Global Trends in Digital Security

Civil Society & Media

Internews
Local voices. Global change.

Introduction

Worldwide, civil society and media organizations are increasingly operating in challenging environments due to shrinking civic spaces; rising authoritarianism, both political and digital; and conflict. Governments and other actors deploy digital tactics and tools to restrict civic space and hamper the work of activists, human rights groups, and journalists. They frequently rely on tactics that include the use of commercial spyware to spy on targets and extract sensitive information, the interception of communications, device seizures, and distributed denial-of-service (DDoS) attacks targeting websites of independent media and civil society organizations. On top of these threats, the digital spaces that civil society organizations and journalists have been using to disseminate their work and build audiences have become increasingly unsafe. Rising polarization offline and online and the layoffs affecting the trust and safety teams of big tech impact the ability of these organizations to operate safely; platforms also continuously fail to implement lasting and systemic solutions that put to a halt the harassment, gender-based violence, and hateful content that plague their services.[1]

This report explores the digital threats that civil society groups, journalists, and activists face, and the impacts of these threats on their work and activities in an increasingly unstable world. Each section covers a specific type of threat, discusses its impacts, and provides tips on protection and mitigation.

October 2023

Researched and Written by Afef Abrougui
Reviewed and Edited by Martijn Grooten, Ashley Fowler, and Marc Shaffer
Graphic Design by Skyler Sallick

Table of Contents

Methodology

This report's methodology combines desk research and findings from the forensic analysis on digital attacks against civil society groups conducted by Threat Labs. Internews collaborated with Conexo, based in the Latin America and Caribbean region; CyberHub-AM, based in Armenia; Digital Security Lab Ukraine, based in Ukraine; Jordan Open Source Association, based in Jordan; MariaLab, based in Brazil; SHARE Foundation, based in Serbia; and SocialTIC based in Mexico. The Threat Labs generally support individuals and organizations within these target countries but do handle cases from other countries as well. The incidents used to inform this report were documented between September 2022 and June 2023. Additional data was collected using credible secondary sources such as news websites, press agencies, statements, and research by human rights and digital rights groups. Sources published over the past three years were prioritized, however older sources were referred to as needed.

Threat Labs are 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.

Key Terms

Backdoor: a method of bypassing existing security measures in a computer system to gain access to a network, website, or application.[2]

Doxing: the practice of exposing personal information (for the purpose of harassing, threatening, and stifling victims. This information may include private addresses, photos, phone numbers, information on family members, etc. Information can be extracted from publicly available sources - such as government registries or photos that victims previously shared via social media or email - or through unauthorized access - such as data leaks, hacking, phishing, or the use of spyware.[3]

Interception: the practice of saving and reading others' communications and internet traffic. Actors may listen to calls, view and read messages and other content, and monitor online activities.[4]

Malware (or "malicious software"): a blanket term for any malicious program or code that is harmful to information systems, including websites, devices, storage systems, and social media accounts. Malware includes viruses, spyware, adware, and ransomware.[5]

Phishing: a method of crafting messages using social engineering that are aimed at tricking people into a damaging action that benefits the sender. Phishing is often done by a criminal seeking to commit fraud or a political actor seeking to access sensitive information. Phishing messages take different forms, including bulk phishing and spear phishing. In bulk phishing, an actor impersonating a well-known company or organization sends a generic message to many recipients at one time to trick them into clicking on a malicious link, gaining access to

sensitive personal data like financial information and account log-in details. In spear phishing, a threat actor uses phishing techniques to target a specific individual or organization. [6]

Social engineering: the use of psychological manipulation tactics by threat actors to trick a target into granting access to accounts, devices, or personal information. Criminals can use the information they obtain illicitly to conduct fraud, or in the case of authoritarian regimes, use it to harass and silence dissidents and journalists.[7]

Spyware: a type of malware that infects devices and collects personal information and monitors the activities of users, often without their knowledge, and shares the extracted information with third-parties, usually governments.[8]

Threat actor: state or non-state actors that are involved in attacks or actions that threaten the cybersecurity of an organization or individual. In the context of civil society and media, these are generally national security agencies, individual hackers, or hacker groups that infect devices with spyware or conduct coordinated phishing campaigns to target the information systems of civil society to make a political statement, or cybercriminals seeking to commit fraud.[9]

Two-factor authentication (2fa): a method of logging into an account that adds an extra layer of protection by requiring a second method of identification in addition to the username and password combination. 2fa methods include SMS verification, using an authenticator app, and hardware tokens.[10]

Zero-click attack: a cyberattack that does not need a user's interaction to execute malware that infects a device, network, computer system, website, or application.[11]

Zero-day: a vulnerability in a computer system that was previously unknown to its developers or security experts and researchers capable of identifying it.[12]

Context

According to Freedom House's 2023 Freedom in the World report, "Global freedom declined for the 17th consecutive year," and "the most serious setbacks for freedom and democracy were the result of war, coups, and attacks on democratic institutions by illiberal incumbents."[13] In their 2023 Freedom on the Net report, Freedom House also reported that "[g]lobal internet freedom declined for the 13th consecutive year."[14]

The decline in global freedom and rise of authoritarianism both allows for and benefits from the decline in digital freedom and rise of digital threats.

Civil society groups, human rights defenders, and media organizations often find themselves impacted by political polarization and efforts to erode democracy. For example, the Sahel region of Africa witnessed seven coups between August 2020 and August 2023. Unconstitutional transfers of powers, even when they remove dictators, risk creating conflict, economic crises, and political instability. These conditions further add to the multiple challenges that civil society groups face.[15] One of the most notable examples, in Burkina Faso, two coups in 2022 derailed a democratic transition process.[16] In January 2022, the military - led by Lieutenant Colonel Paul-Henri Sandaogo Damiba - deposed the elected president Roch Kaboret, suspended the constitution, and dissolved the parliament.[17] Damiba, who had been appointed as interim president, was then deposed by military officer Captain Ibrahim Traoré in September. Traoré dismissed the transitional government and suspended political and civil society activities.[18] The new government also tightened restrictions on the media and the work of journalists.[19]

Once labelled the "success story"[20] of the Arab Spring - democratic uprisings that swept the Arab region in 2010-2011 - Tunisia's democratic and human rights progress has dwindled over the past two years. Since July 2021, President Kais Saied has dissolved the parliament elected in 2019, expanded his powers, and weakened judicial and legislative powers.[21] The harassment and prosecutions of human rights groups, journalists, and activists have now reached levels not seen since the 2011 ousting of dictator Zine El Abidine ben Ali.[22] In the wake of these events, a decree law issued in September 2022, purportedly to combat cybercrime, has been used to prosecute journalists, lawyers and politicians for expressing their opinions online.[23]

In Brazil, far-right president Jair Bolsonaro lost his re-election bid to Luiz Inácio Lula da Silva, often referred to as Lula, by a narrow margin in late 2022. In addition to falling vaccination rates[24] and rainforest destruction,[25] Bolsonaro's troubled legacy includes declining democracy and a rise in political polarization and violence.[26] After losing the election, Bolsonaro and his supporters attempted to overturn the results by storming government buildings. As ex-president, he continued his strategy of mobilizing followers on social media to attack journalists and critics of Bolsonaro.[27] In 2022, Google terminated more than 100 YouTube channels engaged in coordinated influence operations supportive of Bolsonaro.[28]

War and conflicts have also made the work of civil society more fragile. In its war on Ukraine, Russia has intensified its domestic crackdown on human rights, seeking to crush any expression of dissent. The Russian government has attempted to shut down criticism abroad as well.[29] In

areas Russia occupies in Ukraine, civil society leaders are subjected to torture, detentions, kidnappings, and even murder.[30] Civil society in Ukraine has been targeted in multiple phishing campaigns attributed to APT28 (also known as Fancy Bear), a threat actor associated with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).[31]

As shown in the examples above, the decline in global freedom and rise of authoritarianism both allows for and benefits from the decline in digital freedom and rise of digital threats. Digital tactics and tools are deployed during war, elections, and other conflicts to restrict civic space. Elections in Brazil and Mexico, the war in Ukraine, and the conflict between Armenia and Azerbaijan have all created a more precarious situation in which civil society and the media operate, including an increase in digital attacks. The following sections will review several tactics employed by both state and non-state actors against civil society and the media. These tactics are associated with the rise in digital authoritarianism, as well as more traditional forms of cyberattacks.

Threats and Tactics

Commercial spyware and state targeted surveillance

Commercial spyware and its use by state actors poses a major threat to the work of civil society. Between September 2022 and August 2023, the Threat Labs who collaborated on this report responded to dozens of suspected and confirmed incidents of spyware attacks brought to them by civil society organizations, media organizations, journalists, and human rights defenders. The affected people reported most of these incidents after receiving a notification from Apple that their iPhones may have been the target of a state-sponsored attack.[32]

Pegasus, developed by the Israeli company NSO Group, is the world's most infamous spyware. It is designed to exploit zero-day vulnerabilities in mobile devices and often uses zero-click attacks. Following successful infection, those who deployed the spyware gain access to all communications, messages, and data on the phone. It was first discovered in 2016 when Ahmed Mansoor, an Emirati human rights defender currently serving a 10-year jail sentence for his human rights activism, received a message with a malicious link. Mansoor forwarded the message to Citizen Lab for analysis. Citizen Lab found that the message contained spyware that would install itself and collect communications and location data of infected phones.[33] Since then, it became evident that Pegasus's deployment by both authoritarian and democratic governments is widespread.[34] NSO's clients include the governments of Azerbaijan, Hungary, India, Mexico, Morocco, Rwanda, Saudi Arabia, and the United Arab Emirates. According to a *Financial Times* report, the Indian government is alleged to have used Pegasus to target journalists, academics, and opposition leaders.[35] In September 2023, Citizen Lab, in collaboration with Access Now, revealed that the iPhone of Galina Timchenko, an award-winning exiled Russian investigative journalist and co-founder of the independent media outlet Meduza, was also infected with Pegasus in February 2023.[36]

Pegasus, developed by the Israeli company NSO Group, is the world's most infamous spyware.

And it's not just Pegasus. Other developers of spyware include Cytrox; Gamma Group, the developer of FinFisher; and the now-defunct Hacking Team. After revelations of the misuse of spyware against journalists and opposition politicians, among others, President Biden issued an executive order in March 2021 that limited how US Government agencies can use spyware. He followed this move in November 2021 by adding NSO Group to its "entity list," prohibiting US firms from sharing technology with the group.[37] In July 2023, four more spyware distributors - Intellexa S.A. in Greece, Cytrox Holdings Crt in Hungary, Intellexa Limited in Ireland, and Cytrox AD in North Macedonia - were added to the list.[38]

Despite increased scrutiny and government restrictions on their use, the market of spyware producers continues to thrive.[39] In 2015, the company DarkMatter was founded in the UAE and hired former U.S. intelligence officers to carry out operations on behalf of the UAE government targeting human rights defenders.[40] Following Pegasus's blacklisting by the US Government, India is reportedly looking to acquire alternatives to the controversial spyware.[41]

With its Predator spyware, Cytrox has emerged as a primary competitor to NSO Group.[42] Threat actors used Predator to hack Egyptian opposition politician Ahmed Nour, the Egyptian host of a news program, and Greek journalist Thanasis Koukakis.[43]

Spyware infringes on privacy, an enabler of other fundamental rights. Privacy is necessary to ensure the rights to freedom of expression and assembly. Spyware enables the targeting entity (often state actors in authoritarian regimes) to access sensitive information and use it to crack down on civil society. Such access can endanger the safety of journalists, human rights defenders, and civil society groups, as well as the sources they may be trying to protect. Some governments will not hesitate to use the information they obtain via spyware to prosecute and jail their targets. One case responded to by a Threat Lab documented multiple successful attempts to compromise a journalist's phone that preceded their detention by a few days.

Spyware infringes on privacy, an enabler of other fundamental rights. Privacy is necessary to ensure the rights to freedom of expression and assembly.

Given these serious implications, suspected and confirmed spyware attacks do not only have an impact on victims' abilities to do their work but also their mental wellbeing. Victims experience distress, frustration, fear, stress, panic, anger, and irritation. In Jordan, one victim, who received a notification from Apple that their iPhone was targeted in a spyware attack, mentioned that afterwards they were afraid to use their phone. An Armenian journalist, who also received a notification from Apple, described being unable to do their job because they couldn't trust their own phone anymore. One Azerbaijani investigative journalist was particularly concerned about how the Pegasus infection on her phone could compromise others.[44]

To mitigate the impacts of spyware attacks, iPhone users at risk of these attacks are strongly advised to enable Lockdown Mode, which restricts some apps and phone features to prevent their exploitation in spyware attacks, at the cost of some usability.[45] For those with Android

phones, Google's Advanced Protection Program can offer some mitigation too, though likely less against advanced spyware. Additionally, users should keep their devices as up to date as possible; releases often address security vulnerabilities that can be exploited by spyware providers. Regularly rebooting phones may also mitigate the impact of advanced spyware, as such spyware rarely, if ever, lives beyond a reboot. Finally, users should not open or click any email attachments or links of which there is any doubt. When suspicious, users should forward the email to trusted experts for examination and flag it to their organization's IT department if available.

Phishing

Phishing is the most common type of cyberattack. According to IBM Security X-Force Threat Intelligence Index 2023, 41% of incidents they handled last year involved phishing. Phishing is most widely used by cybercriminals for fraud-related purposes.[46]

Phishing messages targeting email and messenger accounts generally contain malicious links, which lead users to a web page that captures information, such as login details. The threat actor then uses the captured username or email address and password to log in to the relevant account (email, social media accounts, cloud account, etc.). In other cases, the messages include links or attachments that, when clicked on, download malware onto the device.

In an incident responded to by CyberHub-AM, financially-motivated hackers compromised an email account of a civil society organization, rerouting and interfering with existing conversations with an equipment manufacturer. The hackers then pretended to be the manufacturer and submitted an invoice of several thousands of dollars to the NGO, which it paid. When the actual manufacturer wrote to say that they had not received a transfer, the NGO realized it had been a victim of fraud.

In another incident submitted to JOSA, the target was subjected to a social engineering attack through a LinkedIn message that nudged them to click on a link to download files from an iCloud drive. The files contained malware that allowed the attacker to take control of their employer's Facebook account and use the Facebook Ad Manager to publish ads at the employer's expense, resulting in financial losses.

Threat actors may target victims' professional communications, sources, and location data; they are also known to collect personal information, such as intimate photos and videos or information about the victim's relatives, to use in smear and harassment campaigns.

Phishing is also deployed by political actors – usually a state entity – to extract sensitive information from and about opponents, journalists, and civil society actors. Threat actors may target victims' professional communications, sources, and location data; they are also known to collect personal information, such as intimate photos and videos or information about the victim's relatives, to use in smear and harassment campaigns.

An example of politically motivated phishing, NilePhish was a large-scale phishing operation targeting civil society in Egypt. Uncovered in 2017 by Citizen Lab, NilePhish operators used social engineering to craft highly personalized messages bearing the hallmarks of the Egyptian

government to target NGOs. In one case, hours after the December 2016 arrest of Egyptian lawyer Azza Soliman, her colleagues received an email pretending to contain a Dropbox file of her arrest warrant. Clicking on the link led to a fake Dropbox login page, pre-populated with the target's username, that captured the target's password, giving the perpetrator access to the target's account.[47]

Egyptian civil society continues to be targeted with phishing attacks. In 2019, Amnesty International uncovered another coordinated campaign to access the emails of human rights defenders and civil society organizations. Amnesty estimated that several hundreds of individuals were targeted. Many were targeted by a malicious OAuth application, which when granted access can "read, compose, send, and permanently delete" emails.[48] OAuth, short for Open Authorization, is an open standard that allows users to delegate services, such as Google, access to accounts on other services without disclosing their passwords.

As with spyware attacks, successful phishing attacks can expose the sensitive information of victims, including login details, financial information, communications, and the content of their devices. Successful phishing can lead to the loss of money, identity theft, and the disruption of an organization's operations. State-sponsored phishing attacks endanger the safety of members of civil society and their networks. Through phishing, governments can extract information that they may use to persecute and jail activists, human rights defenders, journalists, and NGO workers and volunteers. Even if unsuccessful, these attacks can lead to stress and anxiety, affecting the professional and personal lives of victims.

To help prevent successful phishing attacks and mitigate their impacts, users should avoid clicking on links or opening attachments of which there is any doubt.

To help prevent successful phishing attacks and mitigate their impacts, users should **avoid clicking on links or opening attachments** of which there is any doubt. If they receive suspicious or unexpected messages purporting to be from someone they know, users should **contact that person via a secondary channel to verify the message**. Users should also regularly check which devices have access to their account data on websites and applications and revoke access from those they do not recognize or no longer use. Practicing strong passphrase hygiene (including not reusing passwords across multiple accounts) is also key, and **users should enable two-factor authentication (2fa) on key accounts** (emails, social media, cloud, financial apps, etc.). Organizations should implement internal security policies and practices that tackle phishing attacks and educate their staff about different forms of attacks. In the case of a successful attack, the victim should **immediately change their password, check the account for any malicious activity, and end sessions on other devices**. Those suspecting that malware was installed on a device should run an antivirus scan. If possible, factory resetting the device is a good way to ensure no malware remains.

Account compromise

Threat Labs responded to dozens of incidents pertaining to successful and unsuccessful attempts to compromise accounts, mainly email accounts and social media accounts – including Facebook, Instagram, Telegram, Twitter, Viber, WhatsApp, and YouTube.

Through state-coordinated campaigns targeting civil society, threat actors have hacked many accounts of NGOs, media organizations, and activists, as in the case of NilePhish in Egypt and a 2022 state-backed campaign in Iran targeting activists, journalists, NGO staff, and diplomats.[49]

In addition to password compromise, attackers are sometimes able to intercept 2fa codes sent by SMS, the combination of which allows them to take over accounts using this most basic form of 2fa. On top of this, messaging services like WhatsApp, Telegram or Signal rely on SMS to authenticate, and if no passcode is set on an account, SMS interception is sufficient to take over an account on these services.

DSLU investigated an incident from a Ukrainian organization which had received a Telegram notification saying an incorrect password had been used to attempt to log in to their Telegram account. It appeared that an SMS message with a login code had been intercepted, but as the target was using a password in addition to SMS confirmation for two-step verification, the attackers were prevented from taking over the Telegram account.

In another incident handled by MariaLab, a human rights organization lost access to their Instagram account, despite having enabled 2fa. It was suspected hackers intercepted the 2fa code sent via SMS to access the account.

Account hijacking can result in the loss of hacked accounts and unauthorized access to account data, including messages, location data, and documents. When users are unable to recover their accounts, their work is put on hold, partially or fully.

Account hijacking can result in the loss of hacked accounts and unauthorized access to account data, including messages, location data, and documents. When users are unable to recover their accounts, their work is put on hold, partially or fully.

In one incident handled by JOSA, a victim's Facebook account was compromised, and attackers transferred ownership of a page with many followers to their own account. The victim was not able to log in to their own account, and page administrators lost administrative privilege on the page. In another incident submitted to CyberHub-AM, an Armenian journalist could not perform his work after his Facebook account was hacked.

In Ukraine, the Meta Business Manager of a prominent Ukrainian media organization was hacked, after which hackers renamed Facebook pages, edited posts, and deleted administrators. As a result, the page's owners lost access to it.

In Serbia, a local media organization had their YouTube channel taken over by an unknown actor. Hackers changed the recovery contacts and the channel's details, including the name and profile photo. The organization could not post or access any of their videos on the channel, which they had used for years to publish video materials. They were afraid that they had lost all their content on YouTube.

Hacked accounts can also be used to post content to manipulate audiences or harm the reputation of an organization or individual. In two cases in Armenia, the accounts of a journalist and the media expert of a human rights organization were hacked, after which hackers posted pro-ISIS content. The expert was unable to access Facebook and banned from administering pages and publishing ads campaigns. The journalist's account was blocked for 30 days.

Even attempts that are not politically motivated, when successful, can be detrimental to the work of civil society. In Mexico, SocialTIC received 10 requests from different people about WhatsApp accounts that were taken over in similar ways. Victims received a notification after receiving local and international calls that their accounts were being used on another device. The accounts were stolen and then set up on another device, on which 2fa was enabled. With 2fa enabled, accounts cannot be recovered unless they are first suspended by WhatsApp. These stolen accounts were then used to extort money transfers from family members and people close to the original account holders. The victims felt stressed and overwhelmed by the loss of their daily communication, as well as by the repercussions that could result from being falsely associated with criminal behavior. They have since regained access to the accounts and enabled 2fa.

Basic security hygiene can go a long way in preventing the compromise and loss of accounts. Users should use **strong, unique passwords; should not click on suspicious links; and should rely on a more secure 2fa method**. Rather than SMS, users should enable 2fa using a **trusted authenticator app or a hardware token**. Where possible, messengers such as Signal, WhatsApp, and Telegram should also have 2FA enabled. When alerted about attempts to hack into their accounts, users should change their passwords and log in to their accounts to end any sessions from devices and locations they do not recognize. At-risk users should consider **using disappearing messages on messaging apps**. Automatically deleting messages after a fixed amount of time can limit the amount of information compromised in the event of an attack. 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. Finally, in case it is impossible to regain access to an account, users should **ensure no important data is only accessible through one account**. For more security hygiene recommendations, please refer to Internews' SaferJourno Chapter 2, "Account Security."

Interception

Civil society and media also face government deployment of interception technologies to monitor communications and internet traffic. In the past, internet traffic was generally unencrypted, allowing governments to censor specific content or target people based on what they were viewing or saying online. In 2023, most Internet traffic is now encrypted, so such "deep packet inspection" has ceased to be effective; instead, governments trying to control online behavior will monitor web traffic and either block connection to particular websites or monitor behavior on public websites.

Governments also deploy International Mobile Subscriber Identity (IMSI) Catchers, also informally known as "stingrays," which intercept phone calls and messages by pretending to be a cell phone tower.

Governments also deploy International Mobile Subscriber Identity (IMSI) Catchers, also informally known as "stingrays," which intercept phone calls and messages by pretending to be a cell phone tower. In 2020, three civil society organizations in Mexico found 21 active IMSI catchers.[50] Law enforcement in the United Kingdom and the United States are known to use IMSI catchers during protests;[51] for example, US law enforcement used IMSI catchers to spy on Black Lives Matter protesters.[52]

Interception can also be conducted via direct access to telecommunication networks. In many countries, such access is mandated by law. Russia's System of Operative Investigative Measures (SORM) requires telecom providers to install equipment that enables the authorities to directly access their customers' phone calls, messages, and data.[53] Various regimes in Central Asia also follow this model.[54] Rather than direct access, India requires telecommunications companies to install surveillance equipment at subsea cable landing stations and data centers.[55]

To protect against interception of their internet traffic, civil society should **only visit websites using HTTPS and use encrypted communication apps like WhatsApp or Signal for both messaging and calling**, as traditional phone calls and SMSes are not secure. Using end-to-end encrypted apps can also prevent IMSI catchers from capturing the content of these messages. During protests, activists can avoid being tracked by IMSI catchers by switching off their mobile phones or putting them in airplane mode.[56]

Online harassment and gender-based violence

NGOs, human rights defenders, journalists, and activists around the world regularly face forms of online harassment that range from doxing, hateful attacks, and smear campaigns to gender-based violence and death threats. Attacks often happen or peak at times of protests, elections, political turmoil, and other events where civil society's watchdog role is even more essential. Perpetrators of online harassment often aim to silence civil society and media. Harassment can result in the disruption of activities, decreased credibility of the target, and increased risk of physical violence. It also takes a mental health toll on victims, increasing their stress and anxiety.

Attacks often happen or peak at times of protests, elections, political turmoil, and other events where civil society's watchdog role is even more essential.

In 2019, "HKLEAKS," a coordinated campaign "conducted by professional actors in alignment with Chinese state interests,"[57] doxed the personal information of pro-democracy activists in Hong Kong. Actors launched the attack at the height of a movement protesting the adoption of a bill allowing for the extradition of fugitives to mainland China. Websites that used different "HKLEAKS" domains exposed targets' personal information, such as date of birth, phone numbers, personal addresses, and pictures. According to Citizen Lab's investigation of "HKLEAKS," the campaign began in August 2019 and continued until mid-2021, at which point most of the campaign's targets – journalists, protesters, and activists – had either been arrested or gone into exile.[58] The government crackdown on protests and the law's enactment in 2020 have resulted in the shrinking of Hong Kong's civic space – shuttering political parties, NGOs, media outlets, and unions.[59]

In Mexico, one of the most dangerous country for journalists in the world, Article 19 documented 696 attacks against the press in 2022. Of these attacks, 196 occurred in the digital sphere, with threat actors most often relying on threats, intimidation, and harassment to target Mexican journalists.[60] For example, Vincente Serrano, the director of the digital outlet Sin Censura, received threatening messages that contained homophobic language in September 2022.[61]

Women, minorities, and LGBTQ+ communities are the target of most attacks and the most vicious forms of harassment. 2022 research by SMEX, a digital rights NGO working in West Asia and North Africa (WANA), determined that threat actors disproportionately dox vulnerable groups and individuals, including women, human rights defenders, dissidents, minorities, and LGBTQ+ people.[62]

In a case submitted to JOSA, a threat actor impersonated a women's rights defender in Jordan on Facebook, publishing her personal photos. She was concerned that the impersonation could lead to extortion, defamation, bullying, and harassment, which may affect her reputation and that of her organization.

In Mexico, SocialTIC documented the case of a woman in Mexico who provides support to human rights defenders that became the victim of online harassment herself. The attackers created a false Instagram profile with a link inviting people to buy content on OnlyFans; the link directed those who clicked on it to a website with blurred content and a message saying users would have to pay to see it. The scammers were then able to steal the payment information from people who attempted to buy the content. The victim only discovered the false profile when she received messages from her contacts.

Threat actors continue to develop new techniques and improve existing ones to harass and smear their victims. A May 2023 UN report titled "Human rights impacts of new technologies on civic space in South-East Asia" described the different techniques of state-sponsored trolling:

Trolling takes many forms, including the use of bots or automated messaging software to deliver defamatory messages, disseminate manipulated video or audio content, and spread social media memes alleging misbehavior or affiliation with criminal organizations. Organized and coordinated efforts utilize tools made available by social media platforms such as micro-targeting of advertising and personalization of news feeds. Sophisticated operations are increasingly skilled at manipulating social media algorithms that promote contentious and polarizing content that amplify the effect of trolling.[63]

The impact of harassment campaigns can be particularly devastating for women and LGBTQ+ communities.

The impact of harassment campaigns can be particularly devastating for women and LGBTQ+ communities. According to a 2021 report by the Syrian Female Journalist Network (SFJN), Syrian women human rights defenders and journalists who experienced digital violence suffered not only from psychological distress but also physical symptoms that included shortness of breath, fatigue, dizziness, and migraines. The violence also led to the further exclusion of women from the public sphere.[64]

Members of civil society and journalists at risk of digital harassment can take action to reduce the risk and effects of being targeted. For specific strategies, those at risk can reference PEN America's Online Harassment Field Manual and Chapter 7 of Internews' SaferJourno resource.

While members of civil society can **configure their privacy settings on social media to minimize the exposure of their personal information**, social media platforms should also do more to protect them. This is particularly necessary in authoritarian and challenging contexts where state actors and those affiliated with them are often responsible for these types of campaigns. Technology companies need to invest more in trust and safety teams and the operations of their platforms, as well as ensure that their content moderators are linguistically diverse to cover different languages and dialects. The distribution of content moderators should be proportionate to the number of users in each country where the tech company operates. These companies should work with targeted communities to develop features that can help users stay safe online and make existing features more accessible.

Targeting of websites

State actors, hacker groups motivated by political agendas, and cybercriminals are known to target the websites of media groups and NGOs using cyberattacks like defacement, DDoS, hacking, and backdoor access.

Websites of Armenian groups, for instance, have been targeted by attacks originating from Azerbaijan on several occasions.[65] These attacks have escalated during the armed conflict between the two countries that saw Azerbaijan seize the disputed Armenian enclave of Nagorno-Karabakh.[66]

In an October 2022 case brought to CyberHub-AM, Azerbaijani hackers broke into the network of an Armenian web hosting company and defaced 218 websites, including those of NGOs and human rights groups. Several of the organizations' websites went offline for a week. That same month, Azerbaijani threat actors hacked three websites belonging to the Union of Informed Citizens, an NGO working to promote democracy and human rights. In April 2023, the organization's YouTube channel was also hacked. Access to both their websites and YouTube account has since been restored.[67]

Attackers also target media groups and organizations in retaliation for critical coverage. In Mexico, operators of a new media website approached SocialTIC about an incident of a DDoS attack. Following the publication of an article about corruption, the site received a flood of requests and then became inaccessible. As a result, the website was not available for the outlet's regular communication activities, and the target audience was unable to stay informed and read its coverage.

There is also evidence that some governments are purchasing specialized tools to conduct attacks against websites. For instance, in 2014, the Nigerian government spent US$2m on software with DDoS capabilities.[68]

Attacks against websites hinder the dissemination of content and information, preventing organizations and media groups from accomplishing their mission of informing the public. To

avoid these types of attacks or lessen their impact when they happen, organizations need to **regularly update their websites, install relevant security plug-ins, and utilize mitigation services** such as firewalls and DDoS protection (e.g., Cloudflare or Project Shield). Organizations should also **choose a hosting provider that consistently applies security patches** to its systems. For websites, **keeping regular backups is essential** to be able to recover data in case it gets deleted or in case a previous state needs to be recovered. Sometimes, hosting providers or device manufacturers automatically create backups, which is the most convenient option. If not, **it is best to create new backups weekly** or at least monthly, and store them securely, so that the backups themselves don't become a target.

Platform censorship

Platforms' content moderation policies and practices also hinder civil society organizations' and media outlets' efforts to publish and disseminate content and information, reach audiences, and inform the public.

In the reporting period, Threat Labs responded to incidents that included restrictions on the Instagram of a Ukrainian organization that evacuates animals from war zones, Instagram's removal of a Jordanian queer activist's photo of a historical postcard for violating the platform's community guidelines on "nudity and sexual activity," and a human rights activist in Serbia whose account was restricted for three months after constant reports by other users.

Platform restrictions include the removal of content for violating community guidelines or local laws, suspending or taking down accounts, removing ads, and restricting the reach of certain types of content without the knowledge of users (also known as shadow banning). Platform restrictions can also prevent users from using certain features in the first place, such as running ad campaigns or publishing posts.

Over the past decade, platforms have been facing increased scrutiny over their content moderation policies and the implementation of these policies. Platform accountability falls short for many various reasons, including the lack of diverse and adequately trained content moderators, bias, the increasing role of algorithmic content moderation using non-diverse training datasets, and bowing to the censorship demands of governments.

Platform accountability falls short for many various reasons, including the lack of diverse and adequately trained content moderators, bias, the increasing role of algorithmic content moderation using non-diverse training datasets, and bowing to the censorship demands of governments.

In Turkey, for instance, activists, journalists, and voices critical of the government are routinely censored by platforms[69] that are complying with the country's draconian laws.[70] Platforms are also censoring anti-government content in Vietnam, with Facebook reportedly agreeing to shield Communist Party officials from criticism.[71] Advocacy can address this kind of censorship. If an individual user or organization believes they are being unfairly targeted by this kind of censorship, they could try reaching out to the platform directly, or through an intermediary, such as the Access Now Helpline.

Device seizure

In addition to the use of spyware and phishing tactics, the physical seizure and search of devices remains a serious threat that infringes on the privacy of activists, journalists, human rights defenders, and organizations.

In an incident reported to JOSA in Jordan, a queer activist was called in for interrogation where officials seized their phone overnight, subsequently obtaining access to the passcode. The arrest came following a hate and incitement campaign on social media against the human rights initiative they are part of, resulting in extreme stress and worry about potentially being detained. The initiative halted its planned activities as a result of the arrest and device seizure.

Russian law enforcement is known to search the phones of protesters. During anti-war protests in March 2022, videos emerged of police officers stopping people and demanding access to their phones, screening their messages.[72]

In Tunisia, during a spate of arrests targeting critics of President Saied, officials seized the phones of some activists and journalists, with police later using WhatsApp and Signal conversations during interrogations.

Similar tactics were also documented in India and Tunisia. After revoking the constitutional autonomy of the Jammu and Kashmir territory, the Indian government has imposed restrictions on freedoms of expression and assembly, the freedom of movement, and conducted arbitrary detentions.[73] During raids targeting journalists, activists, and political leaders, officials commonly confiscate devices.[74] In Tunisia, during a spate of arrests targeting critics of President Saied, officials seized the phones of some activists and journalists, with police later using WhatsApp and Signal conversations during interrogations.[75]

Those concerned about device seizure should **utilize disappearing messages on messaging apps**. Automatically deleting messages after a fixed amount of time can limit the amount of information compromised if a device is seized. Compartmentalization, or using a separate device for high-risk work, also limits the damage, but this comes with an obvious extra cost and inconvenience.

If a device has been seized (particularly if it has been taken out of sight), its owner should **assume the data on the device is compromised**, especially if the adversary was able to unlock it. The safest way to keep using the device is to **perform a factory reset and use another device to log the seized device out of all accounts** that had been on the phone. For more information about digital safety while traveling and device seizure, refer to the Internews SaferJourno guide "Safe Travels: Digital Security When Traveling on Assignment."

Conclusion

In an increasingly unstable world, the role of civil society and media is essential to hold those in power to account, protecting democracy, and documenting human rights violations and humanitarian crimes.

Yet, as demonstrated in this report and the corresponding country-specific Digital Threat Landscape reports, the scale and scope of digital threats civil society and the media face worsen in tandem with geopolitical instability and with major events such as elections, coups, protests, and conflicts. Additionally, advancements in technology and the constant shifting in threat actors' techniques and tactics make it more challenging for civil society to navigate digital threats and mitigate their online and offline impacts.

Spyware, phishing attacks, interception, and device seizures pose a risk to sensitive information, which can threaten the safety of civil society organizations, human rights defenders, journalists, and their networks and sources. Attackers often use extracted information in criminal cases, doxing, and smear campaigns. Online harassment, particularly on social media, has a mental health toll on those targeted, with a disproportionate impact on women and LGBTQ+ communities. Attacks on websites and social media account hacks also prevent organizations from disseminating their content and informing the public. Finally, platform censorship remains a challenge to civil society, hindering efforts at disseminating information and knowledge.

To withstand these threats and mitigate their most serious impacts, civil society organizations and the media need support to implement security measures. This requires knowledge, human resources, and financial resources. In some cases, basic knowledge, such as how to protect accounts and avoid becoming a victim of phishing, can go a long way in preventing attacks. Oftentimes, however, affected organizations need in-house experts and investment in protection tools such as DDoS protection (for which there are several free options for NGOs), secure storage systems to protect their work, and modern devices that continue to receive security updates.

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. Dedicating resources to the detection and analysis of these threats allows for this deeper understanding. For more information on the threats faced by civil society and journalists, Internews and their partners have created Digital Threat Landscape Reports for Armenia, Brazil, Mexico, Serbia, and Ukraine. These resources can be found on the Internews' Technology Resources webpage.

Acknowledgements

Since 2021, Internews has worked with seven Threat Labs to respond to incidents affecting the digital security of civil society and media organizations around the world. The data collected through incident response 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 can complete their important work safely and effectively. In total, this project supported Threat Labs in responding to over 200 digital security incidents and in publishing over 60 educational resources through their websites and social media platforms.

This report would not have been possible without the following Threat Labs:

Conexo, an organization with a Latin American reach that seeks to connect best practices and technical solutions with activists and journalists in risk areas who are constantly struggling to adopt new technologies to ensure and develop a better job.

CyberHub-AM, an IT support hub and a Threat Lab for Armenian civil society – NGOs, human rights defenders, activists, journalists, and independent media.

SHARE Foundation, an organization who works to advance human rights and freedoms online and promote positive values of an open and decentralized internet, as well as free access to information, knowledge and technology.

MariaLab, an independent nonprofit 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.

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.

Digital Security Lab Ukraine, an organization working to help Ukrainian journalists, human rights defenders, and public activists solve problems in digital security, as well as promote the realization of human rights on the Internet by influencing government policy in the field of digital rights.

Jordan Open Source Association, a non-profit based in Jordan whose mission is to promote openness in technology and to defend the rights of technology users in Jordan.

Endnotes

[1] McCorvey, J.J. "Tech layoffs shrink 'trust and safety' teams, raising fears of backsliding efforts to curb online abuse." NBC News. February 10, 2023. https://www.nbcnews.com/tech/tech-news/tech-layoffs-hit-trust-safety-teams-raising-fears-backsliding-efforts-rcna69111.

[2] "What is a Backdoor Attack?" Check Point. Accessed October 19, 2023. https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/what-is-a-backdoor-attack/

[3] "What Is Doxing?" Fortinet. Accessed October 19, 2023. https://www.fortinet.com/resources/cyberglossary/doxing

[4] "Interception Attacks." NordVPN. Accessed October 19, 2023. https://nordvpn.com/cybersecurity/glossary/interception-attacks/

[5] "Malware." Malwarebytes. Accessed October 19, 2023. https://www.malwarebytes.com/malware

[6] "What is Social Engineering?" IBM. Accessed October 19, 2023. https://www.ibm.com/topics/social-engineering

[7] Ibid.

[8] "Malware."

[9] "What is a threat actor?" IBM. Accessed October 19, 2023. https://www.ibm.com/topics/threat-actor

[10] "What is two-factor authentication?" Windows. Accessed October 19, 2023. https://www.microsoft.com/en-ww/security/business/security-101/what-is-two-factor-authentication-2fa

[11] "What is zero-click malware, and how do zero-click attacks work?" Kaspersky. Accessed October 19, 2023. https://usa.kaspersky.com/resource-center/definitions/what-is-zero-click-malware

[12] "Malware."

[13] "Freedom in the World 2023." Freedom House. Accessed October 19, 2023. https://freedomhouse.org/report/freedom-world/2023/marking-50-years

[14] Shahbaz, Funk, Brody, Vesteinsson, Baker, Grothe, Barak, Masinsin, Modi, Sutterlin eds. "Freedom on the Net 2023," *Freedom House*, 2023, freedomonthenet.org.

[15] The Continent. Issue 133. September 2, 2023. https://www.thecontinent.org/_files/ugd/287178_d7a1370f1ba14866826753085e64b43d.pdf

[16] "Burkina Faso." Freedom House. Accessed October 19, 2023. https://freedomhouse.org/country/burkina-faso

[17] "Burkina Faso: Ex-president Kabore released from house arrest." Al Jazeera. April 7, 2022. https://www.aljazeera.com/news/2022/4/7/burkina-faso-ex-president-kabore-released-from-house-arrest

[18] "UN 'deeply troubled' by Burkina media clampdown." Africanews. July 4, 2023. https://www.africanews.com/2023/04/07/un-deeply-troubled-by-burkina-media-clampdown//

[19] "Radio station silenced by Burkina Faso's military must be allowed to resume broadcasting, says RSF." Reporters Without Borders. August 16, 2023. https://rsf.org/en/radio-station-silenced-burkina-faso-s-military-must-be-allowed-resume-broadcasting-says-rsf

[20] Grewal, Sharan. "Ten years in, Tunisian democracy remains a work in progress." Brookings. January 22, 2021. https://www.brookings.edu/articles/ten-years-in-tunisian-democracy-remains-a-work-in-progress/.

[21] Boussen, Zied and Malek Lakhal. "Tunisia in the wake of the referendum: A new divisive Constitution." Arab Reform Initiative. August 23, 2022. https://www.arab-reform.net/publication/tunisia-in-the-wake-of-the-referendum-a-new-divisive-constitution/

[22] "Tunisia: Prosecution of journalists is a serious violation of press freedom." Article19. June 14, 2022. https://www.article19.org/resources/tunisia-prosecution-of-journalists-is-a-serious-violation-of-press-freedom/

[23] Aymen. "A new blow to freedom of expression in Tunisia." AccessNow. March 28, 2023. https://www.accessnow.org/a-new-blow-to-freedom-of-expression-in-tunisia/

[24] Silva, Cedê. "Bolsonaro leaves disastrous legacy as term comes to an end." The Brazilian Report. January 1, 2023. https://brazilian.report/society/2023/01/01/bolsonaro-disastrous-legacy/

[25] Buschschlüter, Vanessa and Katy Watson. "Amazon rainforest: Deforestation in Brazil at six-year low." BBC News. August 3, 2023. https://www.bbc.com/news/world-latin-america-66393360

[26] Tirado, Felipe. "Brazilian election: Jair Bolsonaro set to lose but his legacy will be harder to remove." The Conversation. September 28, 2022. https://theconversation.com/brazilian-election-jair-bolsonaro-set-to-lose-but-his-legacy-will-be-harder-to-remove-190862

[27] "Brazil." Reporters Without Borders. Accessed October 19, 2023. https://rsf.org/en/country/brazil

[28] Huntley, Shane. "TAG Bulletin: Q4 2022." Google Threat Analysis Group. January 25, 2023. https://blog.google/threat-analysis-group/tag-bulletin-q4-2022/

[29] Trevelyan, Mark. "Russia crosses new lines in crackdown on Putin's enemies." Reuters. April 21, 2023. https://www.reuters.com/world/europe/russia-crosses-new-lines-crackdown-putins-enemies-2023-04-21/

[30] Zarembo, Kateryna. "Civic Activism Against Geopolitics: The Case of Ukraine." Carnegie Europe. November 30, 2022. https://carnegieeurope.eu/2022/11/30/civic-activism-against-geopolitics-case-of-ukraine-pub-88485

[31] Aimé, Felix. "APT28 leverages multiple phishing techniques to target Ukrainian civil society." Sekoia Blog. May 17, 2023. https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/

[32] "About Apple threat notifications and protecting against state-sponsored attacks." Apple. August 22, 2023. https://support.apple.com/en-us/102174

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

[34] Kirchgaessner, Stephanie et al. "Revealed: leak uncovers global abuse of cyber-surveillance weapon." The Guardian. July 18, 2021. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

[35] Srivastava, Mehul and Kaye Wiggins. "India hunts for spyware that rivals controversial Pegasus system." Financial Times. March 31, 2023. https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9

[36] "Pegasus Infection of Galina Timchenko, exiled Russian Journalist and Publisher." Citizen Lab. September 13, 2023. https://citizenlab.ca/2023/09/pegasus-infection-of-galina-timchenko-exiled-russian-journalist-and-publisher/

[37] Harwell, Drew et al. "Biden administration blacklists NSO Group over Pegasus spyware." The Washington Post. November 2, 2021. https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/

[38] DiMolfetta, David and Aaron Gregg. "U.S. blacklists spyware companies, citing security threats." July 18, 2023. https://www.washingtonpost.com/national-security/2023/07/18/entity-list-spyware-intellexa-cytrox/

[39] Feldstein, Steven and Brian (Chun Hey) Kot. "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." Carnegie Endowment for International Peace. March 14, 2023. https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

[40] Mazzetti, Mark and Adam Goldman. "Ex-U.S. Intelligence Officers Admit to Hacking Crimes in Work for Emiratis." The New York Times. September 14, 2021. https://www.nytimes.com/2021/09/14/us/politics/darkmatter-uae-hacks.html

[41] Srivastava, "India hunts for spyware that rivals controversial Pegasus system."

[42] Marczak, Bill et al. "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware." Citizen Lab. December 16, 2021. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

[43] "Two European spyware firms added to US export blacklist." The Associated Press. July 18, 2023. https://apnews.com/article/spyware-cytrox-intellexa-blacklist-exports-surveillance-technology-6dfd45c27f48f71b8e662326073003c8

[44] Patrucic, Miranda and Kelly Bloss. "Life in Azerbaijan's Digital Autocracy: 'They Want to be in Control of Everything.'" Organized Crime and Corruption Reporting Project. July 18, 2021. https://www.occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything

[45] "About Apple threat notifications and protecting against state-sponsored attacks."

[46] "IBM Security X-Force Threat Intelligence Index 2023." IBM. Accessed October 19, 2023. https://www.ibm.com/reports/threat-intelligence.

[47] Scott-Railton, John. "Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society." Citizen Lab. February 23, 2017. https://citizenlab.ca/2017/02/nilephish-report/

[48] "Phishing attacks using third-party applications against Egyptian civil society organizations." Amnesty International. March 6, 2019. https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/

[49] "Iran: State-Backed Hacking of Activists, Journalists, Politicians." Human Rights Watch. December 5, 2022. https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians

[50] "Mexico: Freedom on the Net 2023." Freedom House. Accessed October 19, 2023. https://freedomhouse.org/country/mexico/freedom-net/2023#footnote21_zfw2q3e

[51] Goodwin, Bill. "Police secrecy over 'IMSI-catcher' mass surveillance of mobile phones." ComputerWeekly.com. July 2, 2020. https://www.computerweekly.com/news/252485535/Police-secrecy-over-IMSI-catcher-mass-surveillance-of-mobile-phones

[52] Zetter, Kim. "How Cops Can Secretly Track Your Phone." The Intercept. July 31, 2020. https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/

[53] Satariano, Adam et al. "When Nokia Pulled Out of Russia, a Vast Surveillance System Remained." The New York Times. March 28, 2022. https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html

[54] "Private Interests: Monitoring Central Asia." Privacy International. November 2014. https://privacyinternational.org/sites/default/files/2017-12/Private%20Interests%20with%20annex_0.pdf

[55] Heal, Alexandra. **"**India's communications 'backdoor' attracts surveillance companies." Financial Times. August 29, 2023. https://www.ft.com/content/adf1cbae-4217-4d7d-9271-8bec41a56fb4

[56] "How IMSI catchers can be used at a protest." Privacy International. May 5, 2021. https://privacyinternational.org/explainer/4492/how-imsi-catchers-can-be-used-protest

[57] Fittarelli, Alberto and Lokman Tsui. "Beautiful Bauhinia: "HKLeaks"– The Use of Covert and Overt Online Harassment Tactics to Repress the 2019 Hong Kong Protests." Citizen Lab. July 13, 2023. https://hdl.handle.net/1807/128586

[58] Fittarelli and Tsui. "Beautiful Bauhinia."

[59] "Hong Kong: Freedom in the World 2022." Freedom House. Accessed October 19, 2023. https://freedomhouse.org/country/hong-kong/freedom-world/2022

[60] "Mexico: Voices Against Indifference." Article19. March 28, 2023. https://www.article19.org/resources/mexico-voices-against-indifference/

[61] "Mexico: Freedom on the Net 2023."

[62] "Doxxing of Residential Information Targeting Vulnerable Groups: Online and Offline Harms." SMEX. February 8, 2022. https://smex.org/report-doxxing-of-residential-information-targeting-vulnerable-groups-online-and-offline-harms/

[63] "Human rights impact of new technologies on civic space in South-East Asia." Office of the United Nations High Commissioner for Human Rights. May 2023. https://www.ohchr.org/sites/default/files/documents/issues/civicspace/OHCHR-TECHCS-SEA2023.pdf

[64] Abrougui, Afef and Rula Asad. "Syrian Women Journalists and Human Rights Defenders in the Digital Space: Risks and Threats." Syrian Female Journalist Network. 2021. Accessed October 19, 2023. https://media.sfjn.org/en/digital-safety-is-a-right/

[65] "Armenia: Freedom on the Net 2023." Freedom House. Accessed October 19, 2023. https://freedomhouse.org/country/armenia/freedom-net/2023

[66] Gunter, Joel. "Deserted Nagorno-Karabakh reveals aftermath of lightning-fast Armenian defeat." BBC News. October 3, 2023. https://www.bbc.com/news/world-europe-66995976

[67] "Armenia: Freedom on the Net 2023."

[68] Roberts, Tony et al. "Mapping the supply of surveillance technologies to Africa: case studies from Nigeria, Ghana, Morocco, Malawi, and Zambia."

[69] Pahwa, Nitish. "Elon Musk Didn't Just Do Turkey's Bidding. Censoring for Strongmen Is Now a Pattern." Slate. May 15, 2023. https://slate.com/technology/2023/05/elon-musk-turkey-twitter-erdogan-india-modi-free-speech.html

[70] "Turkey: Freedom on the Net 2023." Freedom House. Accessed October 19, 2023. https://freedomhouse.org/country/turkey/freedom-net/2023

[71] Dien Nguyen An Luong. "Meta cozies up to Vietnam, censorship demands and all." .coda. September 28, 2023. https://www.codastory.com/authoritarian-tech/vietnam-censorship-facebook/

[72] Dasgupta, Sravasti. "Moscow police 'stopping people to go through their phones' amid anti-war protests." The Independent. March 8, 2022. https://www.independent.co.uk/news/world/europe/ukraine-moscow-protests-phones-war-b2030786.html

[73] "India: Repression Persists in Jammu and Kashmir." Freedom House. August 2, 2022. https://www.hrw.org/news/2022/08/02/india-repression-persists-jammu-and-kashmir

[74] Inzamam, Qadri and Haziq Qadri. "'Meant to Intimidate': Months After Police Raids, Kashmir Human Rights Groups Remain Dormant." The Intercept. July 26, 2021. https://theintercept.com/2021/07/26/india-kashmir-human-rights-nia/

[75] Ben Ismail, Zeïneb. "Kais Saied: jeopardizing rights and freedom." Inkyfada. August 22, 2023. https://inkyfada.com/en/2023/08/22/threats-rights-freedom-kais-saied-tunisia/