storming of government buildings by Bolsonaro supporters after his loss in the 2022 elections. According to critics, the bill poses a threat to privacy and increases the potential of surveillance.

According to cybersecurity company Torchlight, even as the government implements new legislation, the regulatory landscape of cybersecurity still lacks cohesion. Vulnerabilities remain that can be exploited, and companies still need to invest heavily in cybersecurity measures.[29] In recent years, companies have increased their demand for cyber insurance policies in Brazil, and it is estimated that spending on cybersecurity has surpassed a billion US dollars for the first time.[30] The COVID-19 pandemic increased the need for cyber defense as companies increasingly digitalized in response.

In addition to cyberattacks and legislative vulnerabilities, government surveillance is also of increasing concern in Brazil. In the previous decade, several Brazilian military and civilian intelligence bodies discussed the purchase of the Hacking Team spyware.

In addition to cyberattacks and legislative vulnerabilities, government surveillance is also of increasing concern in Brazil. In the previous decade, several Brazilian military and civilian intelligence bodies discussed the purchase of the Hacking Team spyware.[31] Only one of them, the country's Federal Police, has been confirmed as a customer. It is not known whether and how they have used the spyware. In 2021, the Brazilian government reportedly negotiated with the Israeli digital surveillance company NSO Group for the acquisition of its flagship Pegasus spyware.[32] Carlos Bolsonaro, a councilor of Rio de Janeiro and son of then president Jair Bolsonaro, took part in these negotiations. It is unclear whether Brazil purchased Pegasus and if it has, whether it has been used; no signs of Pegasus have been found in the country. According to a report by the Research Institute in Law and Technology of Recife (IP.rec), however, the government has successfully "legitimized" using surveillance software, and these tools have been assimilated into general practice.[33]

The State of Cybersecurity of Civil Society and Media

As in other communities in Brazil, civil society and the media face several threats to their cybersecurity, but CSOs and media organizations face the additional risk of targeting and retaliation.

The psychological impact of even the most basic cybercrime on at-risk people, especially women and LGBTQ+ people, can be huge.

Civil society in Brazil isn't immune to the financially motivated attacks affecting many in the country, with several activists losing money through digital fraud. This doesn't only have a financial impact on a group already strapped for cash; members of civil society can be traumatized by the experience. Activists may have difficulty determining whether attacks are targeted against them, which can lead to significant stress and fear of surveillance. As the case study found in Appendix C shows, the psychological impact of even the most basic cybercrime on at-risk people, especially women and LGBTQ+ people, can be huge.

Several surveillance-focused mercenary actors, or "hackers-for-hire," are active in Brazil and have targeted government officials and journalists. Investigators have found evidence that both domestic and international criminal groups operate in Brazil. In 2016, the cybersecurity company Kaspersky reported on the "Poseidon Group," a targeted attack group likely based out of Brazil. The Poseidon Group specializes in espionage and evidence demonstrates that they may have been operating since at least 2001. Poseidon generally attempts to steal intellectual property and commercial information, but they have been shown to also target journalists.[34] These mercenary actors are known to stay under the radar for years, so it is difficult to know the extent of their operations. Cybersecurity professionals have also proven that cyber actors have been known to target Brazil. One such group, "Void Balaur," a cyber mercenary group likely based out of Eastern Europe that has a wide range of targets and provides several services, including the collection of private data and account access.[35] They have been shown to target politicians and journalists. Security company SentinelOne reports at least one target in Brazil, without providing any further details.[36]

From an operator's point of view, "good" spyware, and "good" hacks in general, are not discovered by the target. And while no spyware is perfect, the less people are actively looking for it, the less likely it is to be discovered. Brazilian civil society, as in many other parts of the world, is generally not actively looking for it, such as through targeted audits or by using advanced security software.

There is very little evidence of the Brazilian government using the Hacking Team or Pegasus spyware to target civil society. This may be somewhat surprising given its prevalence in other Latin American countries, with Mexico a particularly notorious example. In general, only governments and militaries can purchase advanced spyware. Globally, these bodies have deployed the software against civil society under a pretext of protecting national security, even if the motivation for its use is other factors – such as corruption, the targeting of opposition by the extreme right, or retaliation against journalists and activists. Although the evidence of advanced

spyware use in Brazil is limited, the possibility of its use in the future is still of concern and warrants close attention.

From an operator's point of view, "good" spyware, and "good" hacks in general, are not discovered by the target. And while no spyware is perfect, the less people are actively looking for it, the less likely it is to be discovered. Brazilian civil society, as in many other parts of the world, is generally not actively looking for it, such as through targeted audits or by using advanced security software. For now, its existence in Brazil should not be excluded as a possibility.

Mitigation Measures

To better help Brazilian civil society understand the full breadth of digital attacks, more **funding for audits** – in particular audits that include device forensics – **and security software** is recommended.

Account security is important for anyone in Brazil and for members of civil society and the media in particular. **Two-factor authentication is a must** – and mitigates the less controllable use of weak and/or reused passwords. Though better than no second factor at all, SMS shouldn't be considered secure, especially for at-risk users. Using an authentication app is better, while using a hardware token generally provides the best security.

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, which is common in the country.

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**, which in many cases will require paying for it. NGOs should not be shy to discuss this with funders, or to look for free alternatives – either through open-source software or through programs that provide the software free of cost or at reduced prices to eligible NGOs. For organizations looking for longer-term or more self-sustaining solutions, employing or partnering with an IT professional(s) is essential. With proper staffing, organizations may be able to set up and maintain their own infrastructure with a focus on security and data protection. Technical solutions, including the types of software used, will vary depending on the organization's needs and resources.

In Brazil, FASE – the Federation of Organs for Social and Educational Assistance has created a report analyzing the connection between philanthropy and digital care. This report provides more information for civil society organizations looking to connect with donors that could fund digital security improvements, as well as information for donors aiming to help improve the digital security of civil society in Brazil.

While it is unknown whether civil society in the country has been targeted by advanced spyware like Pegasus, those considered high-value targets should note that such spyware commonly uses

zero-day vulnerabilities and zero-click infections. These types of attacks mean a completely patched device can be infected in a way that a user cannot prevent by avoiding a suspicious link or attachment. This should be kept in mind by those at risk of such spyware.

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 a future account compromise. Compartmentalization, by **using separate devices for work and personal use**, or even a **separate device for high-risk work**, also limits the damage, but this comes with extra cost and inconvenience.

Keeping devices up to date is very important, and on iPhones, **regularly rebooting the devices** – 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 that 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.[ii] Rebooting an Android device may also remove evidence of a previous infection, which may be a concern for some users.

Finally, most threats experienced by civil society and media in Brazil are not sophisticated and are successful because targets may not be knowledgeable when it comes to technology. Resources for improving security should provide opportunities for the whole community to learn more about technology and digital security, rather than just information on advanced threats.

Case Studies

Rogue Browser Extension Case Study

A Brazilian civil society organization that focuses on litigation on cases of human rights violation uses the Malwarebytes security software that aims to detect malware on devices. This software is managed centrally – something which is fairly uncommon for smaller civil society organizations – and the administrator received an alert that "spyware" was detected on one of the endpoints.

Looking into the alert and investigating the affected laptop led to the discovery of a browser extension "Netflix party," which was advertised as a possibility for multiple users to watch Netflix together. The user confirmed they had indeed installed this extension, but this was done on their personal laptop. However, because the user was logged into Chrome on both their personal and their work laptop, Chrome automatically synchronized extensions so that the malicious extension also appeared on the work laptop. This kind of synchronization is likely not something many

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

people are aware. This could easily undo some of the benefits of compartmentalizing work and personal devices, emphasizing the need for information security training.

Marialab, an independent non-profit association, operating at the intersection of politics, gender, and technology, performed a brief analysis of the plugin and found it sent every visited URL to the plugin's command and control server and would perform further actions depending on the response of the server, to make money through affiliate schemes.

This research matched what security company McAfee wrote up in an analysis of five malicious Chrome extensions published in August 2022.[37] The exertions included "Netflix Party" and "Netflix Party 2" – both were present on the affected laptop.

To clean up the infection, the extension was uninstalled and all files that Malwarebytes detected as malicious were manually removed. Registry entries created by the plugin were removed too, as Malwarebytes also flagged them.

It should be noted here that it's not uncommon for security software to detect individual files linked to an infection as malicious, even if on their own the files wouldn't have been able to cause any harm. This was the case here, as the extension itself had been uninstalled. It is generally a good idea to remove all files flagged as malicious, though.

After removing these files, a new scan showed the computer as clean. The user was recommended to use a different browser, in this case Firefox, for work-related purposes.

Extensions for Chrome and other browsers can seriously enhance a user's browser experience. These extensions do have a lot of power though, such as access to all browser data, including visited URLs and possible cookies.

This can be used, as was the case here, by the developers of the extension to make money through affiliate schemes, something which has relatively little impact on the user itself. However, it can also be used to hijack sessions from, for example, webmail and financial services. Such a session hijack is effective even if the user uses strong multi-factor authentication to protect the account and it can lead to the theft of personal data or money.

At-risk users have to think very carefully about installing browser extensions. Ideally, they would only install extensions from trusted, verified developers. In case of doubt, if an extension is necessary, potential harm can be mitigated by installing the extension in a different browser than the main one used.

Feminist Activist Receiving Personalized Sextortion Email Case Study

In October 2022, a feminist activist in Brazil received a worrying email. Written in fluent Portuguese, the email mentioned her full name, email address and one of her passwords. Aside from that, it mentioned that the sender had installed spyware on the machine and would publish details of her online activity and recordings from her webcam unless she paid 3000 Brazilian Real (a little over 600 US dollars) to a specified Bitcoin address.

Though this amount is small in the context of the money involved in cybercrime and ransomware, it is a large amount for an individual: more than a third of the average monthly income in the country.

And while receiving a threatening email like this is worrying for anyone, it is a particular concern for someone whose online activities make her a target of various kinds of harassment. On top of that, the sexualization of women online make the possible leak of personal information and images even more harmful.

The activist reached out to Internews partner MariaLab, an independent non-profit association, operating at the intersection of politics, gender, and technology. They looked at the email and confirmed that, despite the inclusion of personal details, it was not targeted at all. Rather, it was an example of a common scam that goes back to at least 2018.[38]

The personal details included in this case come from a data breach, which allows the scammers to send 'personalized' emails like this in large numbers, sometimes even millions of emails per campaign. Using the website "Have I Been Pwned", which keeps track of data breaches, MariaLab was able to confirm the activist's email address had been included in no fewer than three data breaches.

Convinced this was not an actual extortion attempt, she rightly did not pay the 3000 Reals. However, the same Bitcoin address received 20 payments around the same time, suggesting some people did fall for the scam. Marialab did use the opportunity to help the activist better secure her devices and accounts.[39]

"Sextortion" scams like these are common and an example of low-level cybercrime. However, this case – which is not unique among civil society activists and journalists – shows it can still have a very big impact on certain at-risk people.

Spyware is a real threat and spyware that steals information that is later used for extortion does exist, but it is extremely rare. Malware accessing the camera is very rare on modern laptops, though for some extra peace of mind, it does not hurt to use a webcam protector when not actively using the camera. Some laptops have one built in.

There is little one can do to prevent personal information provided to a third party being stolen in a data breach, though thankfully password storage has improved greatly in recent years so that leaks including passwords are becoming less common. Most sextortion emails involve data breaches dating back many years.

There are many good reasons to use unique passwords for every service and using a password manager can help keep track of them. In this case, if the password being used for extortion was unique and only in use with one site or platform, the target of such an email will understand where the breach came from.

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, Mexico, Serbia, and Ukraine. These resources can be found on the Internews' Technology Resources webpage.

History of Brazil

The Federative Republic of Brazil (República Federativa do Brasil) is a federal presidential constitutional republic in South America, the largest country on the continent. Brazil is also the fifth largest country in the world by area and seventh most populated. Brazil is a member of several large international organizations, including the United Nations,[40] the G20,[41] BRICS,[42] Mercosul/Mercosur,[43] and the Organization of American States.[44] Originally inhabited by several indigenous groups, Brazil was colonized by the Portuguese in the early 16th century before becoming an independent country in 1822 as the Empire of Brazil. The Empire of Brazil adopted a constitution in 1824 that established a constitutional monarchy with a bicameral legislature. In 1889, after the abolition of slavery, the military led a coup d'état that reformed the government under a presidential republic. Brazil was under authoritarian military governance from 1964 to 1985, under which human rights abuses and extrajudicial killings were common. In 1985, civilian government was reestablished, and the current constitution was adopted in 1988.[45]

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 MariaLab 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 their cooperation and expertise.

Endnotes

[1] "Democracy Index 2022." *Economist*. Accessed July 2023. https://www.eiu.com/n/campaigns/democracy-index-2022/.

[2] "Democracy Index 2022," Economist.

[3] "Freedom in the World 2023: Brazil." Freedom House. Accessed July 2023. https://freedomhouse.org/country/brazil/freedom-world/2023.

[4] "Freedom in the World 2017: Brazil." Freedom House. Accessed July 2023. https://freedomhouse.org/country/brazil/freedom-world/2017/.

[5] "Afro-Brazilians." Minority Rights Group International, World Directory of Minorities and Indigenous Peoples. Access July 2023. https://minorityrights.org/minorities/afro-brazilians/.

[6] Viapiana, Tabata. "In Brazil, 14 women are physically assaulted per minute: new study." *Brazil Reports*. March 8, 2023. https://brazilreports.com/in-brazil-14-women-are-physically-assaulted-per-minute-new-study/4157/.

[7] Damasceno, Edilana. "8 Every 10 Black and LGPTGIAP+ People Have Been Victims of Hate Speech." Data Labe. March 29, 2023. https://datalabe.org/iea_negres_lgbtqiap/.

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

[9] "UNESCO in Brazil shows the scenario of violence against women journalsits." UNESCO, News. Last updated April 20, 2023. https://www.unesco.org/en/articles/unesco-brazil-shows-scenario-violence-against-women-journalists.

[10] Vieira, Matheus. "Brazil: Amnesty International laments brutal deaths of Bruno and Dom and demands justice." Amnesty International. June 16, 2022. https://www.amnesty.org/en/latest/news/2022/06/brazil-amnesty-laments-brutal-deaths-bruno-dom-demands-justice/.

[11] "Americas: Amnesty International sounds alter over killings of human rights defenders and journalists in first month of 2022." Amnesty International. February 2, 2022. https://www.amnesty.org/en/latest/news/2022/02/americas-alert-killings-human-rights-defenders-journalists/.

[12] Mano, Ana. "Brazil party official shot dead as pre-election political violence escalates." *Reuters*. Last modified July 11, 2022. https://www.reuters.com/world/americas/brazil-party-official-shot-dead-pre-election-political-violence-escalates-2022-07-10/.

[13] De Mattos Rocha, Lia. "The life and battles of Marielle Franco." openDemocracy. March 20, 2019. https://www.opendemocracy.net/en/democraciaabierta/life-and-battles-marielle-franco/.

[14] Carvalho, Igor. Rocha, Ana Paula, trans. "Marielle's murder: 'My mom should be remembered for her work, not for the unsolved crime.'" Brasil de Fato. March 14, 2023. https://www.brasildefato.com.br/2023/03/14/marielle-s-murder-my-mom-should-be-remembered-for-her-work-not-for-the-unsolved-crime.

[15] "Boleto malware may lost Brazil $3.75bn." *BBC*. Last modified July 3, 2014. https://www.bbc.com/news/technology-28145401.

[16] Bautista, Bernard. "Grandoreiro Banking Malware Resurfaces for Tax Season." Trustwave. May 26, 2022. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/grandoreiro-banking-malware-resurfaces-for-tax-season/.

[17] "PixBankBot: New ATS-Based Malware Poses Threat to the Brazilian Banking Sector." Cyble. May 30, 2023. https://cyble.com/blog/pixbankbot-new-ats-based-malware-poses-threat-to-the-brazilian-banking-sector/.

[18] Lytzki, Igal. "Operation Geometrix Do Brazil." Perception Point. July 25, 2023. https://perception-point.io/blog/operation-geometrix-do-brasil/.

[19] Shoorbajee, Zaid. "Misconfigured server exposed half of all Brazilian taxpayer ID numbers, report says." *CyberScoop*. December 11, 2018. https://cyberscoop.com/brazil-data-breach-cpf-120-million-infoarmor/.

[20] Dib, Daniela and Marília Marasciulo. "Instagram account hacked? 'Ethical hackers' will get it back." *Rest of World*. August 21, 2023. https://restofworld.org/2023/hacked-instagram-account-recovery-ethical-hackers/.

[21] Hurel, Louise Marie. "Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future." School of Public Policy at Georgia Institute of Technology, Internet Governance Project. April 5, 2020. https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future/.

[22] Hurel, "Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future."

[23] "Brazil accedes to the Convention on Cybercrime and six States sign the new Protocol on e-evidence." Council of Europe, Cybercrime, News. November 30, 2022. https://www.coe.int/en/web/cybercrime/-/brazil-accedes-to-the-convention-on-cybercrime-and-six-states-sign-the-new-protocol-on-e-evidence.

[24] Bannelier, Karine. "The U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights." *Lawfare*. January 31, 2023. https://www.lawfaremedia.org/article/the-u.n.-cybercrime-convention-should-not-become-a-tool-for-political-control-or-the-watering-down-of-human-rights.

[25] Bannelier, "U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights."

[26] PL 2630/2020. Câmara dos Deputados. https://www.camara.leg.br/propostas-legislativas/2256735

[27] Boadle, Anthony. "Brazil pushes back on big tech firms' campaign against 'fake news law'." *Reuters*. May 2, 2023. https://www.reuters.com/world/americas/brazil-lawmakers-vote-controversial-bill-clean-up-social-media-2023-05-02/.

[28] Ibid.

[29] "Illuminate Your Unknowns." Torchlight AI. Accessed July 2023. https://www.torchlight.ai/illuminate-your-unknowns/.

[30] "Illuminate Your Unknowns," Torchlight AI.

[31] Antonialli, Dennys and Jacqueline de Souza Abreu. "State Surveillance of Communications in Brazil and the Protection of Fundamental Rights." Electronic Frontier Foundation and Internet Lab. December 2015. https://www.eff.org/files/2015/12/17/brazil-en-dec2015_0.pdf.

[32] "Brazil: Million-dollar negotiation for the Pegasus espionage programme, developed by the NSO Group, excluded official government investigation bodies that would directly benefit from the tool." Business & Human Rights Resource Centre. June 8, 2021. https://www.business-humanrights.org/en/latest-news/brazil-million-dollar-negotiation-for-the-pegasus-espionage-programme-developed-by-the-nso-group-excluded-official-government-investigation-bodies-that-would-directly-benefit-from-the-tool/.

[33] André Ramiro, Pedro Amaral, Mariana Canto and Marcos Cesar M. Pereira. "Insecurity merchants: conjuncture and risks of governmental hacking in Brazil." https://ip.rec.br/publicacoes/mercadores-da-inseguranca-conjuntura-e-riscos-do-hacking-governamental-no-brasil/

[34] "Poseidon Group: a Targeted Attack Boutique specializing in global cyber-espionage." SecureList. February 9, 2016. https://securelist.com/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/73673/.

[35] "Void Balaur and the Rise of the Cybermercenary Industry." Trend Micro Research. November 10, 2021. https://www.trendmicro.com/en_us/research/21/k/void-balaur-and-the-rise-of-the-cybermercenary-industry.html.

[36] Hegel, Tom. "Void Balaur: The Sprawling Infrastructure of a Careless Mercenary." SentinelLABS. September 22, 2022. https://www.sentinelone.com/labs/the-sprawling-infrastructure-of-a-careless-mercenary/.

[37] "Malicious Cookie Stuffing Chrome Extensions with 1.4 Million Users." McAfee Labs. August 29, 2022. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malicious-cookie-stuffing-chrome-extensions-with-1-4-million-users/.

[38] "Sextortion Scam Uses Recipient's Hacked Passwords." KrebsonSecurity. July 12, 2018. https://krebsonsecurity.com/2018/07/sextortion-scam-uses-recipients-hacked-passwords/.

[39] "38pnj-nLRXW." Blockchain.com. Accessed July 2023. https://www.blockchain.com/explorer/addresses/btc/38pnj1L9gKLhYWTqGYBTkY2LroM2nnLRXW.

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

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

[42] du Plessis, Carien, Anait Miridzhanian, and Bhargav Acharya. "BRICS welcomes new members in push to reshuffle world order." *Reuters*. August 24, 2023. https://www.reuters.com/world/brics-poised-invite-new-members-join-bloc-sources-2023-08-24/.

[43] "MERCOSUR Countries." MERCOSUR. Accessed July 2023. https://www.mercosur.int/en/about-mercosur/mercosur-countries/.

[44] "Member States." OAS. Accessed July 2023. https://www.oas.org/en/member_states/default.asp.

[45] "Brazil country profile." *BBC*. Last modified June 2, 2023. https://www.bbc.com/news/world-latin-america-18909529.