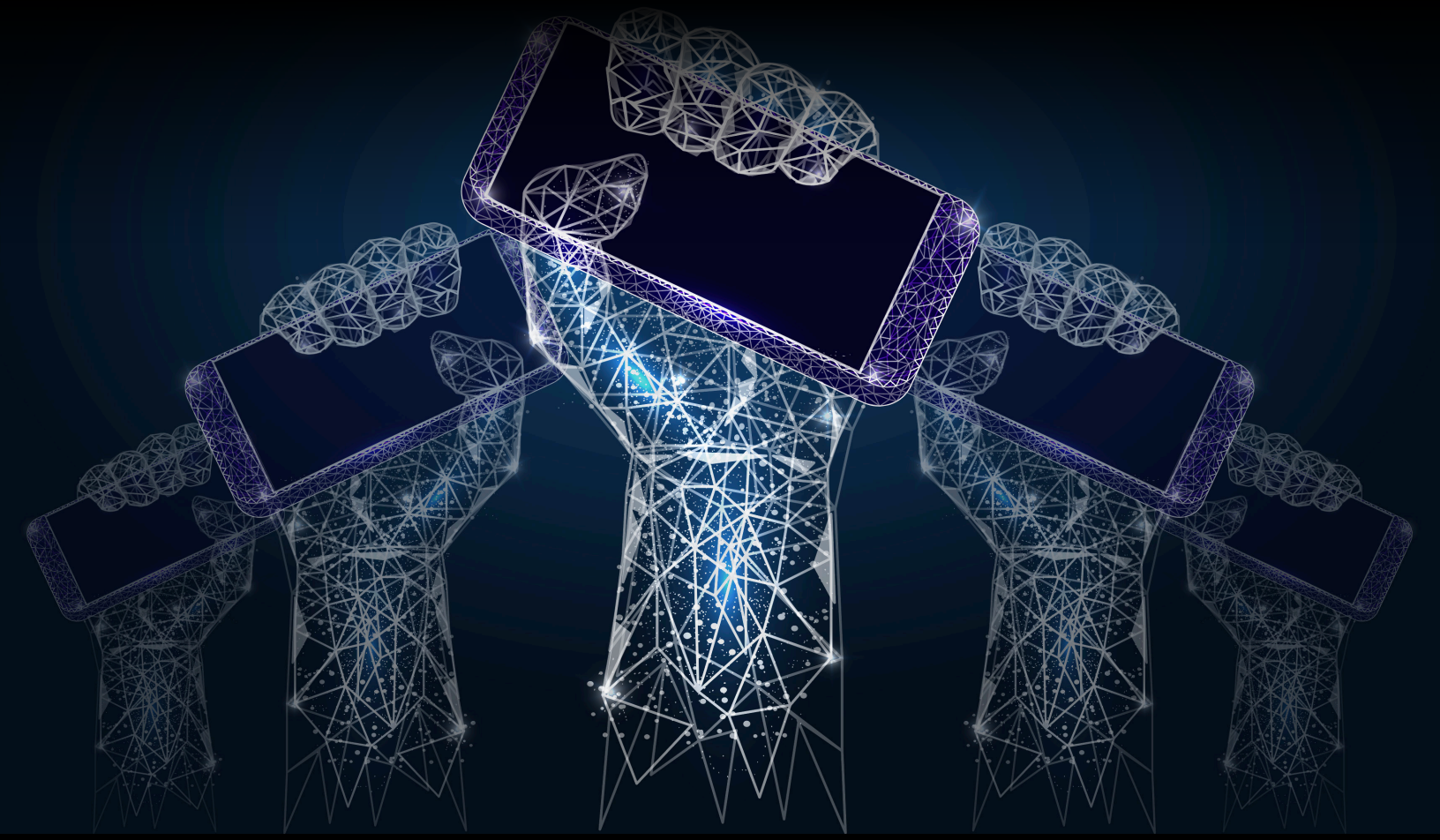
UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY



CLTC WHITE PAPER SERIES

Enhancing Cybersecurity Resilience for Transnational Dissidents

NOURA ALJIZAWI, GÖZDE BÖCÜ, AND NICOLA LAWFORD

CLTC WHITE PAPER SERIES

Enhancing Cybersecurity Resilience for Transnational Dissidents

NOURA ALJIZAWI, GÖZDE BÖCÜ, AND NICOLA LAWFORD

September 2024

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Executive Summary

Grassroots transnational activist organizations are critical to democracy but are vulnerable to cyber threats from state-related actors. This report examines the cybersecurity posture, vulnerability, and resilience of exiled women dissidents in the U.S. and their transnational advocacy and journalism organizations. These exiled dissident women face unique challenges at the intersection of gender, politics, and home country-backed digital repression. The report tries to identify the primary cybersecurity threats faced by these transnational women activists in the U.S., understand the measures they use to protect themselves, and determine key areas for action and improvement to enhance their cybersecurity.

This research is based on 17 semi-structured interviews with women-identifying victims of digital transnational repression (DTR) in the U.S., interviews with five current and former staff from digital rights organizations to gain insights into cyber threats and effective countermeasures. The team developed and used a framework combining SAFETAG methods with new themes from the digital rights organization interviews for data analysis.

Summary of Findings

- Activists face threats such as spyware, phishing, and disinformation, among others. Although privacy features and cybersecurity frameworks are available, they are often insufficient against sophisticated threats.
- Women, queer individuals, and other marginalized groups face targeted harassment and disinformation campaigns. These attacks exploit gender- and identity-based vulnerabilities to discredit, intimidate, and silence these activists, making their cybersecurity needs particularly urgent.
- Activists adopt their own cybersecurity policies and practices based on their unique experience and needs. These forms of resilience extend into all aspects of daily life, including home and family life, external employment, and decisions around navigating their host country and diaspora community.

General cybersecurity recommendations

- Limited financial resources and reliance on insecure software increase activists' vulnerability. When funding is available, it often focuses on short-term projects, neglecting the need for building long-term cyber resilience.
- There is a need for tailored cybersecurity strategies to address complex migration and security dynamics.

Recommendations to U.S. government agencies

- U.S. government agencies should provide comprehensive support to prevent, mitigate, and investigate transnational repression. They should also develop community-based alternatives to law enforcement for activists who are uncomfortable with traditional state mechanisms. Any form of government intervention should be done based on human rights due diligence and in partnership with the impacted communities, to ensure no more policing or surveillance is imposed on transnational dissidents.

Recommendations to U.S. private-sector organizations

- Tech companies should implement protective features for high-risk users, while social media platforms, in particular, should enhance trust and safety measures, improve content moderation, invest in other languages, and enforce policies against disinformation and deepfakes.
- They should also ensure protection for all users against deepfake sexual violence, and invest in content moderation that accounts for diverse languages, cultural contexts, and the specific vulnerabilities of marginalized groups.

Introduction

In today's digital age, cybersecurity plays an important role in preserving democracy. While public institutions like hospitals, local governments, and critical infrastructure are commonly targeted by hackers seeking political and economic advantages, there exists another critical but often overlooked sector under constant attack by state-related actors: grassroots transnational activist organizations. These organizations, vital to the fabric of democratic societies, are often politically vulnerable and lack formal structures and crucial resources to protect themselves against cyberattacks. However, because these organizations are essential platforms that protect and empower politically vulnerable groups such as asylum seekers and refugees from experiencing harm, they often become targets of repressive regimes around the world that seek to silence them. This paper delves into the cybersecurity posture and protections of transnational activists in the United States, profiling their vulnerabilities and resilience in the face of evolving cyber threats.

Within the broader context of digital vulnerability and resistance, this study focuses on a group disproportionately affected by threats: exiled women dissidents. Their positionality and experience, emerging from the intersections of gender, politics, and digital repression, offer unique insights into the complexities of transnational activism in the digital age. Acting across a spectrum of organizations — from grassroots initiatives to formal institutions — these women exemplify the confluence of resilience and vulnerability.

This study explores digital transnational repression (DTR) against women, which we understand as a form of technology-facilitated, gender-based violence against exiled women dissidents, and frame as gendered digital transnational repression (GDTR).[1] The tools of digital transnational repression include targeted spyware and malware, harassment and disinformation campaigns on social media or messaging platforms, distributed denial-of-service (DDos) attacks on websites, doxxing, impersonation, phishing, account hacking, and private digital threats, such as rape threats and threats against family.[2] Women targeted by GDTR, who operate within a variety of organizational contexts in the United States — their country of residence (host country) — engage in diverse forms of activism, journalism, and academic research and are

1 DTR describes a specific form of transnational repression and concerns how states use digital technologies against dissidents, critics, and other target populations with the goal to silence or repress voices beyond their territorial borders. See: Aljizawi, Noura, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert. "Psychological and Emotional War: Digital Transnational Repression in Canada." *Citizen Lab,* (2022). https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/

2 *Supra note 1.*

regularly targeted for this work. While some collaborate with transnational grassroots organizations, others maintain connections with entities in their countries of origin (home country). For some of these women, transnational advocacy constitutes full-time employment, whereas others voluntarily engage in such activities during their spare time. Additionally, a subset of these women are involved with more conventional institutions, such as universities or formal organizations, both within the United States and globally.

The focus on women's experiences in this research is informed by multiple factors. First, we highlight the vulnerability of exiled women within diaspora communities by focusing primarily on those originating from the Global South, where patriarchal norms continue to exert influence transnationally. This patriarchal environment can foster unsympathetic responses to GDTR from communities still in the state of origin. Such dynamics can exacerbate the isolation of women victims, particularly when targeting intersects with social norms and institutionalized forms of oppression in the U.S. This intersectionality often deprives these women of crucial support networks. Exiled women also often face a lack of robust social network support in their host countries, further compounding their vulnerability.

Another significant concern is the absence of organizational policies at their organizations, news agencies, or employers designed to safeguard women employees from technology-facilitated, gender-based violence. This issue is especially acute for exiled women, whose vulnerabilities are magnified by state or state-affiliated actors from their countries of origin targeting them.[3] Moreover, within the hierarchies of movements, institutions, and civil society organizations, women generally occupy less influential positions. Their status as exiled dissidents[4] — a term encompassing a broad category of individuals, including journalists, researchers, human rights defenders, advocates, and social and political activists — further compounds their vulnerability, as it limits their access to social support that might otherwise be available to women in their host countries. Another critical issue is the lack of funding and limited resources available to organizations and transnational advocacy groups addressing these challenges.[5] There exists a misconception that exile inherently provides safety, leading to the erroneous belief that exiled individuals and groups do not require the same level of resources for digital safety as do their counterparts in their home countries.

3 Aljizawi, Noura, Siena Anstis, and Marcus Michaelsen. "Transnational Repression Against Exiled Women Activists." *Middle East Research and Information Project MRIP, 307/308 (Summer/Fall 2023)*. https://merip.org/2023/09/exiled-women/

4 The term "dissidents" in this context refers to a broad category of individuals, including journalists, researchers, human rights defenders, advocates, and social and political activists.

5 Hudson, Alan. "NGOs' transnational advocacy networks: from 'legitimacy' to 'political responsibility'?." *Global networks* 1, no. 4 (2001): 331–352.

Research Objectives and Questions

This paper aims to address the following research questions:

1. What are the primary cybersecurity threats faced by transnational activists in the United States?
2. What cybersecurity measures, if any, do transnational activists employ to safeguard themselves?
3. What are the key areas for action and improvement to enhance the cybersecurity of transnational activists in the United States?

Literature Review

THE CYBERSECURITY CHALLENGES ENCOUNTERED BY UNDER-RESOURCED AND VULNERABLE ORGANIZATIONS

Public interest technology is an emerging domain as corporate developments in cybersecurity rapidly outpace the capabilities of the public sector and civil society.[6] Local governments often lag behind the industry in implementing robust cybersecurity practices, and academic research has not sufficiently focused on the unique cybersecurity challenges they face.[7] At the same time, cybersecurity guides available to groups like journalists are not adequately prioritized or tailored to their needs, leading to vulnerability and a false sense of security.[8] While support is available to politically vulnerable organizations (i.e., those that face cyberattacks from states, political opposition, and radical groups), including from human rights organizations like Access Now, The Citizen Lab, and Amnesty International, this support is often focused on emergency response and does not support long-term development of resilient cyber infrastructure.[9] Underserved populations such as low-income and foreign language-speaking communities often lack awareness of cybersecurity concepts, making it more difficult for them to access economic and social resources online, and leaving them especially vulnerable to scams and targeted attacks.[10]

A THREAT PROFILE OF DIGITAL TRANSNATIONAL REPRESSION

Targets of digital transnational repression often fall at the intersection of these many high-risk groups; as asylum seekers, refugees, and migrants to the U.S., they face economic and language barriers, while also being engaged in activism or journalism that leads to their targeting by state

6 Schneier, Bruce. "Cybersecurity for the Public Interest." *Schneier on Security*, (2019). https://www.schneier.com/wp-content/uploads/2019/02/Cybersecurity-for-the-Public-Interest.pdf

7 Preis, Benjamin, and Lawrence Susskind. "Municipal cybersecurity: More work needs to be done." *Urban Affairs Review* 58, no. 2 (2022): 614-629. https://journals.sagepub.com/doi/pdf/10.1177/1078087420973760

8 Berdan, Kristin. "An evaluation of online security guides for journalists." *Center for Long-Term Cybersecurity, University of California, Berkeley* (2021). https://cltc.berkeley.edu/wp-content/uploads/2021/01/Online_Security_Guides_for_Journalists.pdf

9 Brooks, Sean. "Defending politically vulnerable organizations online." *Center for Long-Term Cybersecurity*, University of California, Berkeley (2018). https://cltc.berkeley.edu/wp-content/uploads/2018/07/CLTC_Defending_PVOs.pdf

10 Sultan, A. H. M. A. D. "Improving cybersecurity awareness in underserved populations." *Center for Long Term Cybersecurity,University of California, Berkeley* (2019) https://cltc.berkeley.edu/publication/improving-cybersecurity-awareness-in-underserved-populations/

actors.[11] When International Partnership for Human Rights conducted an online survey of 98 human rights defenders in exile, primarily in Europe, most respondents indicated that human rights work was their main source of income, and those who did not pursue outside employment often contributed as volunteers or worked on a limited salary from an organization based in their country of origin.[12]

CYBERSECURITY FRAMEWORKS FOR ASSESSMENT

Several cybersecurity frameworks have been created for use by organizations to develop their infrastructure and by external parties to assess their security posture.

MITRE ATT&CK

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) — a comprehensive framework developed by the U.S. nonprofit organization MITRE — lays out common adversary tactics (e.g., reconnaissance, initial access, privilege escalation) and the techniques and procedures used to execute them.[13] MITRE ATT&CK also maps global threat actors by provenance, motivation, common targets, and tactical and technical strategies for which they are known. This allows very fine-grained assessment of specific organizational infrastructure and defense capabilities against specific groups: for example, in the 2022 paper "MITRE ATT&CK-driven Cyber Risk Assessment," Ahmed et al. were able to assess the vulnerability of a U.K.-based healthcare organization to attacks from Lazarus, a North Korean state-sponsored cyber threat group, and menuPass, a threat group with ties to the Chinese Ministry of State Security known to have targeted the healthcare sector.[14] While most enterprises use MITRE ATT&CK internally in their operations, many cybersecurity professionals lack confidence that they protect their

11 Scott-Railton, John. "Security for the high-risk user: separate and unequal." *IEEE Security & Privacy* 14, no. 2 (2016): 79–87. https://ieeexplore.ieee.org/document/7448342?denied= . See also: Nunez, Bryan, Elizabeth Eagen, Eric Sears, John Scott-Railton, and Michael Brennan. "Digital Security & Grantcraft Guide: an Introduction Guide for Funders." *Ford Foundation* (2017). https://www.fordfoundation.org/wp-content/uploads/2017/02/digital-security-grantcraft-guide-v10-final-22317.pdf

12 Beria, Tamar, Masha Chichtchenkova, and Anna Gerasimova. "Life in Exile: A Comprehensive investigation of the challenges facing and support provided to human rights defenders in long-term relocation." *International Partnership for Human Rights*. (2023). https://iphronline.org/wp-content/uploads/2023/12/iphr_life-in-exile_report.pdf.

13 Al-Sada, Bader, Alireza Sadighian, and Gabriele Oligeri. "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database." *IEEE Access* (2023). https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10365138&tag=1

14 Ahmed, Mohamed, Sakshyam Panda, Christos Xenakis, and Emmanouil Panaousis. "MITRE ATT&CK-driven cyber risk assessment." In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pp. 1–10. (2022). https://dl.acm.org/doi/pdf/10.1145/3538969.3544420?casa_token=WbcI7fKaTskAAAAA:xFoHReq3R9DzKc5l18gUwh8K72fBO1KtVQqqKmVWZgpa9Jpjalve7vKQDrg7X8QDRofsjSovJoY

organizations against the framework's tactics and techniques, and they often struggle to map event-specific data to these tactics and techniques and associated threats.[15]

NIST CSF

The National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF), which was updated to version 2.0 in February 2024, provides a more accessible framework that is divided into six key cybersecurity functions: Govern, Identify, Protect, Detect, Respond, and Recover. These are divided into categories and subcategories that outline specific tasks and considerations that organizations should be performing. This framework has been used in academic and professional settings to assess the cybersecurity of organizations such as local governments.[16] NIST has also been combined with MITRE ATT&CK in research on the cybersecurity of the Maine electric grid.[17] The Cybersecurity & Infrastructure Security Agency (CISA) has operationalized the NIST CSF into national Cybersecurity Performance Goals (CPGs), which are prioritized for accessibility to under-resourced organizations.[18] CISA has also created Project Upskill, a series of trainings aimed at individuals from communities "at heightened risk of targeting by threat actors who seek to undermine democracy and human rights."[19]

ISO 27001

ISO 27001 is an international standard directed at organizations building information security management systems. This framework uses risk assessment, and allows organizations to be certified for compliance. The most recent update (2022) is divided into 14 key areas, each split into categories with actionable tasks.[20] The standard has been used in academia to assess the cybersecurity of government institutions.[21] A review of ISO 27001 assessment case studies

15 Basra, Jasdeep and Tanu Kaushik. "CLTC and McAfee Study: MITRE ATT&CK Improves Security, But Many Struggle to Implement." *Center for Long-Term Cybersecurity, University of California, Berkeley,* (2020) https://cltc.berkeley.edu/publication/mitre-attck/

16 Ibrahim, Ahmed, Craig Valli, Ian McAteer, and Junaid Chaudhry. "A security review of local government using NIST CSF: a case study." *The Journal of Supercomputing* 74 (2018): 5171–5186. https://link.springer.com/content/pdf/10.1007/s11227-018-2479-2.pdf

17 Plummer, Benjamin. "Cybersecurity Policy Rubric and Analysis for the State of Maine Electrical Transmission Grid." (2023). https://digitalcommons.usm.maine.edu/cgi/viewcontent.cgi?article=1450&context=etd

18 Cybersecurity & Infrastructure Security Agency (CISA). "Cross-Sector Cybersecurity Performance Goals: March 2023 Update." (2023). https://www.cisa.gov/resources-tools/resources/cpg-report

19 Cybersecurity & Infrastructure Security Agency (CISA). "Project Upskill: Empowering high-risk communities with simple, how-to guides for digital protection." (2024). https://www.cisa.gov/audiences/high-risk-communities/projectupskill

20 International Standards Organization Security Control Framework. "ISO 27001 STANDARD." Accessed (March 31, 2024). https://www.cssia.org/wp-content/uploads/2020/01/ISO_27001_Standard.pdf

21 Maingak, A. Z., Candiwan, C., & Harsono, L. D. (2018). Information Security Assessment Using ISO/IEC 27001: 2013 Standard on Government Institution. *Trikonomika*, *17*(1), 28-37. https://journal.unpas.ac.id/index.php/trikonomika/article/view/1138

across four business types — a nonprofit, an educational institution, a group of enterprises, and a group of small and medium enterprises — revealed that, while none of the organizations was compliant, the nonprofit lagged far behind the others.[22]

Although these frameworks offer valuable tools for cybersecurity assessment and management, our analysis reveals a critical gap in their ability to fully address the needs of the most vulnerable and under-resourced organizations, individuals under threat of digital transnational repression, and others at high risk of nation-state cyber attacks. The complexity and lack of tailored support within existing frameworks often leave these groups inadequately protected. Given this gap, we developed a novel framework to code data from our interviews with targets of GDTR. We conducted five interviews with professionals from digital rights organizations, extracted key themes, and combined them with methods and activities from the SAFETAG framework described below.

SAFETAG

The Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG) is "a professional audit framework that adapts traditional penetration testing and risk assessment methodologies to be relevant to smaller non-profit organizations based or operating in the developing world." The framework was developed by Internews, a media support non-profit.[23] Designed with small civil society groups and independent media outlets in mind, the framework divides the task of auditing such organizations into 18 methods and 75 activities that are derived from standards and best practices, and tailored to the needs and limitations of these small organizations.[24] The Greater Internet Freedom project evaluated the performance, success, and impact of audits based on the SAFETAG framework by reviewing audit reports and interviewing and surveying auditors and audited organizations. They found that audits increase the security of organizations and change the attitudes and behaviors of members. However, audits must be a part of a broader strategy and management commitment to create lasting change, and audits are dependent upon the skill set of the auditor and can have negative impacts such as increasing fear and concern among staff.[25]

22 Hamdi, Zaidatulnajla, Azah Anir Norman, Nurul Nuha Abdul Molok, and Farkhondeh Hassandoust. "A comparative review of ISMS implementation based on ISO 27000 series in organizations of different business sectors." In *Journal of Physics: Conference Series*, vol. 1339, no. 1, p. 012103. IOP Publishing, 2019. https://iopscience.iop.org/article/10.1088/1742-6596/1339/1/012103

23 Safetag. (2024). "SAFETAG™: A Project of Internews." https://safetag.org

24 Safetag. (2024). "A Security Auditing Framework and Evaluation Template for Advocacy Groups." *SAFETAG™: A Project of Internews.* https://safetag.org/guides/Safetag_full_guide.pdf.

25 Greater Internet Freedom. (2023). ""Assessing the performance, success and impact of the SAFETAG audits implemented under the Greater Internet Freedom (GIF) project." *Greater Internet Freedom*. https://greaterinternetfreedom.org/wp-content/uploads/2023/09/Final-Evaluation-Report-Internews-GIF-SafeTag_FINAL-003.pdf.

Methodology

The research methodology includes the following:

I. **Data collection methods, such as surveys of victims and analysis of publicly available reports from organizations.**
Our team conducted 17 semi-structured interviews with woman-identifying victims of digital transnational repression who are currently living in the U.S. The interview questions focused on the domain of technology-facilitated, gender-based violence and cyberattacks. We focused on the nature of attacks experienced, the impacts of attacks, and any technical and non-technical measures taken by the individuals for security and prevention of future attacks. Where applicable, participants were asked about how these experiences and actions extended to their forms of organizing, whether through formal organizations or informal networks.

Additionally, to develop a cybersecurity framework suitable for exiled activists and transnational organizations, we conducted informal interviews with digital rights organizations that provide digital security assistance to exiled dissidents. These interviews gave insights into the latest trends in cyber threats, particularly those employed in DTR, and identified the most effective practices recommended to counter this growing threat.

II. **Data analysis techniques, encompassing comparison with cybersecurity standards and qualitative analysis through interviews.**
The team coded interview quotes using a framework combining methods from the SAFETAG Framework with new themes originating from interviews with staff from digital rights organizations, as detailed in the following section. Where specific quotes matched subcategories of the framework, this was noted.

Cybersecurity Framework for Coding Interviews with People Experiencing DTR

We interviewed staff at five digital rights organizations, which dedicate their work to defend and advocate for freedom and safety in digital spaces against issues like censorship, surveillance, and other digital safety violations. These organizations have experience working with groups experiencing DTR and state-sponsored attacks. Our interviewees were or had been employed at Access Now Digital Security Helpline,[26] CyberHUB-AM,[27] Internews,[28] Media Diversity Institute,[29] R3D Mexico,[30] and Reporters Without Borders (RSF) Digital Security Lab (DSL).[31] As we began coding the contents of our interviews with people experiencing DTR, a set of key themes and ideas emerged, as detailed below.

MIGRATION AND TRANSNATIONAL FACTORS

- Diaspora populations can sometimes be complicit in repression because they may face threats from their state of origin if they publicly support transnational advocacy or associate with transnational dissidents. This fear can lead members of these populations to distance themselves from transnational advocates in their diaspora communities, leaving transnational activists isolated and unsupported. Unlike governments' supporters or agents in the diaspora, diaspora communities practice a form of passive compliance due to the fear of retaliation or to avoid risking the safety of their families back home.
- Security choices should vary depending on the migration goals of the organization and individual: do they need a public platform to raise awareness on an issue? Can they return to their country of origin in the future? Do they wish to live a quiet life in their country of residence, or move to another country?

26 https://www.accessnow.org/help/
27 https://cyberhub.am/en/
28 https://internews.org/
29 https://www.media-diversity.org/
30 https://r3d.mx/
31 https://rsf.org/en/digital-security-lab

- Publishing technical and anecdotal reports of DTR instances is one of the most effective ways to encourage targets to adopt security practices. However, publication of such reports exposes security researchers to targeting.

FUNDING, CAPACITY, AND PRIVILEGE

- Cybersecurity assessments must consider the **capacity** of targeted people and groups. Multiple interviewees from digital rights organizations mentioned the importance of **multiple forms of capital** in cyber defense: groups with more funding are better prepared, but other forms of social capital, such as education, time, and public status, can make securing one's work easier.
- Democratic governments and other donors often **deny funding** to organizations that do not meet certain cybersecurity standards that are unrealistic for organizations experiencing DTR.
- Funders prefer to **focus on short-term projects** over building long-term cyber resilience.
- Organizations and individuals involved in transnational activism often **cannot afford software licenses** and use vulnerable, cracked versions of software.
- **States have access to special information about individuals**, such as dates of entry and exit, full names, addresses and visa statuses of family members, and health and employment information, all of which can be used to socially engineer **personalized phishing messages** to hack devices and install spyware.
- Personal information gained from surveillance (e.g., spyware, IMSI catchers) can be **used in smear campaigns** against activists. This can be **especially damaging for women, queer people, and other marginalized groups**.
- Because of historical patriarchy and male dominance in technology fields, most organizations nominate male-identifying members to work on IT and security, **leaving women and their specific security risks out** of the conversation.
- Some cybersecurity issues require **non-technical expertise and resources** to resolve (e.g., smear campaigns and impersonation).

These key themes were used alongside the applicable methods and activities from the SAFE-TAG framework to code interview quotes.

The Cybersecurity Posture of Transnational Dissidents: Vulnerabilities, Challenges, and Resilience

The following sections outline key themes that emerged in interviews, highlighting illustrative quotes and contrasts between the experiences of participants.

TECHNICAL VULNERABILITIES AND CAPABILITIES

The sub-themes in this section are taken from SAFETAG methods and activities.

Threat assessment

Organizations reported that they are skilled at threat identification, primarily by studying the contents and patterns of threat interactions. States self-identify as attackers in many attacks, including legal threats, arrest warrants, imprisonment, official statements and reports, and the targeting, questioning, and detention of family and other contacts. Many digital attacks, however, are anonymous and difficult to attribute to actors. These include spyware attacks, disinformation and smear campaigns, impersonation, mass coordinated harassment on social media, death and rape threats, phishing, surveillance, stalking, and more. Targets, however, are typically able to identify and attribute threats based on patterns in messaging, timing, and coordination. Targets notice that attacks mirror the language and narratives of disinformation spread by states; they are attacked by many Twitter accounts at once, all with similar profiles, statements, and patterns of interaction. Smear campaigns and threatening calls to loved ones are often timed to when targets are scheduled to speak, testify, or publish about human rights abuses in their countries of origin.

Many threats may also come from opposition groups. As an Iranian journalist-in-exile explained,

> *"Governments create oppositions that are quite similar to themselves in many respects. The impatience and narrow-mindedness present in the government also exist, to*

> *some extent, within various opposition groups and activists. There are opponents of the Islamic Republic who target and attack women, believing that there's only one way to oppose the Islamic Republic."*

Many threats come from within the U.S. and global diaspora, or from other unidentified netizens who do not appear linked to coordinated state-related attacks, as will be discussed further below.

Threats tend to disrupt the targeted organization's core function by exploiting technical vulnerabilities. In most cases, since the organization's main goal is advocacy and/or publication, the attackers' main goal is to discredit, smear, and shift the narrative. For activists with a large following on social platforms, attacks appear as public comments, disinformation, impersonation, and threats in private messages. Journalists are often targeted by hackers attempting to access their cloud accounts and de-anonymize their sources. Organizational blogs and websites are targeted with DDoS attacks and attempts to access sensitive research data on their servers.

Threats seek to discredit organizations not only within their diaspora communities, but also within the communities of their host states in order to create another threat: the host state and U.S. community itself. *"They threatened that they would contact our workplaces and label us as terrorists so that we would be fired,"* said one Iranian interviewee, whose U.S. employment was unrelated to her activism. In the case of a Rwandan activist:

> *"When the U.S. Congress adopted a resolution* [*related to my work*]*, they received messages from the Rwandans asking for amendments that talked about the denunciation of terrorism. . . . It almost would have been contrary to the goal of the resolution if they had included that amendment, but that was directly coming from the knowledge that they have received internally* [*from spyware surveillance*]*. . . . They are directly going up to people we're in touch with and trying to dissuade them from helping us."*

When targets are undocumented or at risk of visa cancellation or denial of an asylum application, threats and disinformation pitting targets against U.S. authorities can be a matter of life and death.

User device assessment

Most interviewees reported that they use specific device and application features to protect themselves, including Apple's Lockdown Mode, which limits apps, websites, and features such as message attachments that are often used to infect a phone with spyware.[32] They also use

32 Apple Support. "About Lockdown Mode." (2024). https://support.apple.com/en-ca/105120

privacy features to limit access to social media posts and block abusive accounts. An activist from Hong Kong running a nonprofit remarked, *"Now, when I block someone on Facebook, there is an option to say 'You are blocking this person and any other accounts this person has.' So it does help with limiting the kind of exposure one can get because this person cannot just start a separate account and not get banned."*

Many transnational dissidents depend on cloud services. For example, journalists and academics rely on data storage and communications platforms, including Google, Yahoo, iCloud, and encrypted communication platforms, to speak with sources; organizations with websites depend on web hosting and blogging services; and all interviewees depend on U.S. social media platforms in some capacity to publicize their work and messages. Some also reported using platforms specific to their countries of origin to communicate with contacts on the ground, particularly where using encrypted applications like Signal could draw the attention of authorities.

The SAFETAG cybersecurity framework has a specific activity to assess "A Night in the Life," or personal device usage. However, for most transnational activists, journalists, and dissidents, it is impossible to draw the line between personal and professional activities. The majority of those interviewed use their personal devices in some capacity for work and activism, face threats to their families, friends, and private dwelling, and limit their personal contacts and behavior at all times. A Moroccan former journalist recounted:

> *"Because I am a journalist, I have to answer calls, especially if they're from unknown callers, because usually it means someone from the government. Unfortunately, I do have to take those calls, and so I'm in a position where I always need to answer my phone. Oftentimes during that time period, the phone calls I could hear had someone breathing. I was getting texts indicating whoever was on the other side knew what I was up to."*

Organizational policy

While many interviewees and their organizations reported that they do not necessarily have a written security policy, most follow security policies in their professional and personal lives. Many interviewees use two-factor authentication and have password strength and security requirements across their accounts; some also use end-to-end encryption, VPN, and antivirus technologies. Some also choose communication and storage platforms based on the sensitivity of information, and share threat information and security practices within communities of others who are engaged in similar work.

Even for those working at established news agencies, academic institutions, and organizations with established information security policies, the policies they follow universally extend beyond written rules into their personal lives and habits. Most interviewees said that they have limited or stopped communication with relatives and friends living in their countries of origin to protect the safety of these contacts, and that they use certain procedures for reaching out to friends and others within the diaspora, often avoiding initiating contact to allow their contacts to actively accept the risk of communicating with them. Many said that they follow rules and take precautions about travel routines and public transit, safety features such as cameras and locks around their home, the neighborhood in which they choose to live, and the physical security of their devices.

Responding to advanced threats

Most targets we interviewed undertake some form of digital forensics and evidence capture, especially in reporting and attribution. This can include saving screenshots and records of attacks, studying patterns in the attacks they receive, tracing edited videos on social media to their original source, and researching perpetrators and their government connections. Many interviewees have worked with digital rights organizations to check for spyware infections, analyze phishing messages, or reach out to social media platforms where they were experiencing abuse. An activist from Buryatia explained that her team works together to research insider threats:

> *"With a group of activists, we identified one Security Service agent who was received by Putin. He tried to infiltrate our community. My colleague met him on Zoom, and he really wanted to meet me and* [*my organization*]. *She wrote about it in our common chat, and I opened a message history with him and saw that he wrote to me a lot. There are so many people like him who write constantly as if they really want to get involved in our activity and get into our team."*

Many interviewees have been in contact with U.S. law enforcement or the FBI about their targeting; however, they often find responses to be insufficient. A Uyghur activist experiencing an extensive smear campaign perpetrated by another diaspora member living outside the US explained:

> *"If there's one thing that I'm frustrated with those attacks, it's not those individuals but our system, our government. . . . Law enforcement should get involved and investigate him . . . and law enforcement should be able to work with social media, not allowing him to have those platforms, because without YouTube, without Facebook, he's nothing, he has no audience."*

Some interviewees explained that they were uncomfortable seeking help from law enforcement in their country of residence because they were members of communities that are subject to overpolicing, securitization, and police brutality, including Muslim communities and communities of color. Others did not trust state mechanisms of justice because of past experiences of being targeted by state apparatuses in their country of origin. An Egyptian academic explained:

> *"I'm not the type of a person who would report anything to the police . . . because I don't trust the police, and I don't believe in their ways of dealing with people. I don't believe in incarceration, I don't believe in prisons, so even if someone is attacking me personally, I don't think I would ever use the mechanisms of the state to protect myself."*

MIGRATION AND TRANSNATIONAL FACTORS

Interaction of migration and security dynamics

"To migrate is to exchange one problem for another," recounted a Venezuelan member of a research and advocacy organization. Like other interviewees, once she moved to the U.S., she was able to go public with her identity as an organizer and become the face of her organization. *"We never could register inside the country due to all the work that we do that is sensitive,"* she explained. State actors in her country of origin denied her entry and placed a block on her passport because it contained her U.S. visa, and the U.S. did not recognize the government of the ruling party.

For many, migration was the only safe option; at home, they were facing arrest, imprisonment, and threats to their families. By moving or fleeing abroad, they hoped for safety. An Ethiopian journalist explained:

> *"I left because I was arrested in Ethiopia . . . because of my journalism work. My imprisonment was harsh, and I experienced a lot of trauma while in prison. After I was released from prison, the surveillance continued. . . . I left because I couldn't live in Ethiopia anymore."*

An Azerbaijani journalist left the country because she faced threats to her children:

> *"One day on the way back from work, I received a phone call from a person telling me they were concerned about my personal safety and my children's safety. They named*

> *my kids, and they were watching my kids — they called me telling me that my kid was on his way to the kindergarten. I tried to investigate who the caller was and applied to the same body that was threatening me, but of course nothing came out."*

It is essential that collaborators who remain in the country remain anonymous. Cover stories are invented for organizational travel. We find that targets replicate and transport their fears from their countries of origin to countries of residence, which has clear implications for their security practices online and offline.

Threats within the diaspora community

"I have stopped seeing anyone coming from Azerbaijan," an Azerbaijani journalist told us, *"not because I don't trust these people, but because I know how manipulative the government is."* The majority of her YouTube channel's audience back home does not subscribe to her channel for fear it could impact their safety. A Uyghur journalist explained why some of the worst attacks come from within the Uyghur diaspora:

> *"They are affiliated with the Chinese government because they have a contract with the government: to keep their families safe inside China, they attack us.... Everyone in the diaspora has family members in the camps, whether direct or extended family members. Why can't we stand firm against the Chinese government?"*

An activist from Hong Kong noticed that coordinated accounts attempted to incite diaspora members unconnected to the state to attack her. She suspects that this form of co-optation is intentional:

> *"They're appealing to certain people with a huge nationalistic devotion to the CCP such that they would actually be the ones doing the offense. These people are not directed or instructed by the Chinese consulate or the Chinese government, so if the FBI was to look into it there would be no connections."*

She believes that women are more vulnerable to these random or coordinated attacks due to mobilization based on nationalism and misogyny. We find that attacks from within the diaspora community strongly influence targets' practices about interacting with others and how they perceive their security online and offline.

FUNDING, CAPACITY, AND PRIVILEGE

Organizations' capacity and socioeconomic factors

Some targets are full-time activists, either paid by a nonprofit or pursuing this work without compensation; others lack the financial resources to carry out their work on a full-time basis, and pursue activism around unrelated employment and other obligations like childcare.

> *"When I return home [from work], I engage with my children, and when they go to sleep, I get involved in activism. My American colleague goes home, and when the children sleep, maybe he goes out with his friends, and he goes fishing on weekends. I am busy with activism throughout the weekends. Our lives differ significantly from those of ordinary people, burdening us with a sense of conscience. For example, my daughter recently shared that her friend mentioned, 'My mom goes out with her friends,' and then she asked me, 'Why do you never go out? Why don't you have any fun? Why doesn't Dad have any fun?' This is because she consistently sees us either in front of a computer or engrossed in reading and writing."*

While dissidents employed by news agencies and nonprofits sensitized to transnational repression were more likely to receive support from employers, others did not feel safe seeking support at work. A Syrian activist explained:

> *"My supervisor is a white American, and he didn't understand the complex role that I played in the Syrian Revolution and what I was going through. In my career I had people say, 'We love you even though you're Muslim.' … When I went to HR, at one point they told me, 'You're amazing, you are such a poster child in the company, but I know you're a ticking time-bomb.' This is purely because I am a hijab Muslim woman in the workplace. This has nothing to do with my activism, but when I receive such comments, I don't feel safe to be able to sit down and have such conversations [about repression] with my employer or with my bosses. This was not a successful venue for me at all. I needed to work and make money to be able to live, to be able to be an activist, to be able to highlight the cause I care about."*

An Egyptian academic felt similarly unsupported by her university, saying, *"I don't trust or feel like the institution is a place for me to go to seek support. I feel like the institution is a place that I have to navigate, that I have to very carefully position myself in, because inherently they are not going to be on my side."*

Other forms of capital, such as the education level of members in digital security and related fields, the public profile of the organization or its leaders in the U.S., and connections to U.S. government support, were also factors that helped organizations respond more effectively to cyber threats. For instance, staff higher levels of staff education could help in promoting a better understanding of trending digital threats and increased adoption of cybersecurity practices. A public profile could attract more attention, resources, and allies to the organization and consequently enables the organization to mobilize support against attacks. Moreover, connections to the U.S. government can provide access to resources, funding, advice, and other support, all of which are essential for putting together robust cybersecurity strategies.

Information gained from state privilege/surveillance used in threats

States have access to classified and/or sensitive information about targets and their relatives, including identification, dates of travel, and visa information. Interviewees reported that they have had their passports and visas canceled, and faced imprisonment and arrest warrants with large bounties; many said that their family members have been threatened, questioned, and imprisoned back home. Beyond information to which they have direct access, states can also obtain information using surveillance tools such as spyware and internet monitoring. A Venezuelan activist explained, *"The main internet provider in Venezuela is a state company. So, by design, one of the things that we also had to do being inside Venezuela was to pay for satellite internet that cost 10 times more."*

States use this wealth of information in legal threats, in disinformation and smear campaigns, and in private threats detailing a target's location and means of attacking their family. A Uyghur activist explained, *"They posted my address and said, 'You're living in this house, we know where you live.'"* Others said that they had noticed vehicles and people watching their homes and received messages about their children's routines.

Disproportionate impact on women, queer, and marginalized groups

By focusing on women interviewees, this project has uncovered intersectional aspects of digital transnational repression. Women face rape threats and sexual accusations; a common tactic is to discredit their work by accusing them of having sexual relationships with American collaborators and government officials. Many women reported seeing edited photos and videos of themselves; *"There was a page on Facebook with a fake video of me, nude with my face on the body of the woman in the video,"* an Azerbaijani journalist reported.

Additionally, other aspects of women's identities are often weaponized. For instance, narratives from historical events, such as a genocide, in the women's country of origin can be used to target their identities. The invocation of such traumatic events to target exiled women dissidents aims to exploit deep-seated fears and collective memories, further marginalizing and silencing these women within their communities.

Threat actors also use dimensions of identity to discredit targets within their host communities, including race-based disinformation and Islamophobic narratives. Such disinformation can threaten individuals' legal status and harm their asylum applications; there is effectively a full siege against them, as they could face legal action from both their country of origin and host state. A Syrian activist explained:

> *"I used to wear the hijab so I was visibly Muslim. I received threats and aggressive messages. . . . I was either covering too much or I was not covering enough, depending on who was sending me those messages and who put me in what box. To some people I was viewed as a religious extremist and to others I was viewed as a U.S. liberal extremist . . . I never pleased a certain group, everyone seemed to be angry and threatening in one way or another just because of my mere existence and voice in the cause."*

Discussion of Findings

Overall, many themes from our coding framework applied thoroughly to the cybersecurity practices and vulnerabilities of transnational dissidents, who all had methods of assessing threats, personal and organizational security policies, risk modeling and investigation practices, and response procedures. The framework highlighted issues of capacity and funding, migration, intersectional oppressions, and other results of the power differential between states and individuals.

Certain codes, however, were discussed less often or manifested differently than expected. Beyond using VPNs and antivirus software, participants lacked capabilities to perform network mapping or vulnerability assessments of their organizations. Issues of software licensing did not come up in conversations about security practices. Interviewees used different applications for a variety of transnational purposes; recommending one encrypted platform for all activists is impossible, as targets cannot be forced to choose between being connected to people on the ground and using secure applications.

Recommendations

GENERAL CYBERSECURITY RECOMMENDATIONS

- **Funding:** Funders often do not allocate resources to help organizations enhance their cybersecurity or resilience; they may fund a project, but the organization does not have the resources to complete it securely, putting the organization and the people it works with at higher risk.
- **Resources:** Compliance-based cybersecurity resources (e.g., NIST, ISO 27001) are not appropriate for these groups as many requirements do not apply (e.g., they typically have no cybersecurity or IT staff, cannot afford software licenses, and have no routers to update). There is a need for a bottom-up framework that addresses the unique vulnerabilities of civil society organizations and individuals at risk, the state actors as perpetrators and their access to sophisticated digital surveillance technologies, and the limited resources that are available to the targets.

RECOMMENDATIONS TO U.S. GOVERNMENT AGENCIES

- In addition to intelligence gathering, U.S. law enforcement (i.e., police, FBI) should provide **prevention, mitigation, investigation, and follow-up support** to organizations facing transnational repression.
- Public institutions should fund **community alternatives to law enforcement**, particularly for dealing with transnational repression. This is because targets may feel uncomfortable working with state mechanisms of justice after being targeted by the same mechanisms in their country of origin. They also may have trauma from dealing with U.S. law enforcement because their community is subjected to overpolicing, securitization, and police brutality, or they may be undocumented or in the process of applying for asylum.
- Work with **all platforms** to ensure that communications are **secure by design**. It is not enough to recommend one end-to-end encrypted application for all activists, as contacts in the country of origin can have their devices seized and searched, and could be prosecuted for using a particular application.

RECOMMENDATIONS TO U.S. PRIVATE SECTOR

- Device manufacturers should **develop settings to protect users who face a heightened risk of state attacks**, such as Apple's Lockdown Mode, which limits message attachments, websites, and other features typically used to infect a phone with the sophisticated spyware used by state attackers.[33]
- Network providers, software manufacturers, and social media platforms should invest in tools for **forensics, evidence capture, and attribution** in the event of cyberattacks, and **avoid sharing data** with providers that may have an incentive to share it with regimes engaged in DTR.
- Social media platforms and other channels for public expression should invest in **trust and safety** measures that are **sensitive to regional and linguistic context**, and provide **public accountability tools** such as API access, which allows users and researchers to automate gathering content to study trends and behaviors on the platform. Several interviewees mentioned experiencing increased attacks on X (formerly Twitter) following changes that weakened trust and safety measures on the platform in late 2022. Some also mentioned being unable to identify threat actors and attribute threats due to a lack of access to API data from X, Facebook, Instagram, and TikTok.
- Platforms should continue to provide privacy features such as **private accounts, limiting direct messages, and blocking multiple accounts at once**.
- Platforms should develop clear policies about **false and/or doctored content discrediting activists, journalists, and academics**, and apply rules equally across all user types and languages. Just as many of these voices migrate to the U.S. to speak with greater freedom, they also migrate to U.S.-based platforms to evade censorship and surveillance while reaching international audiences.

GENDERED AND INTERSECTIONAL CONSIDERATIONS

- Many interviewees reported being targeted with doctored images and videos of them. As deepfake videos become easier for anyone to create, **platforms must consider measures for equal protection of all users**. When deepfake pornography of Taylor Swift was spread on X, the platform responded publicly and limited the ability of users to search for the video.[34] Proactive responses to this form of sexual violence should

33 *Supra note 32.*

34 Woods, Cat. "The spotlight cast by Taylor Swift's deepfake experience." *Law Society of NSW Journal Online.* (2024). https://lsj.com.au/articles/the-spotlight-cast-by-taylor-swifts-deepfake-experience/#:~:text=Rather%20than%20X%2C%20it%20was,removal%20of%20the%20explicit%20images.

not be reserved for celebrities, but should be given to all users who are targeted in this way, regardless of the size of their audience.

- While most interviewees used platform reporting tools to report very explicit content on social media platforms, they often received responses from the platforms saying that no policy had been violated, disincentivizing them from reporting further. Some reported a decline in helpful responses to reports (e.g., removal of harmful content, restrictions or bans of users who violated policy) on X following a shift toward automated content moderation on the platform in 2022.[35] Automated content moderation is not working, and patterns of failure lead to further problems in data used for training and fine-tuning. Platform reporting under the European Union Digital Services Act (DSA) shows low numbers of content moderation staff in most languages other than English.[36,37,38] **Platforms must invest more in other languages, dialects, and contexts in which disinformation can be spread**, and regulators must move to incentivize this through a U.S. counterpart to the DSA.
- The technology sector is white-, Asian-, and male-dominated;[39] by design, it is not inclusive. **Platforms must work with women and marginalized communities** to center platform designs and features around their experiences. This is not a favor to these communities, but a prerogative to design democratic and free global digital spaces.

35 Katie Paul and Sheila Dang, "Exclusive: Twitter leans on automation to moderate content as harmful speech surges," Reuters, December 5, 2022, https://www.reuters.com/technology/twitter-exec-says-moving-fast-moderation-harmful-content-surges-2022-12-03.

36 X. "DSA Transparency Report — April 2024." (2024). https://transparency.x.com/dsa-transparency-report.html

37 Facebook Inc. "Regulation (EU) 2022/2065 Digital Services Act Transparency Report for Facebook. (2023). https://transparency.meta.com/sr/dsa-transparency-report-oct2023-facebook/

38 Tiktok. "Tiktok's DSA Transparency Report October to December 2023." (2023). https://www.tiktok.com/transparency/en/dsa-transparency/

39 Google, Inc. "Google Annual Diversity Report 2023." (2023). https://static.googleusercontent.com/media/about.google/en//belonging/diversity-annual-report/2023/static/pdfs/google_2023_diversity_annual_report.pdf?cachebust=2943cac

Conclusion

Transnational activists, journalists, and researchers perform a variety of cybersecurity functions using their own resources and communities. Nonetheless, cybersecurity frameworks are not designed for their situations, and technology products and services do not meet their needs. Government actors and private companies can take a variety of actions to address these shortcomings and mitigate the harms of intersectional barriers to their security and advocacy for freedom.

Acknowledgments

Parts of the research and interview data for this paper were drawn from a forthcoming study on gender-based digital transnational repression (GDTR) undertaken by the Citizen Lab at the University of Toronto, coauthored by Noura Aljizawi, Siena Anstis, Marcus Michaelsen, Veronica Arroyo, Shaila Baran, Maria Bikbulatova, Gözde Böcü, Camila Franco, Arzu Geybulla, Muetter Iliqud, Nicola Lawford, Émilie LaFlèche, Gabby Lim, Levi Meletti, Maryam Mirza, Zoe Panday, Claire Posno, Zoë Reichert, Berhan Taye, and Angela Yang, with Ron Deibert as Principal Investigator.

We extend our gratitude to Luis Fernando García of R3D Mexico, Paolo Nigro Herrero of Access Now Digital Security Helpline, Artur Papyan of CyberHUB-AM and Media Diversity Institute, Viktor Schlüter of Reporters Without Borders (RSF) Digital Security Lab (DSL), and Jon Camfield, formerly of Internews, for participating in consultation interviews about cybersecurity frameworks.

Special thanks to John Scott-Railton and Jeffrey Knockel for their valuable feedback on drafts and their support in shaping the research. We thank Ron Deibert, the Director of The Citizen Lab, for his invaluable guidance, support, and leadership throughout this research project.

We are grateful to the University of California, Berkeley Center for Long-Term Cybersecurity (CLTC) for sponsoring this report and providing the necessary support. We also extend our thanks to Shannon Pierson for her invaluable assistance and support from the start of the process.

Most importantly, we would like to express our deepest gratitude to the survivors of DTR who shared their invaluable insights and experiences with us. Their courage and willingness to contribute are fundamental to the understanding and advancement of this critical area of study.

About the Authors

Noura Aljizawi is a senior researcher at the Citizen Lab, at the Munk School of Global Affairs & Public Policy, University of Toronto. Her research focuses on digital authoritarianism, disinformation, and digital transnational repression, informed by her background in human rights activism during the Syrian uprising. Aljizawi holds a Master's degree in Global Affairs from the University of Toronto and has been recognized for her work in online safety and digital security.

Gözde Böcü is a Ph.D. Candidate in the Department of Political Science at the University of Toronto, specializing in Comparative Politics and International Relations. Her research interests include transnationalism, migration, and authoritarianism. In her dissertation project, Gözde explores authoritarian diaspora policies and their effects on diasporas from a comparative perspective. She is a Doctoral Research Fellow at the Citizen Lab, where she focuses on digital transnational repression, cybersecurity, and human rights.

Nicola Lawford is a Citizen Lab Fellow and Master's Candidate in Technology and Policy at the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) Internet Policy Research Institute (IPRI). She holds a Bachelor's degree in Engineering Science, Electrical and Computer Engineering from the University of Toronto. Her work has focused on digital transnational repression, free expression, and privacy online.


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley