CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

# Defending Politically Vulnerable Organizations Online

SEAN BROOKS

CLTC WHITE PAPER SERIES

# Defending Politically Vulnerable Organizations Online

SEAN BROOKS

JULY 2018

CLTC
Center for Long-Term
Cybersecurity

CENTER FOR LONG-TERM CYBERSECURITY

# Contents

# Acknowledgements

The Center for Long-Term Cybersecurity (CLTC) would like to thank the following individuals for their expertise, feedback, and contributions to this document: Daniel Bedoya Arroyo, Michael Carbone, Arturo Carrillo, Patricia Cartes, George Conard, Masashi Crete-Nishihata, Catherine Crump, Ester Eriksson, Luis Fernando Garcia, Camille Francois, Eva Galperin, Lucia Gamboa, John Gershman, Eleni Glessiou, Jesse Goldhammer, Keith Hiatt, Michael Kleinman, Alexa Koenig, Josh Levy, Kristin Lin, Tord Lundstrom, Bill Marczak, Matt Mitchell, Vern Paxson, Xiao Qiang, Melissa Romaine, Lobsang Gyatso Sither, John Scott-Railton, Alissa Starzak, Eli Sugarman, Collin Sullivan, Aaron Rieke, Trevor Timm, Cynthia Wong, Nicole Wong, Chris Worman, and Harlan Yu.

In particular, CLTC would like to express appreciation to Ron Deibert, Eric Sears, and Alex Stamos for making this work possible.

Special thanks to Betsy Cooper, Allison Davenport, Chuck Kapelke, Jonathan Reiber, and Steven Weber of CLTC for their feedback and contributions to this report.

# Executive Summary

This paper provides an overview of online threats to civil society organizations and individuals—including non-governmental organizations, journalists, and activists—that are targeted for political purposes, and it explores the ecosystem of resources available to help these organizations improve their cybersecurity. The report describes different methods commonly used to attack "politically vulnerable organizations," and it identifies gaps in support resources that must be filled to ensure these organizations can securely carry out their missions online.

Politically vulnerable organizations, and civil society at large, are underinvesting in cybersecurity as attackers continue to expand their offensive capabilities. These organizations face a number of resource constraints that limit their access to expertise and technology, while their adversaries—including governments, hate groups, and private-sector spyware companies—employ increasingly sophisticated techniques to disrupt their services. But more often, politically vulnerable organizations are victimized by simple attacks that take advantage of their aging or poorly configured technical infrastructure.

While a range of organizations have sprung up to assist global civil society with cybersecurity, their efforts are primarily focused on advocacy and analysis, rather than providing tangible support for organizations in need. Some training and specialized tools are available, but these are often offered without appreciation for politically vulnerable organizations' political, organizational, cultural, or social contexts and capabilities. Direct technical assistance is rare. While some organizations have developed strong models for protecting politically vulnerable organizations against particular attacks, the scale of technical response is not capable of meeting the breadth of the need. In part, this is because most direct technical assistance is concentrated on supporting organizations in the midst of an emergency, while little support is available to effectively and affordably build organizations' resilience to cybersecurity risks on a long-term basis.

The report describes a range of research questions that should be pursued to help politically vulnerable organizations build their cybersecurity capacity and build resistance to a variety of online attacks. In particular, more work must be done to better understand the state of politically vulnerable organizations' technology practices, and to establish broadly-accepted methods for evaluating the quality of technical assistance. At the heart of the issues identified in this report lies a critical question of scale. As civil society organizations become increasingly reliant on the internet to pursue their missions, what methods of response can be effectively scaled to support those organizations who might be targeted for political purposes?

# Introduction

For individuals and organizations involved in political advocacy, cybersecurity threats are no longer abstract or isolated incidents, but are an increasingly common reality of operating in the digital world. Civil society has always been under attack from ideological, political, and governmental opponents who seek to silence dissenting opinions, but the widespread adoption of connected technologies by the individuals and organizations that make up civil society creates countless new means and methods of attack.

The cybersecurity threats facing civil society are as varied as the organizations themselves, and part of what makes these threats so insidious is that they can increasingly be carried out by actors with limited purchasing power and low levels of technical sophistication. High-profile, costly attacks, such as a $1 million zero-day exploit sent in 2016 to an activist in the United Arab Emirates, make up only one corner of a broad threat landscape that includes phishing emails, troll campaigns, and government-sanctioned censorship.[1] For example, in Thailand, the range of cybersecurity threats against political dissidents includes:

- Normalized mass surveillance by the government;
- Censorship under pro-royalist laws;
- Information gathering about activists' social media habits through spoofed Facebook and Google login pages; and
- An army of citizen informants searching for and reporting online conduct, such as comments critical (or even neutral) of the monarch.[2]

Attacks against civil society are often carried out by governments, political opponents, or radicalized individuals and organizations, and the targets for these attacks are wide-ranging. Over the past two years in Mexico, targets of spyware attacks have ranged from human rights and legal aid organizations to the young child of a journalist to the then-president of Mexico's Senate.[3,4] Cyberattacks affect civil society in even the most developed countries, including the United States: in 2016, the Democratic National Committee was the target of a Russian phishing attack that saw its servers compromised and private emails released to the public in the lead-up to the 2016 election.[5]

While civil society institutions may take rudimentary steps to protect themselves, such as installing firewalls and anti-virus software, these organizations largely lack the technical ability or capital to establish robust protections against cyberattacks.[6] Despite the prevalence of these attacks, cybersecurity is simply not seen as a priority for civil society actors.

This report highlights the large disparity between the technical capabilities of politically vulnerable organizations and of those who oppose them. The paper begins with an overview of the threat landscape facing politically vulnerable organizations. It then catalogs the types of attacks they face, discussing what types of attacks are most common as well as prominent examples of each of these attacks. Next, the paper reviews the organizations that support cybersecurity in civil society and the types of assistance they offer. Finally, the paper concludes with observations about the support resources available to help politically vulnerable organizations improve their cybersecurity, along with an overview of further research objectives in this area. The report's appendix provides a reference to many of the organizations working to defend the internet as a safe home for free expression and assembly.

## POLITICALLY VULNERABLE ORGANIZATIONS

This paper is focused on threats to politically vulnerable organizations, a subset of global civil society. The focus is on organizations that are attacked because of the political nature of their work. Politically vulnerable organizations may be the target of governments, criminals, hate groups, hacktivists, and many other threat actors, and they may be targeted for many different reasons. The term "politically vulnerable" is not intended to define an organization as inherently weak, but rather to highlight that they may be subject to attack for expressing minority or politically unpopular opinions.

## METHODOLOGY

This paper relies heavily on information and context gained from over 30 interviews with active members of organizations supporting politically vulnerable organizations, and from an open-source review of the work of more than 100 organizations (the full list of which can be seen in Appendix B). While online attacks against civil society have been well documented by many academic institutions, scholarship on the ecosystem of organizations attempting to protect civil society's use of the internet is rare. As a result, this paper often draws from broader surveys about civil society's use of technology in order to make inferences about practices within politically vulnerable organizations. Those observations are supported by the information collected in our interviews, but also point to the need for further research about the state of politically vulnerable organizations' cybersecurity practices.

# The Threat Landscape Facing Politically Vulnerable Organizations

Civil society organizations have always been defined by their missions. Most are run as charitable endeavors or in the public interest, and as a result, they generally have limited resources. This creates a substantial resource asymmetry between states and large private institutions, and the organizations who serve as their watchdogs. This asymmetry has persisted online, and a number of critical threats have emerged as civil society has come to rely heavily on connected technologies as a tool to amplify their voices and reach their constituencies.[7]

Some segments of civil society are particularly vulnerable to aggressive actors because the nature of their work makes them political targets. This section reviews how politically vulnerable organizations and people, such as political dissidents, journalists, environmental defenders, and human rights advocates, have been targeted by state, hacktivist, and criminal organizations seeking to disrupt their operations, restrict their messages, and even cause them physical harm.

## CIVIL SOCIETY IS A SOFT TARGET

Technically immature organizations share a wide variety of vulnerabilities that criminals, repressive governments, and hacktivists can exploit.

The Citizen Lab *Communities @ Risk* report describes some key findings on the state of civil society cybersecurity:[8]

- *In the digital realm,* [*Civil Society Organizations*] *face the same threats as the private sector and government, while equipped with far fewer resources to secure themselves.*
- *Counterintuitively, technical sophistication of malware used in* [*attacks on CSOs*] *is low, but the level of social engineering employed is high.*
- *Digital attacks against CSOs are persistent, adapting to targets in order to maintain access over time and across platforms.*
- *Targeted digital threats undermine CSOs' core communications and missions in a significant way, sometimes as a nuisance or resource drain,* [*and,*] *more seriously, as a major risk to individual safety.*
- *Targeted digital threats extend the 'reach' of the state (or other threat actors) beyond borders and into 'safe havens.'*

The broad asymmetry between attackers and defenders online is unsurprising; politically vulnerable organizations lack resources and are therefore particularly under-protected. This problem is not unique to politically vulnerable organizations. Many public and private organizations have underinvested in cybersecurity and have become soft targets for criminals and other bad actors.[9] Online attackers have continued to develop their offensive capabilities, exacerbating the mismatch. The primary theme of CrowdStrike's *2018 Global Threat Report* was the increasingly blurred line between the attack capabilities of state-sponsored and non-state threat actors, as the advanced tools developed by states have begun to leak out of their secure enclaves.[10] For its *Communities @ Risk* report, The Citizen Lab interviewed targeted organizations and found that many of the victims knew they had underinvested in security, but considered their core mission needs to be a more important use of their funds. Those same organizations also cited a lack of education and awareness as the cause for failing to adopt better security practices. A program manager for a human rights organization told The Citizen Lab,

> *We don't have a unified network with all our field offices . . . so we don't have the same enterprise level of security and capacity there. . . .* [*The field offices and NGO partners*] *have to face a range of threats that are from the physical world as well.*[11]

Existing data and research on nonprofit IT capabilities supports The Citizen Lab's conclusion that politically vulnerable organizations face the same sorts of risks and vulnerabilities as companies and governments, but have fewer resources to defend themselves. On average, small nonprofits (defined as organizations with 15 or fewer employees) have one IT person on staff, and the ratios of IT staff to non-technical staff are significantly worse in larger organizations.[12] Given that cybersecurity jobs only account for 11 percent of all IT jobs,[13] the small IT staffs of most nonprofits are unlikely to provide much, if any, cybersecurity support. A 2016 survey found that 71 percent of not-for-profit organizations had not conducted a cybersecurity vulnerability assessment in the past year, nor did they maintain an incident response plan.[14]

## A Month of State-Sponsored Attacks in August 2016

In August 2016 alone:

- The Bahraini government employed Netsweeper filtering software to block access to human rights websites, news outlets critical of the government, and websites with content critical of Islam.[15]
- The Mexican government targeted a scientist studying the effects of soda consumption on obesity with inflammatory text messages—including a lie that the scientist's daughter was in critical condition after being in a car accident.[16]
- The United Arab Emirates attempted to exploit an iPhone zero-day vulnerability with an estimated worth of a million dollars to spy on a single activist by hijacking the phone's camera and microphone.[17]

Few comprehensive studies exist to substantiate the degree to which politically vulnerable organizations and individuals—and nonprofits more broadly—invest in their IT and security capabilities. The few surveys that have been conducted generally focused on journalists. Their findings draw into sharp focus the potential impact of low investment in digital security. In a Freedom House survey, Mexican journalists cited hacking of personal accounts and online surveillance as the risks of greatest concern for journalists operating online.[18] Given that 70 percent of the journalists surveyed had been either physically threatened or attacked because of their work, one might expect a more substantial investment in cybersecurity by this community. Nevertheless, the same survey found a low adoption of encrypted communications, VPNs, and other technologies that might be used to prevent the surveillance that facilitates these physical attacks.

Another report found that, while many journalists were aware of cybersecurity measures they could use to defend their communications, many did not use them in their most sensitive conversations with sources.[19] The journalists cite their sources' lack of technical ability or the lack of tools available to those sources as the biggest barriers to adopting cybersecurity measures in their communications. Echoing the Citizen Lab *Communities @ Risk* report's findings, the journalists' mission-driven need to conduct interviews outweighed their concerns about digital security threats. Because the mission extends beyond the boundaries of the organization, the ability to secure critical communications channels is often dependent on individuals or communities of interest who are even more resource-constrained, such as journalists' sources or members of communities served by a nonprofit. Extending cybersecurity protections outside the boundaries of an organization is a challenge for even sophisticated private and government actors, and politically vulnerable organizations often lack the skills to train and deploy technologies to partners or individuals with whom they need to collaborate.

The 2017 WannaCry ransomware attack is a prime example of the havoc that can be wreaked on organizations with out-of-date software.[20] Under-resourced organizations, like local libraries, were victimized by ransomware attacks that took advantage of common, unpatched software vulnerabilities.[21] Increased connectivity has put politically vulnerable organizations directly in the path of some of the most sophisticated offensive cybersecurity operations in the world.

In the context of a broader cybersecurity workforce shortage problem, nonprofits face intense competition to attract IT talent. Some studies have estimated that the global cybersecurity labor market (including both the public and private sectors) will face a shortage of 1.8 million workers by 2022.[22] Given that 92 percent of nonprofits surveyed in a 2010 study by the John Hopkins Center for Civil Society Studies indicated a lack of funds to be a primary barrier to increasing their IT capacity, it would be unrealistic to expect that these organizations have the capital to compete with the private sector to attract cybersecurity talent.[23] Nonprofits have traditionally used their missions to attract staff at sub-market rates, but they would still be challenged to court the number of individuals needed to make up this gap.

In addition to a lack of funds, nonprofits face a variety of technological barriers to strengthening their cybersecurity infrastructure. In a survey from Johns Hopkins University, 59 percent of respondents indicated that a lack of IT staff is a barrier to taking full advantage of information technology. Still, that technology is broadly recognized to be a critical component of civil society's ability to function, as 88 percent of nonprofits surveyed indicated that technology is integrated into "many" or "all" aspects of their operations. Almost all nonprofits surveyed maintain websites, and almost all (98 percent) reported that they use information technologies in their programming or service delivery. More recent IT budget surveys suggest this trend has substantially accelerated as nonprofits have come to better understand the potential utility of technology for their organizations.[24] Nonprofits have begun to hire more professionals with skills to manage large data sets, which points toward a particular need to protect sensitive information particularly as many nonprofits hold and generate information about marginalized, at-risk, or underserved individuals.[25]

A more recent 2018 report from the Public Interest Registry surveyed over 5,300 NGOs and demonstrated that, while nonprofits invest in information technology to conduct mission-critical activities, information security investment continues to be low.[26] However, the report does illustrate that the increase in the adoption of security controls like end-to-end encryption by major technology platforms has benefited NGOs who might not otherwise be actively deploying cybersecurity measures; such NGOs indirectly benefit when they rely on the major technology platforms for services. The findings from the Public Interest Registry report include:

- Ninety-two percent of NGOs have a website, and 44 percent of those surveyed use Wordpress.
- Ninety-three percent have a Facebook page (and 30 percent have a Facebook group), 77 percent have a Twitter profile, 56 percent have a LinkedIn page, and 50 percent have an Instagram page.
- Eighteen percent use messaging apps to communicate with supporters and donors, 64 percent use Whatsapp, and 58 percent use Facebook messenger.

    - While both WhatsApp and Facebook messenger provide end-to-end encryption, only two percent of those surveyed use the more explicitly security-oriented Signal messaging app.[27]
    - Roughly the same percentage of NGOs use the Android operating system as use iOS on their mobile devices (38 percent vs. 34 percent). Apple's default messenger is encrypted (though only for communications with other iOS users) and Android's is not.
- Forty-five percent of NGOs use customer relationship management ("CRM") software to track donations and manage communications with donors and supporters. Of those, 64 percent use a cloud-based CRM software.
- Forty-one percent of NGOs use encryption technology to protect their data and communications.
    - Thirty-two percent use encryption to protect organizational data, 29 percent to protect donor information, 23 percent to protect email privacy, and 13 percent to protect mobile privacy.
- The vast majority of NGOs surveyed (80 percent) use the Windows operating system, with many organizations finding Apple hardware to be beyond their budgets. While both operating systems have known security flaws, older versions of Windows are more heavily targeted by hackers.

Beyond low cybersecurity investment, mission-driven organizations often lack the expertise at the staff level to fend off even the most basic online threats. Connectivity is crucial for organizations with decentralized operations or a wide volunteer base. As a result, organizations establishing such connectivity often circumvent many of the basic steps that more technically mature organizations would take to preserve system integrity (like using formal identity systems or multi-factor authentication) in order to establish an online presence quickly.

Politically vulnerable organizations also seem to have an uneven understanding of online threats. A recent survey by The Collaboration on International ICT Policy in East and Southern Africa asked East African civil society organizations how they perceived phishing, surveillance,

## Cybersecurity in East African Civil Society

A recent survey of East African civil society organizations by The Collaboration on International ICT Policy in East and Southern Africa revealed:[28]

- Most organizations perceived phishing, surveillance, hacking, or censorship as "very low" or "moderate" threats.
- Most received digital security training, but did not pass their knowledge on to new recruits.
- Organizations had a high adoption rate for firewalls and anti-virus software.
- Organizations had a low adoption rate for encrypted communications and password managers.

hacking, or censorship as threats to their operations. The vast majority responded they found those threats to be "very low" or "moderate." But civil society organizations in Uganda, whose internet infrastructure was the best developed of all countries surveyed, responded nearly universally that these threats were "high" or "extreme." The same report found that most organizations surveyed had at some point received digital security training, but new staff rarely received that training. The adoption of anti-virus software was common (over 80% of the organizations surveyed in each region). Cloud storage among those organizations surveyed was most frequently used by Ugandan organizations (80%) and least frequently by Burundian organizations (22%). Other cybersecurity tools, like communications encryption and password managers, were very uncommon (less than 30% of organizations in all countries surveyed, and even down to 0–10% in some countries).[29]

This survey highlights an interesting trend: greater connectivity leads to more reliance by civil society on the internet, which in turn exposes these organizations to greater risk. Given that internet connectivity is more available in the developed world, politically vulnerable organizations that are likely to become newly reliant on the internet in the coming years are likely to be in underdeveloped or fragile states. This points to a potential tradeoff for politically vulnerable organizations in the developing world and the Global South: are the benefits of an increased online presence worth the introduction of new security risks?

NIST's Cybersecurity Framework describes a basic tiered system for measuring the sophistication of organizations' cybersecurity preparedness.[30] The lowest tier, "Partial," describes organizations with a reactive, informal cybersecurity risk management process, low awareness of cybersecurity risk, and little ability to coordinate with external partners on cybersecurity issues. Our research suggests that many politically vulnerable organizations struggle to maintain even a "partial" cybersecurity program, as they lack sufficient staff capacity to undertake regular risk assessment.

## TYPES OF ATTACKS FACED BY POLITICALLY VULNERABLE ORGANIZATIONS

Civil society generally is underprepared for cyberattacks. AccessNow's 2012 *Global Civil Society at Risk* report describes a series of threats that took advantage of civil society's poor security posture.[31] The following section explores how the threat landscape has evolved since the AccessNow report's publication, describing twelve types of cyberattacks and documenting examples of each. Some of the categories, such as "Malware" and "Advanced Persistent Threats," are intentionally broad in order to capture the many types of threats that take advantage of similar vulnerabilities in organizations' systems, practices, and knowledge.

*Cyberattacks on politically vulnerable organizations often have real-world impact. They facilitate intimidation, arrests, and physical assaults.*

Many closed communities exist to share information about new variants of malware and other forms of online attacks. Some of these communities, like ShadowServer or the National Vulnerabilities Database, are open source (the code is free and available for review and contributions by the online public), but they require a significant amount of technical sophistication from users. This is one of the many ways in which more highly resourced organizations in government and the private sector are able to apply more proactive, flexible approaches to cybersecurity, as they are more adept at sharing information about new threats and modifying their practices or systems in response. Politically vulnerable organizations, on the other hand, are often unable to take advantage of knowledge about these new security threats and deploy appropriate mitigations.

Some of these attacks, such as malware or DDoS attacks, are strictly technical in nature. Others, such as compelled data disclosures and takedown demands, are not technical in nature. Still others, like phishing and trolling attacks, use a hybrid approach, combining non-technical intelligence gathering and harassment techniques with technical capabilities to expand the scope and sophistication of the attack.

## Vandalism

Website defacements can interfere with individuals' access to services or disrupt the reputation of an organization. For example, a recent Wordpress vulnerability allowed hackers sympathetic to ISIS to deface a wide variety of websites, replacing the sites' content with messages supporting the Islamic State.[32] Nonprofits were particularly vulnerable because their sites were in many cases out of date and they lacked the expertise to mitigate the damage in a timely fashion.[33]

## Phishing

Research detailing online attacks against civil society demonstrates that phishing is the most damaging type of attack organizations are likely to face.[34] Phishing, along with more targeted spear-phishing attacks,[35] use deceptive emails, websites, or other fraudulent forms of electronic communication to lure targets into providing sensitive information like passwords and user credentials. Phishing attacks are relatively easy to execute, often requiring only an email account or a web page cloned from a familiar service; such attacks may be an entry point for more sophisticated attacks that leverage compromised credentials or privileged endpoints. Because outdated or under-protected politically vulnerable organizations' networks are easy to compromise, account credentials or information garnered from phishing attacks can grant attackers broader access than they could gain from networks protected with multi-factor authentication, intrusion prevention systems, or better password discipline.

Many broad phishing attacks have been waged against civil society organizations as a way to test for vulnerable systems on a massive scale. State-sponsored phishing attacks have been documented in Egypt, Qatar, and Nepal, and repeated phishing attacks contributed heavily to the sustained campaign against U.S. political parties during the 2016 elections.[36]

## Operation Kingphish

Amnesty International's investigation of the "Operation Kingphish" attacks, which used a wave of phishing attacks to compromise the communications of organizations, describes a wide range of individuals targeted with links that pointed to fake Google login pages designed to steal their account information:

> *Most identified targets were activists, journalists, and labour union members. While some of targets had published critical opinions about Qatar's international affairs, the majority of identified targets were affiliated with organisations supporting migrant workers in Qatar. Interestingly, a significant number of them are from Nepal, which is one of the largest nationalities amongst migrant workers in Qatar, and a country that has featured prominently in the migrant worker narrative on Qatar.*

The breadth of the targets of the attacks is significant, as they span a large portion of civil society's voices on immigrant labor in Qatar. The attackers cultivated relationships with targets through private chats using the fake persona "Safeena Malik," for whom they developed fake Facebook, LinkedIn, and Twitter accounts with hundreds of connections. While the true identity of the attackers was never revealed (it is suspected they may have been contractors hired by the Qatari government), the attacks were successful in gaining intimate access to the data and communications of a wide range of advocates working on behalf of, and often beside, vulnerable immigrant laborers.[37]

## Malware

Malware, or malicious software, comes in many forms, including Trojans, worms, viruses, and spyware. Generally, malware is used to target individuals and specific devices, though it may create entry-points into networks for other attacks. Malware ranges widely in scope and complexity, and the execution of attacks can require a variety of user interactions, from opening a malicious document to more indirect methods of getting users to accept arbitrary code (such a link encouraging users to download software that prevents antivirus software). Malware attacks on politically vulnerable organizations have been widely documented, but some notable examples include attacks on those sympathetic to Tibetan sovereignty, Mexican advocates of a soda tax, and critics of ISIS.[38] Governments have contracted with commercial spyware companies like Hacking Team and NSO Group to target politically vulnerable organizations and political adversaries.[39] The Italian Ministry of Economic Development stripped Hacking Team of its export license after the company was found to be selling surveillance technology to the Egyptian government, and the US Bureau of Industry and Security has fined actors for selling filtering technologies to countries under strict export controls.[40, 41] But outside these notable examples, many of these intermediaries have not faced significant consequences for their work on behalf of governments.[42]

YOUR FILES ARE ENCRYPTED
Your photos, documents and other important files have been encrypted with unique key, generated for this computer.
NEXT

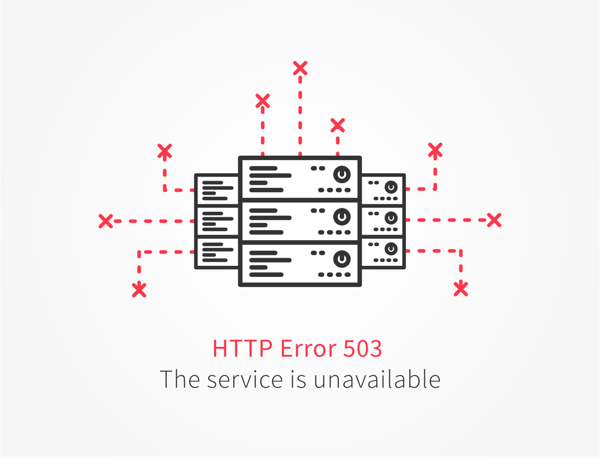
*Ransomware attacks often have high recovery costs, particularly for under-resourced organizations.*

Some malware attacks exploit previously unknown vulnerabilities ("zero-day" attacks) and are deeply concerning because they are difficult to prevent and expensive to use (in research hours or cost of purchase). In one example, a triad of zero-day exploits that were deployed to compromise a single human rights advocate in the United Arab Emirates was estimated to cost over $1 million.[43] Such attacks demonstrate that adversaries of civil society organizations are taking advantage of asymmetries in both financial power and technical sophistication to compromise politically vulnerable organizations.

The Citizen Lab *Communities @ Risk* report highlights that the technical sophistication of attacks against politically vulnerable organizations is often low.[44] But recent uses of aggressive zero-day exploits against journalists and human rights workers suggest that, as politically vulnerable organizations' cybersecurity improves, adversaries are likely to deploy more advanced weapons.

## Distributed Denial of Service (DDoS)

Denial-of-service attacks, which flood sites or services with malicious traffic in order to block legitimate requests for access, are one of the oldest known types of information system attacks. In recent years, distributed denial of service (DDoS) attacks, which send traffic at a single target from a variety of sources, have become increasingly powerful and common. Though many businesses exist to help organizations balance traffic loads in the event of such an attack, hackers have no shortage of sources of malicious traffic, and DDoS attacks continue to grow in size and scope.[45] DDoS continues to be a popular tool for criminals, hacktivists, and governments for censoring and disrupting civil society online.[46] Network-based malware like the Mirai botnet, which infects cameras, monitors, and other vulnerable "internet of thing" devices, are capable of sending massive amounts of traffic to politically vulnerable organizations' websites. The tools controlled by governments, meanwhile, present even more complex threats to the stability of sites and services: China's "Great Cannon" and the US's QUANTUM system can hijack legitimate web traffic both to deliver large volumes of pings to targets, and to deliver malware.[47]



*Sites under DDoS attacks are inaccessible to visitors.*

## Attacks on Website or Service Infrastructure

Simply having a public-facing website can expose organizations to attack. Attackers can use a variety of methods to hijack websites of civil society organizations to surveil visitors, expose sensitive data, or disrupt services. One possible type of attack is cross-site scripting, in which attackers run malicious code through a vulnerability in a public-facing website to attack visitors to that site. Another common method is SQL injections, which allow attackers to query a website's back-end database and reveal sensitive information. These attacks do not require the use of compromised credentials or breaking into a secured network, making them both difficult to detect for organizations without sophisticated security and hard to prevent without training and up-to-date secure web design. Actors motivated by anti-abortion sentiments recently used a SQL injection to attack the website of Planned Parenthood and extract employee data and other information that was later leaked online.[48]

### Man-in-the-Middle (MITM) Attacks

By compromising central pieces of the internet's shared security architecture or taking advantage of the vulnerabilities of low-security communications and websites, governments and other malicious actors can collect detailed information about individuals that visit civil society websites or can listen in on their communications. Man-in-the-middle attacks (MITM) often take advantage of websites with poorly configured Transport Layer Security (TLS), which secures the connection between an individual's computer and the website. Poor TLS configurations can allow attackers to surveil the activity of visitors to politically sensitive sites.

Another example of MITM attacks requires compromising the decentralized "trust architecture" of the web. Multiple instances have been documented of governments compromising certificate authorities (CAs), which issue certificates used to verify the ownership of web domains in TLS connections.[49] By compromising a CA, a government can place itself between the connection of a site and an individual's computer, or even can direct individuals to fake websites instead of to their desired destination. Compromised certificates allow for many types of attacks, including MITM attacks. For example: two popular Chinese browsers, Baidu and UC, initially deployed weak security to protect data they transmitted. As a result, researchers revealed that sensitive information was leaked by the Baidu browser, and that attackers could replace legitimate downloads with "arbitrary" (in other words: any software they want) code packages that could run malicious software.[50] An analysis of materials from the Edward Snowden disclosures similarly revealed data leakages due to poor transit security in the China-based UC Browser, which enabled US intelligence agencies (and their allies) to identify individuals' browsing behavior.[51]

### Advanced Persistent Threats (APTs)

After account credentials have been compromised or malware has made its way onto an organization's network, there is a chance for a single compromise to evolve into what is broadly called an "advanced persistent threat" (APT).[52] An APT is a sustained, embedded attack that strives to remain undetected, enabling surveillance, service disruptions, and data theft over a long period of time. Such attacks are sophisticated operations that often require ongoing management by attackers, but can result in the exfiltration of sensitive data, the disruption of networks and services, and other malicious actions. A notable recent example of an APT in action against a civil society organization was the months-long attack on the US Democratic National Committee and its affiliates, but other attacks of this type have been documented recently in Tibet, China, and beyond.[53]

### Infrastructure-based Attacks

Governments can take advantage of their privileged position to tap into layers of the internet not publicly accessible in order to conduct widespread surveillance.[54] They also have the power to compel service providers to shut off access to the internet across wide areas, often as part of an effort to limit civil unrest. Internet "blackouts" disproportionately hurt journalistic endeavors and other portions of civil society, though they can also often have unexpected consequences for the broader internet and economy.[55] Notable internet blackouts were documented in Egypt during the Arab Spring, but have also occurred (at a much smaller scale) in the United States.[56]

### Data Disclosure

While there are many technical means for governments to conduct surveillance on the internet, one of the easiest and most common forms of surveillance is to compel private service providers to disclose data about individuals, organizations, and communities. Many governments have used compelled disclosure (requiring a service provider to reveal user data via legal or political means) to surveil politically vulnerable organizations, and the chilling effect on free expression that results has been well-documented.[57] While many western nations have formal governance processes for compelled disclosure, more repressive regimes have begun to view private internet service providers and social media companies as easy vehicles for cataloging dissenting voices.[58] As politically vulnerable organizations begin to house more data themselves, they become significant targets for compelled disclosure requests as well.

### Takedown Demands and Internet Filtering

Similar to compelled data disclosures, takedown demands are another active but non-technical method of limiting civil society's ability to operate online. Using a variety of laws as justification, including rules on copyright, political and hate speech, blasphemy, and "lèse-majesté", governments can demand that service providers or social media companies remove posts found to be overly critical, controversial, or otherwise objectionable.[59]

Governments may also use their privileged position on the internet to deploy aggressive censorship and internet filtering campaigns, which can block access to politically vulnerable organizations' web pages or posts. China's "Great Firewall" is the best known example, but many other regimes have procured sophisticated filtering technology to flag individuals and organizations posting controversial content before blocking access to their websites.[60] Not all filtering is done explicitly by the government; many private companies accept draconian filtering rules as a precondition for operating within certain countries, and they conduct keyword and topic filtering on behalf of the state.[61]

## Trolling and Impersonation

Trolling encompasses a wide variety of threats toward organizations and individuals, from online harassment to “doxing” (publicly revealing individuals’ identities or sensitive personal information). In recent years, a number of criminal and government organizations have utilized automated troll armies (sometimes called “sockpuppets”) to invade controversial conversations on social media in order to influence public opinion. These sockpuppets, combined with leaks of sensitive or unflattering information obtained from other attacks, have become potent weapons for spreading disinformation and discrediting civil society organizations.[62] In many instances, governments have employed hundreds of operators to manufacture the appearance of broad social response online.[63] The Citizen Lab’s report on “tainted leaks” illustrates the power of adding fake or misleading information to leaked data in order to cause additional outrage and further damage the legitimacy of targeted organizations.[64] Trolling can include coordinated efforts to embarrass or frighten individuals by sending them a constant stream of abusive messages.[65] In other instances, individuals in high-profile positions at politically vulnerable organizations have had fake accounts impersonate them, seeking to damage their reputations.[66]

An active presence on social media is critical to many politically vulnerable organizations’ missions. But online engagement with the public also creates many opportunities for attacks by adversaries. By turning public opinion against targeted organizations, or by finding disgruntled individuals to serve as proxies, politically vulnerable organizations’ adversaries can facilitate reputational attacks that are decentralized and conceal their true origins.

These threats highlight the wide range of potential vulnerabilities that under-resourced public-interest organizations face. Not all of these threats will be equally applicable to all organizations, as attacks may vary depending on the mission, technical sophistication, and core constituencies of each target.

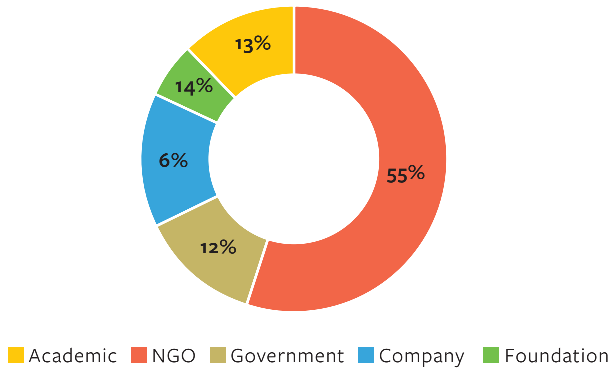
# The Organizational Ecosystem Supporting Civil Society Cybersecurity

A wide number of organizations work to mitigate, prevent, or draw attention to the various online threats to civil society. This section describes the range of support provided by those organizations, and includes an example along with each type of support provided (a full index of organizations reviewed for this report can be found in the Appendix). Since little work has been done on the specific types of support provided to politically vulnerable organizations, this section relies on interviews conducted with more than 30 experts, and on research on supporting cybersecurity in the broader not-for-profit sector.

In 2012, the Johns Hopkins Center for Civil Society Studies found that the 10-year growth of the nonprofit sector had surpassed the rate of the growth of GDP in the vast majority of countries reviewed. The pace of this growth was particularly notable in the developing world.[67] Given the limited resources traditionally available to these organizations for infrastructure beyond their mission-oriented work, the need for assistance with cybersecurity-related issues is likely to increase. A wide variety of organizations provide some sort of cybersecurity assistance to politically vulnerable organizations.

Of more than 100 such organizations reviewed for this report, more than half are non-governmental organizations (NGOs). Most of these are relatively small organizations (with fewer than 30 staff members), but some, including Amnesty International and the American Civil Liberties Union (ACLU), are large, established institutions. Government agencies, academic institutions, and private foundations make up nearly equal shares of the organizations providing support to politically vulnerable organizations.

TYPES OF ORGANIZATIONS SUPPORTING CIVIL SOCIETY

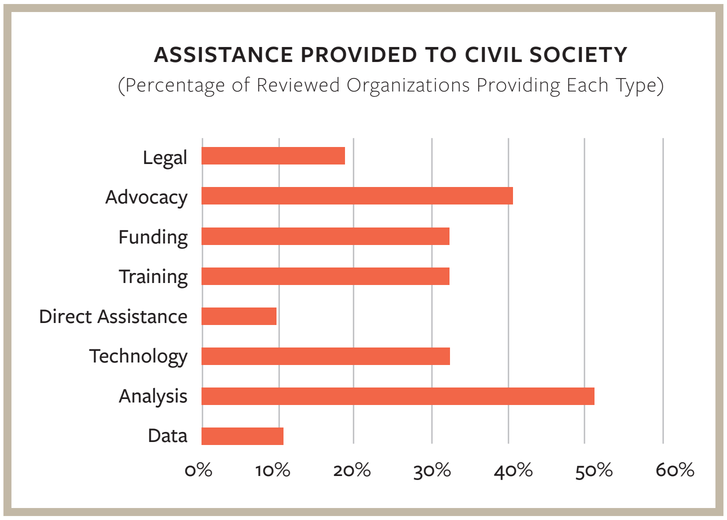


The government agencies (like the U.S. State Department) and foundations (like the MacArthur and Ford Foundations) that we reviewed are generally large, well-resourced institutions that have recently (within the last 10–15 years) emphasized supporting human rights online.

Academic institutions vary widely in their approach to these issues: some have programs dedicated to understanding threats to civil society online (like the Citizen Lab at the University of Toronto), while others have broader research agendas that touch on these issues (like the Berkman Center at Harvard University). Private companies comprise a small segment of the organizations providing assistance, and these range in size and capacity. Some of the companies that contribute to this space (such as Google and Cloudflare) do so only on a pro-bono basis; others (such as Greenhost and eQualit.ie) see civil society as a core component of their potential customer base.

## TYPES OF ASSISTANCE AVAILABLE TO CIVIL SOCIETY

CLTC's analysis identified eight types of cybersecurity assistance available to civil society organizations: Data, Analysis, Technology, Direct Assistance, Training, Funding, Advocacy, and Legal. Each of these general types of support is deployed through numerous different models and types of organizations. This section describes each assistance method in detail, including examples of organizations that provide that assistance and how they provide it. While many of the organizations offered multiple types of assistance to civil society, much of the support is concentrated in the analysis and advocacy space. Direct technical assistance or publishing data about attacks is rare.



The types of support the organizations reviewed provide to civil society can be summarized as follows:

- While many organizations are active in this space, the scale of the response pales in comparison to the scope of the threats to politically vulnerable organizations.
- Analytical reports, publications, and blog posts make up the bulk of assistance. Fifty-three percent of the organizations reviewed provide analysis; 40 percent engage in advocacy. These are the most popular offerings in the field.

- Funding, training, and technology development are the next most popular forms of assistance, with just over 30 percent of the organizations in the space providing one or both of those offerings.
- Other forms of assistance for politically vulnerable actors—legal assistance, direct technical assistance, and data collection and publishing—are offered far less frequently than analysis and advocacy efforts.

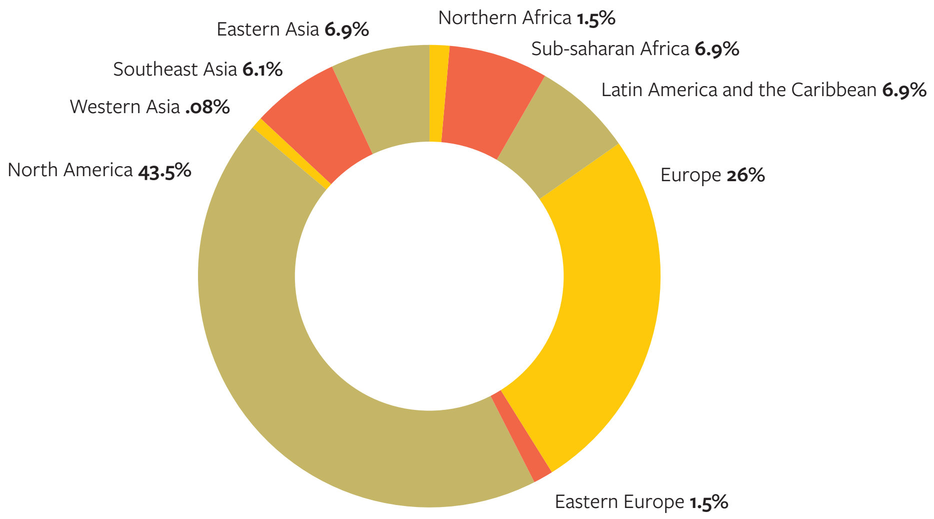
Politically vulnerable organizations exist in every country, and the scope of threats to the free and open operations of civil society online is massive. While there are many organizations active in this space, it is not nearly enough to support the vast security needs of global civil society, particularly as the online presence of politically vulnerable organizations continues to grow. New models, particularly for direct technical assistance, are needed to expand and complement the scale of the existing response to online threats.

Nearly 70 percent of the organizations reviewed are based in North America or Europe. Most of the organizations based in North America or Europe serve populations (or focus on issues) abroad. (This follows a somewhat predictable pattern of many rights- and development-oriented organizations, with the vast majority of organizations and institutions based in the West and focused on the developing world.) While this may reflect the more intensive needs of politically vulnerable populations in the developing world, the attacks documented in this report illustrate that politically vulnerable organizations based in the West may also face serious threats from foreign governments and sophisticated hacktivists as well.

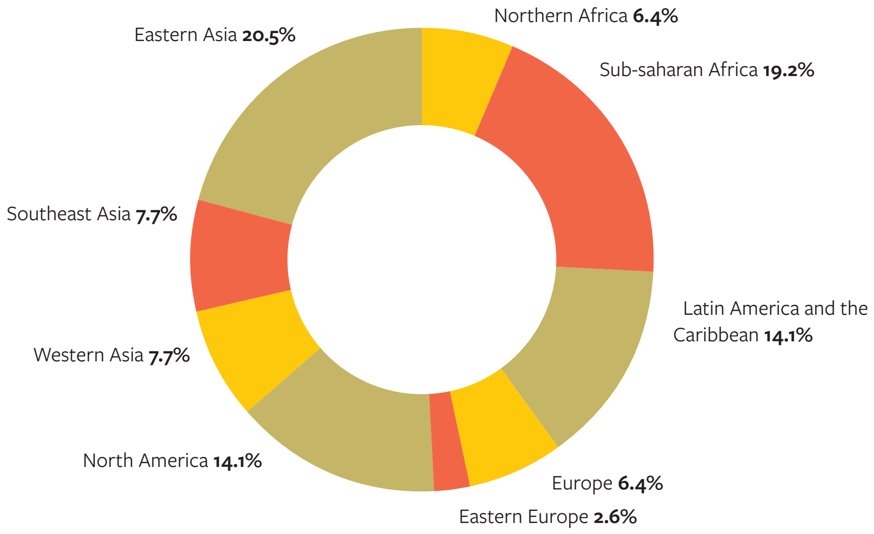
About 30 percent of the organizations identified in this review are located in the developing world. However, the assistance they provide is almost exclusively limited to advocacy, analysis, and training. The development of technology tools and the provision of direct assistance was notably absent from organizations in the developing world, suggesting that NGOs working in this space may themselves lack the technical sophistication to defend against potent cyberattacks. While training is often provided by NGOs in the developing world, it is more generally focused on development[68] issues, which include a wide range of technical topics beyond cybersecurity.

The following section details the different types of cybersecurity assistance available to politically vulnerable organizations through a short description, and some examples of organizations that provide that form of assistance. The examples are illustrative and should not be considered an endorsement of any particular provider of assistance.

### GEOGRAPHIC BASE OF ORGANIZATIONS REVIEWED, BY REGION



### SUPPORT ORGANIZATIONS SURVEYED: GEOGRAPHIC REGIONS SERVED BY ORGANIZATIONS REVIEWED (where specified)



## Analysis

By far the most common form of assistance provided to civil society, *analysis* reviews law, policy, attacks, government action, criminal organizations, and other actors in the space to inform policymakers, citizens, experts, and other audiences about the health of civil society online. Over half of the organizations reviewed provide some sort of analysis, often in addition to some other form of assistance (very few organizations reviewed provide analysis exclusively). Strong analysis is critical to justifying all other assistance methods, and is provided by NGOs, governments, academic institutions, companies, and foundations. The organizations reviewed provide a range of types of analysis, from policy briefs to in-depth, longitudinal studies of internet freedom. For example, technical analysis from Citizen Lab provided the technical groundwork for international outcry over aggressive surveillance by the NSO Group, an Israeli firm that provided tools to the Mexican government to spy on journalists covering their nation's efforts to pass a tax on sugary drinks.[69]

Some organizations notable for their analysis include:

- **The Citizen Lab:** A research lab based at the University of Toronto that investigates surveillance and cyberattacks targeted at activists and other politically vulnerable people. The Citizen Lab publishes papers describing incidents and methods, often in an attempt to identify the perpetrators. They also partner with a wide variety of organizations to provide technical analysis. Citizen Lab has produced research on attacks in Tibet, Egypt, Ethiopia, China, Mexico, Myanmar, Iran, and other nations.
- **Derechos Digitales:** A Latin American digital rights advocacy organization that provides analysis of legal, political, and corporate actions affecting the technology landscape and internet freedom.
- **The Open Technology Institute (OTI):** New America's technology think tank, OTI provides a wide range of legal and policy analysis focused on cybersecurity and internet freedom, as well as other technology policy issues. OTI has run a number of technology and advocacy projects, including analysis of high-level cybersecurity policy and the "Ranking Digital Rights" project.

## Advocacy

A complement to analysis, *advocacy* encompasses lobbying, coalition building, or other activities intended to sway public opinion, policy, law, private organizations' practices, or other institutional actions. Advocacy is the second most common form of assistance among the organizations we reviewed, with 41 percent of organizations providing advocacy on behalf of politically vulnerable organizations of some kind. The popularity of advocacy is unsurprising, as the vast majority of active organizations in the space are NGOs that pursue specific social outcomes. Most advocacy is targeted at governments, although private-sector companies are also a popular target, as they operate many of the internet's most popular services and shared infrastructure. Advocacy generally focuses less on technical details than on laws and policies that facilitate surveillance, censorship, and state-sponsored cyberattacks. However, some advocacy organizations, like the Electronic Frontier Foundation, bring a high level of technical sophistication to their analysis and advocacy positions. For example, based on the Citizen Lab's research on attacks on journalists in Mexico, Red en Defensa de los Derechos Digitales has led a large advocacy campaign to lobby lawmakers and inform Mexican citizens about the dangers of targeted mass surveillance.

Other examples of relevant organizations include:

- **American Civil Liberties Union:** The ACLU's Privacy and Technology and National Security programs have been strong, vocal advocates for policy change at many levels of American government on issues of mass surveillance and government use of spying technology. The ACLU combines its legal analysis and aid capabilities with a large activist and mobilization platform to advocate for changes through many channels.
- **Global Voices:** An NGO dedicated to promoting and amplifying commentary and analysis from bloggers around the world by providing a censorship-resistant platform for citizen journalists to publish their work.
- **Mozilla Foundation:** A nonprofit technology company with significant advocacy and policy-convening roles, the Mozilla Foundation promotes an "Internet Health" agenda that encompasses a wide variety of internet freedom, openness, and access issues.

## Funding

In recent years, the funding landscape for internet freedom has grown substantially, with more private and public grant-makers engaging as cybersecurity issues continue to affect a larger cross-section of their grantees. Funders include many of the traditional organizations that provide support to civil society: private foundations, government development agencies, and even some larger nonprofits. Grants available to politically vulnerable organizations to address cybersecurity issues range from small, emergency funds (such as the emergency fund at the Digital Defenders Partnership, which provides up to €10,000 (about $11,727 USD) to organizations under active threat, and the Open Technology Fund's Direct Financial Support grants, which offer up to $50,000 in rapid-response funding), to project-based funding (ranging from $5,000 from AccessNow to $900,000 from OTF, or even more from larger foundations), to significant initiative funding of cybersecurity writ broadly (such as the $65 million Hewlett Foundation Cyber Initiative, or the multi-million dollar Ford Foundation Internet Freedom program). Based on the reviewed organizations, funding is a more popular form of assistance than direct technical assistance, although funders are very focused on civil society's ability to utilize technology effectively. A variety of programs exist to improve the utilization of technology in nonprofits, government agencies, and politically vulnerable organizations, and cybersecurity is increasingly considered part of the portfolio of issues in need of support.

Given the importance of civil society organizations—particularly political opposition or watchdogs—in developing democracies, organizations that traditionally fund international development efforts have also begun to take interest in cybersecurity for politically vulnerable organizations. Government development agencies like USAID and the Swedish International Development Cooperation Agency (SIDA) have added "internet freedom" programs to their portfolios, though it is difficult to ascertain the extent of the cybersecurity-specific funding currently available through "ICT4D" programs.

While the funders identified in this review specifically provide grants for furthering civil society cybersecurity, the broader internet freedom funding space is very crowded. The Open Technology Fund has collected a list of organizations that provide funding for journalists, politically vulnerable organizations, and individuals related to internet freedom issues, including many rapid-response funders who focus on defending human rights workers and journalists under threat.[70] Most of the organizations that provide rapid-response services do not specialize in helping politically vulnerable organizations grow their cybersecurity capacity or respond to online threats. Instead, these organizations tend to focus on helping organizations with more general technology adoption, physical security, or assistance for staff detained by authorities.

Notable funders in the space include:

- **The Open Society Foundation:** A large foundation that funds open internet and cybersecurity-related programs through many of its initiatives, including those focused on government accountability, media and information, and rights and justice.
- **The MacArthur Foundation:** One of the largest private foundations in the United States, the MacArthur Foundation has a dedicated Human Rights program with a significant interest in the online security of civil society. MacArthur supports a number of high-profile projects in the internet freedom space, including the NetGain Partnership, Citizen Lab, and New America.
- **U.S. Department of State, Bureau of Democracy, Rights, and Labor (DRL):** The U.S. government's foremost supporter of democracy development abroad, DRL funds a broad

spectrum of development projects and supports global, bilateral, and multilateral foreign policy efforts. The Bureau houses the State Department's Internet Freedom program, which funds a number of censorship circumvention, technology development, and advocacy efforts globally.

## Training

Thirty-two percent of the organizations reviewed for this report provide training to politically vulnerable organizations and individuals to improve their operational security and practices. Training comes in many forms, including in-person events and the distribution of online guides and resources. Because many politically vulnerable organizations lack technical sophistication, training often focuses on basic information security literacy and practices, including adopting encrypted communications, spotting phishing emails, and utilizing private web browsing. Training usually includes a review of standard sets of concepts, tools, and practices, but is rarely tailored to the specific risks present in an organization. Many experts interviewed for this report complained about the state of cybersecurity training for politically vulnerable organizations, citing a lack of appreciation for organizations' context. Such context might alter organizations' threat models and make commonly recommended tools or techniques impractical or unsafe.

Most training materials have been developed by NGOs and academic organizations and are usually shared publicly, though it was suggested in many interviews conducted for this report that many guides have fallen out of date. Notable examples of well-referenced training materials include EFF's "Surveillance Self-Defense" guide, the Freedom of the Press Foundation's "Protect Yourself" page, and the "Security in a Box: Digital Security Tools and Tactics" guide developed by the Tactical Technology Collective.[71] The Citizen Lab has developed a tool to help individuals assess threats and deploy simple mitigations called "Security Planner."[72]

Some other notable organizations in the training space include:

- **Digital Defenders:** The Digital Defenders Partnership, sponsored by Hivos, is best known for its "Digital First Aid Kit" (now managed in partnership with RARENET). The First Aid Kit offers a detailed look at tools and best practices for recovering from a variety of cyberattacks.
- **Social TIC:** A Latin American NGO dedicated to providing a centralized repository of tools and guides for civil society actors. Tools cover a variety of topics (data, work management, etc.) and include a sizable privacy and security tool repository.
- **Freedom of the Press Foundation:** This press freedom advocacy and crowdfunding organization provides a number of digital security guides and tools for investigative media organizations, and also offers tailored trainings in digital security for a fee.

## Technology

Just under 30 percent of the organizations reviewed have developed cybersecurity or data gathering tools, services, browser add-ons or plugins, and systems for civil society and at-risk individuals. The tools range from substantial products with ongoing support and development, to small web plugins that increase the transparency of normally hidden web processes. Common functions of these tools include enabling individuals to hide their identities, securing or obscuring communications, and observing or reporting censorship or signal interference.

Training, advocacy, or direct assistance organizations regularly suggest that the politically vulnerable organizations they support use tools developed by the internet freedom community. The tools are, with very few exceptions, free and open-source. Such tools are generally updated through contributions and vulnerability assessments from a decentralized community of users. While the openness of these tools provides many security benefits (anyone can audit the code), updates are usually dependent on the original publishers, and contributions from external reviewers can be rare.[73]

Despite the availability of many free and open tools, at-risk individuals and organizations do not always find these tools to be useful or approachable. In general, the use of secured communications technology has increased, with marked jumps in recent years in the deployment of HTTPS and the use of encryption.[74] Yet the public (including civil society) has adopted security tools at an uneven rate. For example, other than a significant jump in the wake of the Snowden revelations in 2013, public usage of Tor's surveillance-circumvention and private browsing package has not gained a consistently larger audience.[75] At the same time, the encrypted messaging app Signal recently saw a 400 percent increase in installations.[76] PrivacyBadger, a third-party ad tracking blocker developed by EFF, recently surpassed one million installations. While it may be tempting to attribute the ease of use of Signal and PrivacyBadger to their success (compared to the relatively complicated Tor package), the usage of OpenPGP keys (personal keys for using the OpenPGP encryption standard, used to facilitate high-assurance and secure email and file exchanges) has continued to steadily increase without abatement.[77] This is surprising, because PGP is a relatively difficult technology to use compared to tools like Signal, and it has had a number of security vulnerabilities. However, the increase in keys does not necessarily translate into new users. While OpenPGP keys are disposable, once individuals no longer use a key, the key is not necessarily "revoked"—it no longer is used. So the stable "growth" in the number of keys may simply be a matter of a stable audience of OpenPGP users adopting new keys at a regular rate.

The reach of these tools is broad: the Open Technology Fund estimates that more than two billion people use the open-source security technologies it supports, including Tor, Signal, Qubes OS, Tails, and many others. However, it is unclear what percentage of politically vulnerable organizations have adopted these technologies. In a recent survey of politically vulnerable organizations in East Africa, most had adopted older information security tools like firewalls and anti-virus software, but few reported using more modern tools, like encryption for email or data.[78] A 2013 survey of Mexican journalists found similar patterns: 40 percent of the journalists reported using some basic security technologies (like anti-virus software) with some regularity, but fewer (less than 30 percent) had adopted more significant communications security technologies like transit encryption or anonymized browsing.[79] Most preferred to use non-technology mechanisms like codenames to conceal communications, or they opted to avoid technology altogether when conducting sensitive conversations.

The most common form of assistance that private companies reviewed for this report provide to politically vulnerable organizations is technology support. Companies like Cloudflare and Google have set up DDoS mitigation services for nonprofits under attack at greatly reduced

## Adoption of Cybersecurity Tools

Among all internet users and services:

- The use of secured web-based communications has increased in marked jumps, with broader deployment of HTTPS, end-to-end encryption, strong TLS (protocols that secure data in transit), and DMARC (which enables much strong email authentication and can reduce phishing attacks).
- In 2016, Signal, an encrypted messaging application, saw a 400 percent spike in installations.
- PrivacyBadger, an ad-blocking and online tracking prevention tool from the Electronic Frontier Foundation, surpassed one million installations in 2017.

In politically vulnerable organizations:

- There is little available data or research to illuminate whether recent trends in security technology adoption have applied to politically vulnerable organizations.
- Some surveys of civil society IT practices suggest that older security tools like firewalls and antivirus software are more commonly used than modern capabilities like end-to-end encryption, though the improved access to end-to-end encryption through popular apps like iMessage and Whatsapp may have helped.
- Some politically vulnerable individuals, particularly journalists, have a documented preference for avoiding technology for sensitive conversations, preferring to use codenames or speak offline.

prices or for free. Other companies—like SpiderOak, eQualit.ie, and Open Whisper Systems—have focused their market strategies on providing highly secure and privacy-enhancing tools, and occasionally highlight the use of their technologies by politically vulnerable organizations as proof of their security.

Significant technology providers in this space include:

- **Jigsaw:** A technology incubator at Alphabet that tackles geopolitical problems, Jigsaw developed the Project Shield service, a free DDoS mitigation service for civil society organizations at risk of attack.
- **The Tor Project:** Home of the "onion routing" surveillance-circumvention and private browsing package of the same name, the Tor Project is a nonprofit primarily supported by volunteers. It is also home to the Open Observatory of Network Interference, which tracks internet censorship.
- **SecurityFirst:** Developer of the open-source Umbrella app, which provides up-to-date cybersecurity information for at-risk users, organizations, and security trainers.

## Legal

Twenty percent of the organizations reviewed provide some sort of legal aid to politically vulnerable organizations, including pushing back against private or governmental legal actions related to internet freedom. Legal aid may come in the form of clinical support from law schools, amicus briefs from advocates, and other forms of direct or indirect client engagement that help with court filings, appearances, litigation, and review of critical documents. Notable organizations providing legal assistance to politically vulnerable organizations include:

- **The Electronic Frontier Foundation (EFF):** One of the leading and most influential internet freedom organizations, EFF provides a variety of advocacy, technology, and legal support to individuals and organizations across civil society.
- **Samuelson Law, Technology & Public Policy Clinic:** A clinic at the UC Berkeley School of Law, the Samuelson Clinic provides legal aid to politically vulnerable organizations and individuals on many technology and policy issues, and frequently takes on cases related to privacy and surveillance.
- **Amnesty International:** A major international human rights NGO providing a variety of assistance to human rights workers globally, Amnesty International maintains a significant legal fund and has defended individuals such as Chinese journalist Shi Tao, who was imprisoned after authorities compelled Yahoo to release Tao's emails, which included evidence he leaked a Communist Party document on media restrictions to Western press outlets.[80]

## Data Collection and Publishing

Roughly 11 percent of the organizations reviewed publish data related to attacks, takedowns, and trends that are relevant to the operations of politically vulnerable organizations and individuals online. The most commonly collected information relates to censorship and internet filtering. NGOs that publish data often do so as a part of a larger advocacy or watchdog effort, as they use the data to highlight trends and particular issues of note. Academic organizations more often publish raw information and high-level analysis, although some also contribute to advocacy-oriented projects. Data publishing efforts are often tied to analysis efforts, though the collection and hosting of data can be an entirely standalone service. For example, the Open Observatory of Network Interference (OONI) documents and analyzes network interruptions around the world, but its primary publishing mechanism is an open API and web interface for viewing the data, allowing other organizations to utilize their data for secondary research.

Hard data on the full extent of surveillance and cyberattacks conducted against politically vulnerable organizations is limited or non-existent, likely for a few reasons: the lack of a centralized reporting system, the difficulty for non-state entities to assess mass surveillance exercises, and the more subtle/covert nature of surveillance and related attacks. Some examples of data providers include:

- **Herdict**: A project supported by the Berkman Center that provides a user-driven platform for identifying web blockages as they happen, including denial of service attacks, censorship, and other types of online filtering.
- **GreatFire:** An organization focused on censorship circumvention in China, GreatFire provides ongoing data regarding domain and keyword blocking and filtering from behind the "Great Firewall" since 2011.
- **Lumen:** A database of a wide range of requests and demands to remove online content, run as a collaboration among law school clinics and the Electronic Frontier Foundation (EFF).
- **OpenNet Initiative:** A collaborative partnership between The Citizen Lab, Berkman Center, and SecDev Group aimed at "identifying, exposing, and analyzing Internet filtering and surveillance practices." Prior to 2013, the OpenNet Initiative published country-by-country data on internet blocking and filtering practices and targets. The Initiative has not published additional data since 2013.

## Direct Assistance

"Direct assistance" describes the provision of technical support to help politically vulnerable organizations recover from and prevent cyberattacks. Few organizations operate in this space, and those that do rely on the work of individuals who assist multiple organizations

simultaneously. Of more than 100 organizations reviewed, only nine offer some form of direct technical assistance to individuals or civil society institutions, and the scope of that assistance is relatively limited compared to the landscape of threats.

Direct assistance providers most often provide politically vulnerable organizations with support in fending off DDoS attacks, whether by helping manage pro-bono secure hosting and traffic management services from programs like Google Project Shield or Project Galileo, or paid services like those from Equalit.ie, Qurium Foundation, or Greenhost. Many direct assistance providers offer support against vandalism, malware, MITM, and phishing attacks. They also provide security and risk assessments to identify other areas of vulnerability. It is not clear based on public information whether these organizations specialize in particular attacks or forms of assistance, or whether they receive a disproportionate number of requests for assistance on any given topic.

A variety of direct assistance organizations promise to provide wide-ranging support, but the direct assistance community does not cover all the threats detailed in this report. None of the organizations reviewed provides support to counter harassment and trolling, and only a few offer secure design assistance to prevent web-based attacks. Those organizations that offer direct technical assistance also do not help manage takedown demands or compelled data disclosures. This is generally left to the legal assistance community, though many direct assistance organizations provide referrals to legal assistance organizations when a need is identified.

Many of these organizations structure their assistance as emergency response, but it is not well-defined what the scope of an "emergency" includes. Very few of the organizations describe publicly any limits on support that might exist after a certain time frame or cost is exceeded, nor do they make clear the duration of their availability to pro-bono clients. OTF's annual report provides the most comprehensive view on the range of services offered for emergency assistance: OTF's Rapid Response Fund can provide individuals and organizations with digital security audits, DDoS response and mitigation, secure email, and web hosting, monitoring, and resiliency during special events (elections, campaigns etc.), and VPN and other secure internet connections. Following attacks, OTF can provide forensic analysis, recovery of compromised websites, audits of presumably compromised services, and malware analysis.

The total value of emergency support received from OTF cannot exceed $50,000, and awards range on average between $5,000 and $25,000.[81] In 2015, OTF provided a total of $389,916 in services through its Rapid Response Fund.[82]

The technical infrastructure that direct assistance organizations offer to politically vulnerable organizations varies widely in scope and sophistication. Large companies, like Google and Cloudflare, offer full versions of their robust platforms that serve governments and large companies, providing a significant amount of service and security. Other direct assistance providers are limited in what kind of internal technology development they provide, and rely on open-source software to offer a suite of services to politically vulnerable clients. However, open-source software has its limitations. For example, Greenhost and RiseUp both rely on open-source mail servers to provide hosted email to civil society organizations. But, because those open-source packages do not have multi-factor authentication capabilities, neither Greenhost nor RiseUp offers MFA for hosted email accounts, a security control that is seen as deeply necessary for most high-risk users.[83] The gulf between the security capabilities of companies and NGO technical assistance providers illustrates an important point: subsidized service options for politically vulnerable organizations in need of substantial security are limited, particularly if the organizations do not wish to depend on large companies. This is not always the case—Qurium Foundation, for example, provides a series of significant security services at a reduced price for civil society customers—but in general, the bar for “good” security (i.e. capable of resisting sophisticated threats) is set high by large tech companies, and is difficult for NGOs or smaller companies to match.

Direct assistance organizations often work together to address multiple elements of complex compromises; for example, Qurium and Greenhost are OTF’s partners in providing rapid response support. Such collaborations expand each provider’s capabilities. But the direct assistance community’s ability to address more sophisticated, advanced threats is limited by the time and resources that politically vulnerable organizations can dedicate to investing in their own capacity. After an emergency is remedied, politically vulnerable organizations’ ability to invest in services or capacity building continues to be limited by their tight budgets and low internal expertise.

Notable providers of direct assistance include:

- **The Open Technology Fund:** An NGO supported by Radio Free Asia, this organization provides funding for technology services and tools, emergency grant funds for organizations under attack, and a network of technical staff to help provide emergency recovery services.

- **AccessNow:** A global internet freedom advocacy organization that maintains a "Digital Security Helpline" to provide 24/7 cybersecurity support to organizations under threat.
- **Frontline Defenders:** One of the original contributors to the Digital Defenders project and a major influence on the cybersecurity emergency response ecosystem, Frontline runs an emergency contact line for human rights defenders globally; this hotline operates in many languages and can provide a number of digital emergency response services. Frontline resources are referenced often in capacity-building toolkits like the Digital First Aid Kit.

# Conclusion

This paper highlights the disparity in technical capacity and economic resources between politically vulnerable organizations and their opponents, which are often large corporations and government entities with broad offensive capabilities. Politically vulnerable organizations are susceptible to a range of attacks, and so even less sophisticated governments can target oppositional organizations, often successfully, with simple attacks.

Many kinds of assistance are available to help politically vulnerable organizations ward off the simplest attacks. While a number of assistance organizations offer analysis and advocacy, few offer direct technical assistance to help fend off or respond to cyberattacks. Where direct assistance is available, it tends to focus on emergency response rather than longer-term capacity building. There are also many types of indirect assistance to help organizations protect against cyberattacks, including technology tools, funding, and legal aid. While such assistance can provide tools and strategies, politically vulnerable organizations often lack the capacity to use these resources effectively.

The effectiveness of these various mechanisms for assistance is uncertain. The nature of cyberattacks requires a multifaceted approach at all stages of intrusion. Ideally, steps would be taken to secure politically vulnerable organizations against cyberattacks before they happen, so as to render assistance during and after attacks less necessary. Realistically, monetary or technical assistance during and after attacks will always be a necessity, and analysis after attacks can be a helpful tool in learning and planning for the future. The most significant gap in the assistance ecosystem is direct technical assistance, and the limited IT departments and lack of cybersecurity specialists in these organizations makes this an urgent need.

Research areas that remain open and require attention include:

- Measuring and evaluating the number and method of attacks against civil society and politically vulnerable organizations, including how the threats are likely to change in the next 5-10 years with the proliferation of new technology;
- Developing profiles of threat actors and their likely attack methods;
- Understanding the current technical and operational cybersecurity practices of politically vulnerable organizations, as well as the types of assistance they require;
- Measuring effects of surveillance on the quality, volume, and diversity of free speech and assembly online, particularly for politically vulnerable organizations; and

- Studying the rate, duration, spread, and barriers to politically vulnerable organizations' adoption of tools, techniques, and policies, as well as the potential responses of threat actors.

Answering these questions will help ascertain whether or not models for assistance are improving politically vulnerable organizations' cybersecurity, and will help the organizations that provide assistance move beyond their current, reactive posture and provide assistance that preempts or anticipates new cyberattacks.

While the online threats to global civil society are significant, there is an emerging understanding within the internet freedom ecosystem about how to provide effective cybersecurity support to organizations struggling against potent adversaries. Lobsang Gyatso Sither, Digital Security Program Director at the Tibet Action Institute, said in an interview about his organization's collaboration with Citizen Lab:

> *In the "Targeted Threats" report, we saw 90% of the attacks used attachments. So, we had to do a campaign to inform the community about how to move away from attachments (we called it "Detached from Attachments"). It used humor, it used religion—a hyper-localized approach to digital security. The ideas, the framing, they had to be from the community. In this case, it was the Tibetan context of humor. It started with the way people really engage—not from a technical perspective, but a human one.*

The developing appreciation of what effective assistance looks like points to one of the greatest needs: new models for direct technical assistance. As detailed in this report, significant gaps remain in the support services available to help politically vulnerable organizations improve their cybersecurity. New models can help complement the existing work and expand its impact. In order to be successful, new direct assistance models will need the ability to:

- Provide support that appreciates the context of politically vulnerable organizations, and tailors support to match the risks and capabilities present in that context;
- Provide long-term support and partnership to organizations seeking to grow their own cybersecurity capacity over time;
- Scale the support provided to a wider population of politically vulnerable organizations; and
- Document and distribute lessons learned to inform and expand the capabilities of the broader ecosystem.

Politically vulnerable organizations will likely always have the scales tilted toward their adversaries. But if the community of organizations providing cybersecurity support can continue to grow and evolve, they will help advance the online safety and security—and the missions—of journalists, human rights organizations, NGOs, and other members of civil society for generations to come.

# Appendix: Organizations Supporting Civil Society Cybersecurity

This appendix is not an exhaustive list of organizations supporting politically vulnerable organizations' cybersecurity. It is a representative list of the diverse forms of assistance in the ecosystem, designed to serve as a guide for those seeking information about online threats to politically vulnerable organizations.

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| 7iber | NGO | Western Asia | Western Asia | Analysis<br>Training | https://www.7iber.com/ |
| AccessNow | NGO | Global | North America<br>Latin America and the Caribbean<br>Europe<br>Northern Africa<br>Eastern Asia<br>South Eastern Asia | Analysis<br>Direct Assistance<br>Funding<br>Advocacy<br>Legal | https://accessnow.org |
| American Civil Liberties Union | NGO | North America | North America | Analysis<br>Training<br>Advocacy<br>Legal | https://aclu.org |
| Amnesty International | NGO | Global | North America<br>Europe | Analysis<br>Training<br>Advocacy<br>Legal | https://www.amnesty.org |
| ASL19 | NGO | Western Asia | North America | Technology<br>Advocacy | https://asl19.org |
| Asociación por los Derechos Civile | NGO | Latin America and the Caribbean | Latin America and the Caribbean | Analysis<br>Legal | http://adc.org.ar/ |

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| Benetech | NGO | Global | North America | Analysis<br>Technology<br>Training | https://www.benetech.org/ |
| Berkman Center for Internet and Society | Academic | Global | North America | Analysis<br>Funding<br>Advocacy<br>Legal | https://cyber.harvard.edu/ |
| Bill and Melinda Gates Foundation | Foundation | Global | North America<br>Eastern Asia<br>Europe<br>Sub-Saharan Africa | Funding<br>Advocacy | http://www.gatesfoundation.org/ |
| Bloomberg Philanthropies | Foundation | Global | North America | Training<br>Funding<br>Advocacy | https://www.bloomberg.org/ |
| Briar Project | NGO | Global | | Technology | https://briarproject.org/ |
| Bytes for All | NGO | Eastern Asia | Eastern Asia | Analysis<br>Training<br>Advocacy | http://content.bytesforall.pk/ |
| Center for Democracy and Technology | NGO | North America<br>Europe | North America<br>Europe | Analysis<br>Advocacy<br>Legal | https://cdt.org |
| Center for International Media Assistance | NGO | Global | North America | Analysis<br>Training | http://www.cima.ned.org/ |
| Center for Internet and Society | NGO | Eastern Asia | Eastern Asia | Analysis<br>Advocacy | https://cis-india.org/ |
| Center for Internet and Society (Stanford) | Academic | North America | North America | Analysis<br>Legal | http://cyberlaw.stanford.edu/ |
| Citizen Lab | Academic | Global | North America | Data<br>Analysis<br>Training | https://citizenlab.org/ |
| CiviCERT | NGO | Global | Europe<br>North America | Technology<br>Training<br>Legal | https://civicert.org/ |

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| Collaboration on International ICT Policy for East and Southern Africa | NGO | Sub-Saharan Africa | Sub-Saharan Africa | Data<br>Analysis | https://cipesa.org/ |
| Colnodo | NGO | Latin America and the Caribbean | Latin America and the Caribbean | Analysis<br>Advocacy | http://www.colnodo.apc.org/index.shtml |
| Committee to Protect Journalists | NGO | Global | North America | Analysis<br>Training<br>Advocacy<br>Legal | https://www.cpj.org/about/ |
| Counter-Power Lab | Academic | Global | North America | Technology | https://www.icsi.berkeley.edu/icsi/projects/networking/counter-power-lab |
| Cyber Stewards Network | Academic | Global | North America | Data<br>Analysis<br>Advocacy | https://cyberstewards.org |
| Danish International Development Agency (DANIDA) | Government | Europe | Europe | Funding | http://um.dk/en/danida-en/ |
| Derechos Digitales | NGO | Latin America and the Caribbean | Latin America and the Caribbean | Analysis<br>Advocacy<br>Legal | https://www.derechosdigitales.org |
| Digital Defenders | NGO | Global | Europe | Training<br>Funding | https://www.digitaldefenders.org/digitalfirstaid/ |
| Digital Security Exchange | NGO | Global | Europe | Direct Assistance | https://www.digitalsecurityexchange.org/ |
| DW Akademie | Government | Global | Europe | Training<br>Funding<br>Advocacy | http://www.dw.com/en/dw-akademie/about-us/s-9519 |
| Electronic Frontier Foundation | NGO | Global | North America | Analysis<br>Technology<br>Training<br>Advocacy<br>Legal | www.eff.org |

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| Equalit.ie | Company | Global | Europe | Technology<br>Direct Assistance | https://equalit.ie/ |
| European Endowment for Democracy | Foundation | Europe | Europe | Funding | http://www.democracyendowment.eu/ |
| European Federation of Journalists | NGO | Europe | Europe | Training<br>Legal | http://europeanjournalists.org/blog/2015/01/22/cyber-security-training-for-journalists/ |
| Ford Foundation | Foundation | Global | North America | Funding | https://www.fordfoundation.org/ |
| Foundation for Media Alternatives | NGO | Southeast Asia | Southeast Asia | Advocacy | http://www.fma.ph/ |
| Free Press Unlimited | NGO | Global | Europe | Analysis<br>Technology<br>Training<br>Advocacy | https://www.freepressunlimited.org/ |
| Freedom House | NGO | Global | North America | Analysis<br>Advocacy | https://freedomhouse.org/report/freedom-net/freedom-net-2015 |
| Freedom of the Press Foundation | NGO | Global | North America | Analysis<br>Technology<br>Training<br>Funding<br>Advocacy | https://freedom.press/ |
| Freedom Online Coalition | Government | Global | Europe | Analysis<br>Funding<br>Advocacy | https://www.freedomonlinecoalition.com/ |
| French Media Cooperation Agency (CFI) | Government | Northern Africa<br>Sub-Saharan Africa<br>Western Asia<br>Southeast Asia | Europe | Funding | http://www.cfi.fr/en/content/institution |
| Front Line Defenders | NGO | Global | Europe | Analysis<br>Direct Assistance<br>Technology<br>Training<br>Funding<br>Advocacy<br>Legal | https://www.frontlinedefenders.org/ |

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| German Federal Ministry for Economic Cooperation and Development (BMZ) | Government | Global | Europe | Funding | http://www.cima.ned.org/donor-profiles/german-federal-ministry-economic-cooperation-development-bmz/ |
| Global Affairs Canada | Government | Global | North America | Funding | http://www.international.gc.ca/international/index.aspx?lang=eng |
| Global Network Initiative | NGO | Global | North America | Analysis<br>Advocacy | http://globalnetworkinitiative.org/ |
| Global Voices | NGO | Global | Europe | Analysis<br>Advocacy | https://globalvoices.org/ |
| Government of the Netherlands | Government | Europe | Europe | Funding | https://www.government.nl/topics/human-rights/promoting-freedom-of-expression-including-internet-freedom |
| GreatFire | NGO | Eastern Asia | Unknown | Data<br>Analysis<br>Technology<br>Advocacy | https://en.greatfire.org/ |
| Greenhost | Company | Global | Europe | Technology<br>Direct Assistance | https://greenhost.net/products/rapid-response-services/ |
| Guardian Project | NGO | Global | North America | Analysis<br>Technology | https://guardianproject.info/ |
| HeartMob | NGO | Global | North America | Technology<br>Training | https://iheartmob.org/ |
| Herdict | Academic | Global | North America | Data | https://www.herdict.org/ |
| Hewlett Foundation | Foundation | Global | North America | Funding | http://www.hewlett.org/ |
| Human Rights Education Institute of Burma | NGO | Southeast Asia | Southeast Asia | Analysis<br>Training<br>Advocacy | https://humanrightsinasean.info/content/human-rights-education-institute-burma-hreib.html |
| ICT Watch | NGO | Southeast Asia | Southeast Asia | Analysis<br>Technology<br>Training<br>Advocacy | http://ictwatch.id/ |
| Information Society Project | Academic | North America | North America | Analysis<br>Legal | https://law.yale.edu/isp |

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| Internews | NGO | Global | North America<br>Europe<br>Sub-Saharan Africa<br>Eastern Europe<br>Southeast Asia | Analysis<br>Training | http://www.internews.org |
| Japan International Cooperation Agency | Government | Europe<br>Northern Africa<br>Sub-Saharan Africa<br>Eastern Asia<br>Southeast Asia<br>Western Asia<br>Oceania<br>Latin America and the Caribbean | Eastern Asia | Funding | https://www.jica.go.jp/english/about/mission/#vision |
| Jigsaw (Alphabet) | Company | Global | North America | Data<br>Technology<br>Direct Assistance | https://jigsaw.google.com |
| Justice Forum | NGO | Global | North America<br>Southeast Asia | Data<br>Analysis<br>Advocacy | http://justiceforum.org/ |
| Knight Foundation | Foundation | North America | North America | Funding | http://www.knightfoundation.org/ |
| La Red en Defensa de los Derechos Digitales (R3D) | NGO | Latin America and the Caribbean | Latin America and the Caribbean | Analysis<br>Advocacy<br>Legal | https://r3d.mx |
| Lumen | Academic | Global | North America | Data | https://lumendatabase.org/ |
| MacArthur Foundation | Foundation | Global | North America<br>Eastern Asia<br>Latin America and the Caribbean<br>Sub-Saharan Africa | Funding | https://www.macfound.org/ |
| MayFirst/ People's Link | NGO | Global | North America<br>Latin America and the Caribbean | Technology<br>Training<br>Advocacy | https://mayfirst.org/ |
| Media Democracy Fund | Foundation | Global | North America | Funding | http://mediademocracyfund.org/ |
| Moroccan Digital Rights Organization | NGO | Northern Africa | Northern Africa | Training<br>Advocacy | https://www.facebook.com/raqmiya |

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| Mozilla Foundation | Foundation | Global | North America | Analysis<br>Technology<br>Advocacy | https://www.mozilla.org/en-us/foundation/ |
| National Endowment for Democracy | Foundation | Global | North America | Funding | http://www.ned.org/ |
| Net Alert | Academic | Global | North America | Analysis<br>Technology | https://www.opentech.fund/project/net-alert |
| Net Gain Partnership | Foundation | Global | North America | Analysis<br>Funding<br>Advocacy | https://netgainpartnership.org/ |
| New America Open Technology Institute | NGO | North America | North America | Analysis<br>Technology<br>Funding<br>Advocacy<br>Legal | https://www.newamerica.org/oti/ |
| Norwegian Government (Ministry of Foreign Affairs and the Norwegian Agency for Development Cooperation) | Government | Europe | Europe | Funding | https://www.regjeringen.no/en/dep/ud/id833/ |
| Omidyar Network | Foundation | Global | North America<br>Eastern Asia<br>Sub-Saharan Africa<br>Europe<br>Southeast Asia | Funding | https://www.omidyar.com/ |
| Open Observatory of Network Interference | NGO | Global | North America | Data<br>Analysis<br>Technology | https://ooni.torproject.org/ |
| Open Society Foundation | Foundation | Global | Europe<br>Eastern Europe<br>North America | Funding | https://www.opensocietyfoundations.org |
| Open Technology Fund | Foundation | Global | North America | Data<br>Analysis<br>Technology<br>Direct Assistance<br>Training<br>Funding | https://www.opentech.fund/projects |

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| Open Whisper Systems | Company | Global | North America | Technology | https://whispersystems.org/ |
| OpenNet Initiative | Academic | Global | North America | Data Analysis | https://opennet.net/ |
| OpenNet Korea | NGO | Eastern Asia | Eastern Asia | Analysis<br>Advocacy<br>Legal | http://opennetkorea.org/en/wp/?ckattempt=2 |
| Paradigm Initiative Nigeria | NGO | Sub-Saharan Africa | Sub-Saharan Africa | Analysis<br>Advocacy | https://pinigeria.org/ |
| Project Galileo | Company | Global | North America | Technology<br>Direct Assistance | https://www.cloudflare.com/galileo/ |
| Qurium | NGO | North America<br>Northern Africa<br>Sub-Saharan Africa<br>Eastern Asia<br>Western Asia<br>Southeast Asia<br>Eastern Europe<br>Europe | Europe | Analysis<br>Technology<br>Direct Assistance<br>Training | https://www.qurium.org/history |
| RAREnet | NGO | Global | Global | Technology<br>Training | http://www.rarenet.org/projects/ |
| Riseup | NGO | Global | North America | Technology | https://riseup.net |
| Samuelson Law, Technology & Public Policy Clinic | Academic | North America | North America | Analysis<br>Legal | https://www.law.berkeley.edu/experiential/clinics/samuelson-law-technology-public-policy-clinic/ |
| Security First / Umbrella App | NGO | Global | Europe | Technology<br>Training | https://secfirst.org/ |
| Security Without Borders | NGO | Global | Global | Direct Assistance<br>Training | https://securitywithoutborders.org/ |
| Silent Circle | Company | Global | North America | Technology | https://www.silentcircle.com/ |
| SocialTIC | NGO | Latin America and the Caribbean | Latin America and the Caribbean | Technology<br>Training<br>Advocacy | https://socialtic.org |
| Sulá Batsú | NGO | Latin America and the Caribbean | Latin America and the Caribbean | Analysis<br>Training<br>Advocacy | http://www.sulabatsu.com/ |

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| Swedish International Development Cooperation Agency (SIDA) | Government | Northern Africa<br>Sub-Saharan Africa<br>Eastern Asia<br>Southeast Asia<br>Western Asia<br>Eastern Europe<br>Europe<br>Latin America and the Caribbean | Europe | Funding | http://www.sida.se/english/how-we-work/our-fields-of-work/democracy-human-rights-and-freedom-of-expression/freedom-of-expression/ |
| Tactical Technology Collective | NGO | Global | Europe | Analysis<br>Technology<br>Training | https://tacticaltech.org/ |
| Tails | NGO | Global | North America | Technology | https://tails.boum.org/about/index.en.html |
| The Center on Privacy & Technology | Academic | North America | North America | Analysis | https://www.law.georgetown.edu/academics/centers-institutes/privacy-technology/ |
| The Takedown Project | Academic | Global | North America | Analysis<br>Legal | http://takedownproject.org/ |
| Tibet Action Institute | NGO | Eastern Asia | North America | Analysis<br>Training<br>Advocacy | https://tibetaction.net/ |
| Tor Project | NGO | Global | North America | Technology | https://www.torproject.org/ |
| U.S. Department of State, Bureau of Democracy, Human Rights, and Labor (DRL) | Government | North America | North America | Analysis<br>Training<br>Funding<br>Advocacy | https://www.state.gov/j/drl/internetfreedom/index.htm |
| UNESCO—International Program for the Development of Communication | NGO | Global | Europe | Funding | http://www.unesco.org/new/en/communication-and-information/intergovernmental-programmes/ipdc/about-ipdc/ |
| Upturn | NGO | North America | North America | Analysis | https://teamupturn.com |

| Organization | Type of Org | Geographic Region Served | Geographic Region Based | Assistance Provided | Website |
|---|---|---|---|---|---|
| USAID Center of Excellence on Democracy, Human Rights, and Governance | Government | Global | North America | Funding | https://www.usaid.gov/who-we-are/organization/bureaus/bureau-democracy-conflict-and-humanitarian-assistance/center# |
| Web We Want | NGO | Global | North America<br>Southeast Asia<br>Europe<br>Sub-Saharan Africa | Funding<br>Advocacy | http://webwewant.org/about/ |

# Endnotes

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

[2] Pinkaew Laungaramsri, "Mass Surveillance and the Militarization of Cyberspace in Post-Coup Thailand," *Austrian Journal of South-East Asian Studies* 9, no. 2 (July 2016): 195–213.

[3] John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware* (Toronto: Citizen Lab, June 19, 2017), https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

[4] ohn Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, *Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware* (Toronto: Citizen Lab, June 29, 2017), https://citizenlab.ca/2017/06/more-mexican-nso-targets/.

[5] Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[6] Ashnah Kalemera, et al., *Safeguarding Civil Society: Assessing Internet Freedom and Digital Resilience of Civil Society in East Africa* (The Collaboration on International ICT Policy in East and Southern Africa, 2017), https://cipesa.org/2017/03/safeguarding-civil-society-assessing-internet-freedom-and-the-digital-resilience-of-civil-society-in-east-africa/.

[7] World Economic Forum, *The Future Role of Civil Society* (Geneva: World Economic Forum, January 2013), http://www3.weforum.org/docs/WEF_FutureRoleCivilSociety_Report_2013.pdf.

[8] Citizen Lab, *Communities @ Risk: Targeted Digital Threats Against Civil Society* (Toronto: Citizen Lab: 2014), https://targetedthreats.net/.

[9] David Israelson, "Hackers Refine Techniques to Go after Smaller Companies," *Globe and Mail*, May 12, 2017, https://www.theglobeandmail.com/report-on-business/hackers-refine-techniques-to-go-after-smaller-companies/article34967980/.

[10] *CrowdStrike 2018 Global Threat Report* (Sunnyvale, CA: Crowdstrike, 2018), http://crowdstrike.lookbookhq.com/global-threat-report-2018-web/cs-2018-global-threat-report.

[11] Citizen Lab, *Communities @ Risk, supra* note *8*.

[12] Lyndal Cairns, "Nonprofit Technology Staffing and Investments Report," *Non-Profit Technology Network*, May 2017, https://www.nten.org/article/your-guide-to-nonprofit-it-investment/.

[13] Burning Glass, "Job Market Intelligence: Cybersecurity Jobs, 2015," *Burning Glass Technologies*, July 2015, http://burning-glass.com/research/cybersecurity/.

[14] "Third Annual Not-for-Profit Governance Survey Reveals Declining Confidence in Governance Policies," *CohnReznick*, September 20, 2016, https://www.cohnreznick.com/insight/reports-and-whitepapers/2016-not-for-profit-governance-survey-report.

[15] Jakub Dalek, Ron Deibert, Bill Marczak, Sarah McKune, Helmi Noman, Irene Poetranto, and Adam Senft, "Tender Confirmed, Rights At Risk: Verifying Netsweeper in Bahrain," (Toronto: The Citizen Lab), September 21, 2016, https://citizenlab.org/2016/09/tender-confirmed-rights-risk-verifying-netsweeper-bahrain/.

**16** John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata, "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links," (Toronto: The Citizen Lab), February 11, 2017, https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/.

**17** Citizen Lab, *supra* note *1*

**18** Jorge Luis Sierra, *Digital and Mobile Security for Mexican Journalists and Bloggers: Results of a Survey of Mexican Journalists and Bloggers* (Washington, DC: Freedom House, 2013), https://www.icfj.org/resources/digital-and-mobile-security-mexican-journalists-and-bloggers.

**19** Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner, "Investigating the Computer Security Practices and Needs of Journalists" (Presentation, 24th USENIX Security Symposium, Washington, DC, August 12–14, 2015), https://www.usenix.org/node/190977.

**20** Lily Hay Newman, "The Ransomware Meltdown Experts Warned About Is Here," *WIRED*, May 12, 2017, https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.

**21** Danuta Kean, "Ransomware Attack Paralyses St Louis Libraries as Hackers Demand Bitcoins," *The Guardian*, January 23, 2017, https://www.theguardian.com/books/2017/jan/23/ransomware-attack-paralyses-st-louis-libraries-as-hackers-demand-bitcoins.

**22** Frost & Sullivan, *2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk* (Clearwater, FL: Center for Cyber Safety and Education), 2017, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS.pdf.

**23** Stephanie L Geller, Alan J Abramson, and Erwin de Leon, *The Nonprofit Technology Gap–Myth or Reality* (Johns Hopkins Listening Post Project, Communique 20, 2010), http://ejewishphilanthropy.com/wordpress/wp-content/uploads/2010/12/Nonprofit-Technology-Gap-Dec.-2010.pdf.

**24** "Study: Number Of Data Staff At Nonprofits Increases," *The NonProfit Times*, August 22, 2014 http://www.thenonprofittimes.com/news-articles/study-number-data-staff-nonprofits-increases/.

**25** *Id.*

**26** Nonprofit Tech for Good, *2018 Global NGO Technology Report* (Reston, VA: Public Interest Registry, 2018), http://techreport.ngo/.

**27** The encryption offered by many different messaging services often does not interoperate, so communications sent across different messaging platforms are usually not encrypted. Fragmentation in the online messaging marketplace may result in a level of security inconsistent with NGOs' expectations. If an SMS application promises "end-to-end encryption", but that is only true for messages with other users of the app (and all other messages are not encrypted), user may not always understand that distinction.

**28** *See* Kalemera et al., *supra* note *6*.

**29** *See* Kalemera et al., *supra* note *6*.

**30** "Cybersecurity Framework," National Institute of Standards and Technology, last updated April 16, 2018, https://www.nist.gov/cyberframework.

**31** AccessNow, *Global Civil Society at Risk: An Overview of Some of the Major Threats Facing Civil Society* (New York: AccessNow, January 2012), https://s3.amazonaws.com/access.3cdn.net/3aa0654d836dbffdf6_drm6ibn8c.pdf.

**32** "FBI Warns of ISIS-Sympathetic Hackers Attacking and Defacing WordPress Sites," *VentureBeat*, April 7, 2015, https://venturebeat.com/2015/04/07/fbi-warns-of-isis-sympathetic-hackers-attacking-and-defacing-wordpress-sites/; "Internet Crime Complaint Center (IC3) | ISIL Defacements Exploiting WordPress Vulnerabilities," (Washington DC, Federal Bureau of Investigation), April 7, 2015, https://www.ic3.gov/media/2015/150407-1.aspx.

**33** Nick Fogle, "When ISIS Hacks Your Website," *NickFogle.com*, January 7, 2015, http://nickfogle.com/hacked-by-isis/; Laura Haight, "NonProfit Hacks: Too Small to Be Hacked? Not!" *Portfolio*, July 2, 2015, https://www.portfoliosc.com/blog/2015/7/2/nonprofit-hacks-most-at-risk-least-prepared.

**34** The vast majority of attack chains described in the source material for this report start with phishing as an entry point into a target's network. The 2017 Verizon Data Breach Report noted "Phishing via email was the most prevalent variety of social attacks." Verizon Enterprise Solutions, "2017 Data Breach Investigations Report" 2017, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

**35** A spearphishing attack may use specific information about a target to make them more likely to fall for the scam. For example, a broad phishing attack might lead recipients to click on a link to find out if they won a contest. A more targeted spearphishing attack might pretend to be from a relative or close friend, encouraging a targeted individual to click on a malicious link disguised popular photo sharing site.

**36** Lipton, Sanger, and Shane, *supra* note *5*.; Nex, "Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal," *Amnesty Insights* (New York, Amnesty International), February 14, 2017, https://medium.com/amnesty-insights/operation-kingphish-uncovering-a-campaign-of-cyber-attacks-against-civil-society-in-qatar-and-aa40c9e08852; John Scott-Railton, Bill Marczak, Ramy Raoof, and Etienne Maynier, "[Updated] Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society," *Citizen Lab* (blog), February 2, 2017, https://citizenlab.org/2017/02/nilephish-report/.

**37** *Id.*

**38** Katie Kleemola, Masashi Crete-Nishihata, and John Scott-Railton,"Tibetan Uprising Day Malware Attacks," *Citizen Lab* (blog), March 10, 2015, https://citizenlab.org/2015/03/tibetan-uprising-day-malware-attacks/; John Scott-Railton and Seth Hardy, "Malware Attacks Targeting Syrian ISIS Critics," *Citizen Lab* (blog), December 18, 2014, https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/; Citizen Lab, *supra* note *13*.

**39** Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri, and Katie Kleemola, "Hacking Team's Tradecraft and Android Implant," *Citizen Lab* (blog), June 24, 2014, https://citizenlab.org/2014/06/backdoor-hacking-teams-tradecraft-android-implant/; Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Hacking Team and the Targeting of Ethiopian Journalists," *Citizen Lab* (blog), February 12, 2014, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/; Bill Marczak, John Scott-Railton, and Sarah McKune, "Hacking Team Reloaded," *Citizen Lab* (blog), March 9, 2015, https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

**40** Hannah Kuchler and James Politi, "Italy Strips Hacking Team of Licence to Export Outside EU," *Financial Times*, April 19, 2016, https://www.ft.com/content/74d87c9e-053c-11e6-96e5-f85cb08b0730.

**41** U.S. Department of Commerce, "Italian Company Agrees to $100,000 Penalty for Unlawful Technology Export to Syria" (press release, U.S. Department of Commerce, February 24, 2014), https://www.bis.doc.gov/index.php/all-articles/107-about-bis/newsroom/press-releases/press-release-2014/755-italian-company-agrees-to-100-000-penalty-for-unlawful-technology-export-to-syria-2.

**42** There are a number of potential reasons for the use of highly sophisticated exploits against politically vulnerable organizations. It may be these governments see these organizations as targets worth a significant expense. Or it may be that these governments that are less experienced in cybersecurity operations are not sophisticated customers, and have been "upsold" expensive capabilities where less costly attacks would have sufficed. While it may never become apparent why such expensive exploits were used to target activists in the UAE, Mexico, and elsewhere, one thing is certain: the amount of money being channeled to private spyware companies by governments is substantial.

**43** *See* Citizen Lab, *Million Dollar Dissident*, *supra* note *1*.

**44** *See* Citizen Lab, *Communities @ Risk*, *supra* note *8*.

**45** Brian Krebs, “DDoS on Dyn Impacts Twitter, Spotify, Reddit,” *Krebs on Security* (blog), October 16, 2016, https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.

**46** Joshua McLaurin, “Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks,” *Yale Law & Policy Review* 30, no. 1 (December 10, 2015), http://digitalcommons.law.yale.edu/ylpr/vol30/iss1/7; Fahmida Y. Rashid, “FBI to Investigate China-Based DDoS Attacks Against Change.org,” *eWEEK*, April 29, 2011, http://www.eweek.com/cloud/fbi-to-investigate-china-based-ddos-attacks-against-change.org.

**47** Bill Marczak, et al., “China’s Great Cannon,” *Citizen Lab* (blog), April 10, 2015, https://citizenlab.org/2015/04/chinas-great-cannon/; Nick Weaver, “A Close Look at the NSA’s Most Powerful Internet Attack Tool,” *WIRED* (opinion), March 13, 2014, https://www.wired.com/2014/03/quantum/.

**48** William Turton, “Planned Parenthood Hacked, Database Dumped Online,” *The Daily Dot*, July 27, 2015, https://www.dailydot.com/layer8/planned-parenthood-hacked-anti-abortion-3301/.

**49** TLS is commonly represented by the “padlock” icon in browsers; it ensures that individuals are connecting with the domain they intend to reach. *See* Seth Schoen and Eva Galperin, “Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities,” *Electronic Frontier Foundation* (blog), August 29, 2011, https://www.eff.org/deeplinks/2011/08/iranian-man-middle-attack-against-google; Phil Muncaster, “China Launches Man in the Middle Attack Against Google,” *Infosecurity Magazine*, September 5, 2014, https://www.infosecurity-magazine.com/news/china-man-in-the-middle-attack/.

**50** Jeffrey Knockel, Sarah McKune, and Adam Senft, “Baidu’s and Don’ts: Privacy and Security Issues in Baidu Browser,” (Toronto, The Citizen Lab), February 23, 2016, https://citizenlab.org/2016/02/privacy-security-issues-baidu-browser/; “A Tough Nut to Crack: A Further Look at Privacy and Security Issues in UC Browser,” (Toronto, Citizen Lab), August 7, 2016, https://citizenlab.org/2016/08/a-tough-nut-to-crack-look-privacy-and-security-issues-with-uc-browser/.

**51** *Id.*

**52** Some sophisticated attackers have been identified by researchers as persistent online threat actors, often based upon analysis of consistent methods across multiple attacks. These groups, who are often state-sponsored, will occasionally receive a designation by security researchers such as “APT 1”.

**53** *See* Citizen Lab, *Communities @ Risk*, *supra* note *8*; Lipton, Sanger, and Shane, *supra* note *5*.

**54** Olga Khazan, “The Creepy, Long-Standing Practice of Undersea Cable Tapping,” *Atlantic*, July 16, 2013, https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

**55** Peter Svensson, “Pakistan Causes YouTube Outage for Two-Thirds of World,” *ABC News*, February 26, 2008, http://abcnews.go.com/Technology/story?id=4344105&page=1; Darrell M West, *Internet Shutdowns Cost Countries $2.4 Billion Last Year* (Washington, DC: Brookings Institution, 2016), https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/.

**56** Noam Cohen, “Egyptian Internet Blackout Pushed Protests to Streets,” *New York Times*, February 20, 2011, https://www.nytimes.com/2011/02/21/business/media/21link.html; Michael Cabanatuan, “BART Admits Halting Cell Service to Stop Protests,” *SFGate*, August 12, 2011, http://www.sfgate.com/news/article/BART-admits-halting-cell-service-to-stop-protests-2335114.php.

**57** Jon Penney, “Chilling Effects: Online Surveillance and Wikipedia Use,” *Berkeley Technology Law Journal 31* (Berkeley, Berkeley Law), no. 1: 117, *available at* https://papers.ssrn.com/abstract=2769645.

**58** Human Rights Watch, *‘They Know Everything We Do’* (New York: Human Rights Watch, 2014), https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia; Laungaramsri, “Mass Surveillance,” *supra* note *2*; Alex Comninos and Gareth Seneque, “Cyber Security, Civil Society and Vulnerability in an Age of Communications Surveillance,” in *Global Information Society Watch 2014: Communications Surveillance in* *the Digital Age* (Association for Progressive Communications (APC) and the Humanist Institute for Cooperation with Developing Countries (Hivos), 2014), https://www.giswatch.org/sites/default/files/cyber_security_civil_society_and_vulnerability.pdf.

**59** Gary King, Jennifer Pan, and Margaret E. Roberts, "Reverse-Engineering Censorship in China: Randomized Experimentation and Participant Observation," *Science* 345, no. 6199 (2014): 1–10.

**60** Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107, no. 2 (2013): 326–43, https://doi.org/10.1017/S0003055413000014; Laungaramsri, "Mass Surveillance," *supra* note *ii*; Jakub Dalek, et al., "Tender Confirmed, Rights At Risk: Verifying Netsweeper in Bahrain," *Citizen Lab* (blog), September 21, 2016, https://citizenlab.org/2016/09/tender-confirmed-rights-risk-verifying-netsweeper-bahrain/; Reem al Masri, "In Jordan, the 'Invisible Hand' Blocks Internet Archive," (Toronto, the Citizen Lab), April 10, 2017, https://citizenlab.org/2017/04/jordan-invisible-hand-blocks-internet-archive/.

**61** "We (Can't) Chat: '709 Crackdown' Discussions Blocked on Weibo and WeChat," (Toronto, the Citizen Lab), April 13, 2017, https://citizenlab.org/2017/04/we-cant-chat-709-crackdown-discussions-blocked-on-weibo-and-wechat/; Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, "Tibetans Blocked from Kalachakra at Borders and on WeChat," (Toronto, the Citizen Lab), January 10, 2017, https://citizenlab.org/2017/01/tibetans-blocked-from-kalachakra-at-borders-and-on-wechat/; David Robinson, Harlan Yu, and Anne An, *Collateral Freedom: A Snapshot of Chinese Internet Users Circumventing Censorship* (Washington, DC: Open Internet Tools Project Report, 2013), http://www.teamupturn.org/static/files/CollateralFreedom.pdf.

**62** Nadiya Romanenko, Iaryna Mykhyalyshyn, Pavlo Solodko, and Orest Zog, "The Troll Network," *ТЕКСТИ.ORG.UA*, accessed May 15, 2018, http://texty.org.ua/d/fb-trolls/index_eng.html; "Russian Troll Farms behind Campaign to Topple Ukraine's Government," *StopFake.org* (blog), October 11, 2016, http://www.stopfake.org/en/russian-troll-farms-behind-campaign-to-topple-ukraine-s-government/.

**63** Aric Toler, "Inside the Kremlin Troll Army Machine: Templates, Guidelines, and Paid Posts" *Global Voices*, March 14, 2015, https://globalvoices.org/2015/03/14/russia-kremlin-troll-army-examples/.

**64** Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, "Tainted Leaks: Disinformation and Phishing with a Russian Nexus," (Toronto, the Citizen Lab), May 25, 2017, https://citizenlab.org/2017/05/tainted-leaks-disinformation-phish/.

**65** Samantha Bradshaw, Philip N. Howard, and P. Bradshaw, "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation" (University of Oxford Computational Propaganda Research Project, Working Paper 2017.12, 2017), http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf.

**66** Katie Grant, "Twitter 'Failing in Its Moral Duty' to Stop Trolls," *Independent*, February 20, 2015, http://www.independent.co.uk/news/uk/home-news/twitter-failing-in-its-moral-duty-to-protect-users-from-abuse-says-leading-autism-campaigner-10060668.html.

**67** Lester M. Salamon, S. Wojciech Sokolowski, and Megan A. Haddock, *The State of Global Civil Society and Volunteering: Latest Findings from the Implementation of the UN Nonprofit Handbook* (Baltimore: Johns Hopkins Center for Civil Society Studies, 2012), http://ccss.jhu.edu/wp-content/uploads/downloads/2013/04/JHU_Global-Civil-Society-Volunteering_FINAL_3.2013.pdf.

**68** Information Communications Technology for Development (ICT4D) is a significant component of many international development agencies' and organizations' work. However, it historically focuses on infrastructure and communications technology access, and rarely includes efforts to improve privacy or the cybersecurity of politically targeted individuals or groups.

**69** *See* Citizen Lab, *Bitter Sweet; supra* notes *12*.

**70** "Alternative Sources of Support," Open Technology Fund, accessed July 3, 2017, https://www.opentech.fund/apply/alternative-sources-support.

**71** "Protect Yourself," Freedom of the Press Foundation, accessed May 15, 2018, https://freedom.press/training/; "Surveillance Self-Defense," Electronic Frontier Foundation, accessed May 15, 2018, https://ssd.eff.org/en;"Security in a Box - Digital Security Tools and Tactics," Tactical Technology Collective, accessed May 15, 2018, https://securityinabox.org.

**72** "Security Planner—Improve Your Online Safety with Tools for Your Needs.," Security Planner, 2018, https://securityplanner.org.

**73** For example, the popular Privacy Badger tool developed by EFF is open source, but changes to the tool since the initial release have come almost exclusively from within the EFF organization. *See* "commits" and "contributors" on the EFF github repository, *available at* https://github.com/EFForg/privacybadger/network.

**74** Troy Hunt, "HTTPS Adoption Has Reached the Tipping Point," *TroyHunt.com* (blog), January 30, 2017, https://www.troyhunt.com/https-adoption-has-reached-the-tipping-point/; Maria Korolov, "Study: Encryption Use Increase Largest in 11 Years," *CSO Online*, June 28, 2016, http://www.csoonline.com/article/3088916/data-protection/study-encryption-use-increase-largest-in-11-years.html.

**75** "Users—Tor Metrics," TorProject.org, https://metrics.torproject.org/userstats-relay-country.html?start=2012-01-01&end=2018-06-01&country=all&events=off.

**76** Gabriel Avner, "Privacy Badger Burrows Past 1 Million Downloads, Blocking Third-Party Tracker," *Geektime* (blog), April 5, 2017, http://www.geektime.com/2017/04/05/privacy-badger-burrows-past-1-million-downloads-blocking-third-party-tracker/.

**77** "SKS Keyservers: History of Number of OpenPGP Keys," sks-keyservers.net, accessed May 15, 2018, https://sks-keyservers.net/status/key_development.php.

**78** *See* Kalemera et al., *supra* note *6*.

**79** Sierra, *supra* note *15*; *Digital and Mobile Security for Mexican Journalists and Bloggers: Results of a Survey of Mexican Journalists and Bloggers*; McGregor et al., *supra* note *xvi*.

**80** Associated Press, "Shi Tao: China Frees Journalist Jailed Over Yahoo Emails," *Guardian*, September 8, 2013, http://www.theguardian.com/world/2013/sep/08/shi-tao-china-frees-yahoo.

**81** This is accurate as of June 2018, but this award amount may change over time.

**82** Open Technology Fund, "2015 Annual Report", 2016, https://www.opentech.fund/sites/default/files/attachments/2015otfannualreport.pdf

**83** Greenhost email security recommendations can be found here: https://riseup.net/en/email/webmail/2factorauth. Information on RiseUp's authentication security can be found here: "Two Factor Authentication with Roundcube Webmail," RiseUp.com, accessed May 15, 2018, https://riseup.net/en/email/webmail/2factorauth.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley