Security without Safety: Queering Cybersecurity in the Age of Digital Transnational Repression

Noura Aljizawi, Shaila Baran, Marcus Michaelsen, and Siena Anstis

Exiled activists increasingly face government-sponsored digital threats, including surveillance, hacking, and spyware, while residing in host states such as the United States, Canada, and the United Kingdom. This phenomenon, known as digital transnational repression (DTR), involves the use of digital technologies to track, intimidate, and silence individuals across borders. Drawing on interviews and questionnaire data with exiled women activists from Global Majority countries, this article focuses on a subset of participants who identify as queer to analyze how intersecting identities of gender and sexual orientation shape their experiences of DTR. We found that exiled queer activists were targeted with spyware and phishing, alongside threats of gendered violence, sexualized harassment and smear campaigns. Situating our analysis within an intersectional feminist framework, we analyze the experiences of exiled queer activists targeted with DTR and identify a critical protection gap that mainstream cybersecurity frameworks and technical-oriented approaches to DTR do not address the associated state-sponsored identity-based attacks and the social, reputational, and psychological harms caused by these threats. We conclude by adopting a duty of care framework, to reconceptualize the defense against DTR, moving beyond digital security toward safety.

1 Introduction

For exiled activists, the physical departure from a repressive regime's territory is often mistaken for an arrival at safety. However, the geographic borders that once provided sanctuary are increasingly rendered obsolete by transnational repression (TNR),[1] which is expanded and amplified by digital technologies. As authoritarian governments leverage digital surveillance and disinformation to monitor, harass, and silence dissidents abroad,

1. Following convention in this literature, transnational repression standing alone is abbreviated TNR, while the compound forms DTR and GDTR, both introduced below, render the same phrase without the N.

Journal of Online Trust and Safety 3 (3)
DOI: 10.54501/jots.v3i3.321
Research Article

Stanford Tech Impact and Policy Center

a new landscape of risk has emerged. This phenomenon, digital transnational repression (DTR), occurs when states use digital technologies to surveil, intimidate, and silence individuals living in exile or in the diaspora.

While existing studies focus on the different tactics and technologies used in DTR, less attention has been paid to the lived experiences of those navigating these threats. Such targeting is more than a technical phenomenon; it is politically motivated to facilitate the expansion of authoritarianism on a global scale. Our research on DTR at the Citizen Lab has addressed this gap by examining the experiences of targeted individuals and the overall impact on their lives (Aljizawi et al. 2024; Al-Jizawi et al. 2022). This gap becomes most visible when DTR intersects with gender and sexuality. For women and queer[2] activists, repression is inherently gendered, frequently weaponizing targets' identity through defamation, publicly disclosing their sexual orientation, doxxing, and reputational harm to silence or discredit individuals. These tactics are used alongside other forms of repression, including surveillance, the use of spyware, and other intrusive technologies. We define these dynamics as gender-based digital transnational repression (GDTR). While research on technology-facilitated gender-based violence (TFGBV) often situates online harassment against women as an extension of misogyny and within the broader patriarchal social norms (Henry and Powell 2015; Dunn 2020), our research demonstrates that state and state-related actors strategically exploit these ideas in politically motivated campaigns aimed at suppressing activists in exile.

Drawing on our interview data and questionnaire our analysis shows that responses to GDTR that rely primarily on standardized digital security training and 'cyber hygiene' practices (Gupta and Furnell 2022)[3] overlook the gender, social, immigration-related, legal, and psychological dimensions of GDTR. This creates a *protection gap*, leaving exiled queer activists vulnerable even after they secure their devices and online accounts.

We argue that a misalignment exists between the abstracted threat models of standardized digital training and the harm exiled queer activists experience in practice. Several research participants reported that technical measures enhanced their confidence in preventing hacking and account compromise; these interventions did little to mitigate identity-based attacks and their impacts. Therefore, it is not access to digital security training, but the framing of protection primarily in terms of device and account security. When safety is assessed through technical compromise alone, harms operating through reputation, relationships, and community standing remain unaddressed. In this context, responsibility and burden shift to targeted individuals to handle and manage these attacks that are social, political, and gendered in nature (Aljizawi et al. 2024).

Instead of treating safety as an individual responsibility to be fixed with more training, we reframe it as an institutional *duty of care* (De Guttry et al. 2018) that requires organizations

2. For the purposes of this article, queer is used throughout this study to identify sexual and gender minorities who do not identify as heterosexual and cisgender.

3. Cyber hygiene refers to a set of practices organizations and individuals perform regularly to maintain the health and security of users, devices, networks and data (Gupta and Furnell 2022).

and advocacy groups to protect their employees and volunteers and to recognize DTR as a significant labor risk for their exiled and queer members. Host states are also obligated to respond (Anstis and Barnett 2022) and adopt an institutional duty of care across agencies and throughout all stages of their responses to TNR. Duty of care refers to an obligation by institutions to implement policies, systems, and oversight to protect people under their authority (De Guttry et al. 2018). Extending the concept of duty of care involves treating threats beyond abstract and universal concepts and applying intersectional feminist frameworks to analyze the systemic and institutional vulnerabilities in overgeneralized cybersecurity models.

From an intersectional perspective, existing digital security training constitutes only one dimension of a more comprehensive conception of safety, which challenges cybersecurity models that prioritize the protection of infrastructure and state stability over embodied, relational and socially situated experiences of harm (Mhajne and Whetstone 2024). In this article, we argue that the mainstream cybersecurity frameworks and responses to digital threats are misaligned with the needs and lived realities of queer exiled activists, as these interventions are primarily focused on surveillance prevention and account protection. Using an intersectional feminist lens, we analyze how these activists describe the digital threats they have experienced and assess the effectiveness of the digital security guidance they received.

2 Literature Review

2.1 DTR and the Weaponization of Gender and Sexuality

Exiled queer activists experience overlapping forms of TNR, DTR, and GDTR. While these terms are related, they operate through distinct mechanisms. TNR broadly refers to the efforts of states to monitor, intimidate, coerce, or silence dissidents beyond their territorial borders. TNR methods vary, including physical attacks like assassination, assault, and kidnapping, co-opting countries, Interpol abuse, and mobility control like passport cancellation and denial of consular service (Schenkkan and Linzer 2021).

DTR is a subsection of TNR, and it occurs when the perpetrating state or state-related actors use digital technologies to surveil, intimidate, harass and silence dissidents in exile. As technology such as AI and the emergence of deepfake and sophisticated hacking software are evolving, governments are equipped with a variety of means to target activists and human rights defenders in exile. We can identify three levels of this repression chain: an identity-based level, including disinformation, deepfakes, smear campaigns, death threats, and defamation; a device level, including mercenary spyware, malware, targeted phishing, and DDoS attacks; and a network level, including telecommunications exploitation (SS7) and commercially available data (Anstis et al. 2026; Miller and Parsons 2023).

DTR can't be isolated from TNR; online threats often escalate into offline attacks. The digital targeting, tracking and subsequent abduction and torture of Saudi activist Loujain al-Hathloul illustrate how digital surveillance facilitates state-sponsored physical violence, including enforced disappearance, against dissidents in exile (Anstis et al. 2026). In 2018, al-Hathloul was abducted in the UAE and forcibly deported to Saudi Arabia. Upon arrival in Saudi Arabia, she was subjected to multiple detentions, interrogation, and severe torture, including threats of rape and murder (EFF 2021). During the interrogation and torture, she was confronted with her private communications, which were later weaponized in the court. This confrontation confirmed to al-Hathloul that she was targeted with a sophisticated surveillance technology before her abduction, which prompted her later in 2021 to file a lawsuit against the Emirati cyber-surveillance firm DarkMatter Group "for illegally hacking her iPhone to secretly track her communications and whereabouts" (EFF 2021). Since her release, al-Hathloul has remained subject to an arbitrary travel ban (HRW 2024) and to digital threats, including a "zero-click" attack with Pegasus spyware confirmed by the Citizen Lab (Schectman and Bing 2022).

Studying how DTR manifests indicates that there are additional forms of attacks based on gender and sexual identities when the targets are exiled women or queer activists. We refer to this understudied phenomenon as GDTR, which emerges at the intersection of DTR and TFGBV. While DTR research examines how authoritarian states use digital technologies to surveil, intimidate, and silence dissidents across borders, TFGBV scholarship focuses on gender-based harassment and abuse enacted through digital environments (Barter and Koulu 2021). GDTR brings this literature together by examining how authoritarian actors weaponize gender and sexuality as part of transnational repression strategies. Unlike many forms of online gender-based violence attributed primarily to misogyny or patriarchal social norms, GDTR involves state or state-aligned actors, transforming such abuse into a form of structured and politically motivated violence (Aljizawi et al. 2024; Michaelsen and Anstis 2025).

Exiled queer activists experience DTR through overlapping vulnerabilities that are best understood by bringing together Kimberlé Crenshaw's framework of intersectional feminism and queer theory (Chan and Howard 2020). Intersectionality explains how multiple systems of power overlap to produce distinct forms of marginalization (Crenshaw 1989). For exiled queer women, their experiences of gendered and sexualized attacks, including sexual and violent threats and doxxing, intersect with immigration status (e.g. asylum), isolation, exclusion, and economic and racial inequities. These intersecting identities shape exiled queer activists' offline experiences and the degree of anonymity, visibility, and safety they are able to maintain online. Building on this intersectional analysis, queer theory informs our analysis by interrogating the normative assumptions embedded within dominant security frameworks that privilege technical threats while marginalizing identity-based, relational and embodied harms (Mhajne and Whetstone 2025). Through this combined analytical lens, cybersecurity is not a neutral domain, but a sociotechnical system governed by power relations that dictate which threats are recognized and

whose safety is prioritized, and what forms of protection are considered legitimate. In this article, intersectionality and queer theory provide a framework for understanding exiled queer activists lived experiences related to surveillance, harassment, or exclusion while revealing the limitations of conventional cybersecurity approaches. Therefore, this article calls for queering cybersecurity by moving beyond technical protection and to recognize that systems are shaped by social norms and power, shaping participants' unequal experiences of safety, visibility, and community in digital spaces.

2.2 Trust, Safety and the Role of Platforms in DTR

As new forms of insecurity have emerged from digital platforms, researchers have defined trust and safety as the study of how people abuse the internet to cause real-world harm and as an umbrella term for companies that work to protect users from harmful experiences on social media platforms (Shulruff and Menking 2026). For activists, digital platforms facilitate engagement with professional and activist networks, political mobilization, information exchange, and the documentation or advocacy against human rights abuses (Michaelsen 2020). Consequently, digital platforms also create vulnerabilities that authoritarian regimes can exploit to monitor, intimidate, and target activists beyond borders. These attacks, including spyware, online harassment, and disinformation campaigns, are coupled with more traditional forms of transnational repression involving smear campaigns through state-controlled media, restricting travel, or, in extreme cases, facilitating physical violence and surveillance (Aljizawi et al. 2024).

In Amnesty's (2024) report on Thailand, women and queer activists were targeted with digital surveillance, including Pegasus spyware and online harassment, by state and non-state actors, in an effort to silence them. Niraphorn Onnkhaow, a student activist, received an Apple threat notification that her device was infected with Pegasus spyware (Amnesty 2024). Onnkhaow said these types of privacy invasions could be used to smear her and end her activism, noting that women and queer activists are "watched, monitored and scrutinized more closely" (Amnesty 2024). For exiled queer women, trust and safety are closely linked to transnational repression as they experience threats from authoritarian states and state actors while navigating social media platforms that respond inconsistently to gendered and sexualized attacks.

In Russia and throughout the MENA region, social media has served as a space for information sharing, community building, and organizing among LGBTIQ+ communities (Acconcia, Perego, and Perini 2024; Oz, Yanik, and Batu 2023).[4] However, these same digital environments have become sites of state control, surveillance, and intimidation amid intensifying internet censorship and state repression due to legal efforts in Russia to restrict LGBTIQ+ content in media, film, and online platforms, including investigations into apps and penalties against streaming platforms for materials with LGBTIQ+ themes (HRW 2025; York 2024). These experiences have led targets of transnational repression

4. This article uses the international term of LGBTIQ+ referring to people of diverse sexual orientations, gender identities and expressions, and sex characteristics (DNC 2025).

to withdraw from their digital public lives and delete their accounts due to fear of criminal convictions (HRW 2025).

Amid a global landscape in which authoritarian states and state actors exploit social media platforms to spread disinformation, hate speech, and targeted attacks, companies such as Meta scaled back their hateful conduct policy. These changes include limiting restrictions on topics such as gender identity and immigration, alongside the removal of explicit restrictions on content portraying women as property or objects (Heydari 2025). X (formerly Twitter) has also been contributing to creating this hostile online environment for queer people, including the removal of transgender protections from the hateful conduct policy and the changes in Community Guidelines, shifting from a "zero tolerance policy towards violent speech" to "we may remove or reduce the visibility of violent speech" (Amnesty 2025). Researchers and policymakers have reported concerns that these policy reversals may be associated with an increase in hate comments and abusive material, as some LGBTIQ+ people will likely self-censor or withdraw from online spaces altogether (Torek 2025).

The European Digital Services Act requires platforms to publish transparency reports on content moderation decisions (European Commission 2024). In response, platforms shared some reports which revealed parts of the alarming issues. For example, in X's 2024 disclosure on the number of staff working on content moderation issues and their language skills, only 1,535 staff members identified their primary language as English, with fewer than 100 staff members having language capabilities in Arabic, French, Polish, and German (X 2024). Digital platforms rely on Eurocentric frameworks and automated tools that often lack linguistic and cultural context, resulting in insufficient protection for users in the Global South and across Africa (Ayalew 2025). Tech companies tend to outsource moderation to third parties to manage different dialects within a language (Elswah 2024). These reports revealed human moderators are inexperienced, untrained, and underpaid, working in inhumane conditions, as found in Sama, a third-party vendor in Nairobi that provides content moderation services for tech companies, paying less than two dollars per hour (USD) (Hellerstein 2023).

For exiled queer activists, uneven forms of content moderation and reporting systems reveal the interconnection of technology, state power and vulnerability in an age of TNR. Yet, digital platforms categorize these attacks as bad actors or isolated harmful posts, which obscures the larger role that platform design and algorithms play in enabling harassment, surveillance, and abuse to spread. Furthermore, the absence of specific moderation categories fails to adequately capture gender-based state-sponsored online threats against journalists and human rights defenders in exile. (Gillett, Stardust, and Burgess 2022; Gillespie 2018). These uneven moderation practices extend to transgender users experiencing disproportionately high rates of content and account removals, with educational and medical content frequently misclassified as adult material (Haimson et al. 2021). Furthermore, inconsistencies in content moderation and account systems

place the burden of safety on users, requiring them to manage risk through privacy settings, blocklists, and content filters (Gillett, Stardust, and Burgess 2022). For exiled queer women who use social media to stay connected with their communities, navigating digital spaces becomes complicated as platforms introduce identity verification systems to protect users (Gillett, Stardust, and Burgess 2022). While these security measures seek to amend inconsistencies with existing platform policies, they put exiled queer women at risk of being tracked, stalked, and surveilled. In this context, technologies that claim to improve safety also increase vulnerability, demonstrating that platform power can protect and extend vulnerabilities toward exiled queer women, thereby requiring a queering of cybersecurity.

In this article, queering cybersecurity is the practice of rethinking cybersecurity as a system shaped by power and norms around gender and sexual identity, demonstrating how digital security training or tools expose vulnerabilities for queer and targeted diaspora groups experiencing DTR. For exiled queer activists, queering cybersecurity requires digital security training tailored to the specific intersectional risks that exiled queer and women activists experience. To do this, existing cybersecurity models must queer cybersecurity, which involves challenging the gendered, racialized, and cisheteronormative frameworks implicated in the practices and knowledge of cybersecurity and technologies (Basu and Biddolph 2025, 2). Queering, conceptually rooted in challenging heteronormative assumptions across fields of study, critically examines how power relations and norms related to gender, sexuality, and identity interact with overgeneralized cybersecurity practices by centering the experiences of exiled queer activists (Basu and Biddolph 2025). These experiences, as outlined in the upcoming questionnaire and interview data, demonstrate the significant impacts for the safety and security of targeted individuals, requiring an urgent need for queer-centric digital security training and durable protection mechanisms (Aljizawi et al. 2024).

3 Research Methods and Ethical Considerations

The interview and questionnaire data in this study were collected from the Citizen Lab's GDTR research project, which interviewed and questionnaires 88 exiled women human rights defenders who self-reported being targeted digitally by state or state-related actors. The interviews were conducted between August 2022 and March 2024 (For a detailed description of the broader study's methodology and data collection procedures, see). In this article, we focus on a subset of 18 interviews and seven responses to the questionnaire with participants who self-identified as LGBTIQ+. The research participants came from 9 different countries of origin and were living in 10 different host countries at

the time of the study.[5] In terms of their professional background, exiled queer women engaged in paid and voluntary human rights work, ranging from contractors at large non-governmental organizations, journalists, advocates, consultancy and more. Our analysis draws on original data to understand the current security trends and responses to GDTR and the misaligned needs and lived realities of exiled queer activists.

Studying DTR raises ethical and methodological challenges, particularly when focusing on the experiences of queer exiled activists. Targeted queer participants from the Global Majority navigate a complex web of vulnerabilities due to their intersecting identities, paired with their status as activists, and broader systemic issues that impact refugees, immigrants, and asylum seekers (such as precarious immigration status and being subject to anti-immigrant and discriminatory practices and policies). For researchers, this context creates unique ethical and security concerns regarding recruitment, communication, interviews, and data handling (Lim et al. 2025). From the design of our study to its execution, we adopted an intersectional and trauma-informed approach that recognized the potential harms resulting from exiled queer activists' experiences and minimized the risks and retraumatization associated with involvement in our research, ensuring that their voices could be heard while prioritizing their safety, agency, and anonymity.

In our research, we recognize that our identities shape how we understand and approach the intersectional implications of GDTR. As researchers based at the Citizen Lab, our work on DTR is driven by the commitment to social justice and well-being and to advancing policy, legal, and institutional change that supports those targeted by DTR. The research team focusing on GDTR at the Citizen Lab was composed of researchers both from the Global North and the Global Majority, exiled women activists and practitioners whose own intersectional identities shaped the design of the project, the questions we asked, and all the project outcomes. Our intersectional approach established the relationships of trust we built with participants and informed the shaping of the framework we brought to this analysis. Several team members share identities with the communities under study, including experiences of exile, political activism, and experiencing sexualized and gendered forms of transnational repression and its digital dimensions. We remain attentive to the power dynamics between researchers and participants, ensuring that our analysis captures their resilience and lived experiences. The lead author of this article is a woman human rights defender from the Global Majority who has personally experienced DTR, bringing lived insight to this analysis. All researchers approach this research in solidarity with the communities involved; several hold intersectional identities connected to these communities.

We addressed the potential security risks faced by participants through different mechanisms. For online interviews, we used secure end-to-end encrypted applications, specifi-

5. In our original study, participants originated from: Cuba, Guatemala, Venezuela, Morocco, Türkiye, Syria, Jordan, Egypt, Sudan, Rwanda, Burundi, Tanzania, Ethiopia, Eritrea, Yemen, Saudi Arabia, Bahrain, Iraq, Iran, Azerbaijan, Myanmar, Hong Kong, China, and Russia and live in: Canada, United States, United Kingdom, Belgium, Netherlands, Denmark, Norway, Sweden, Germany, Poland, Czech Republic, Austria, Switzerland, Spain, France, Türkiye, Georgia, Armenia, United Arab Emirates, Uganda, Kenya, Thailand, and Australia.

cally Signal and WhatsApp, as well as an encrypted asynchronous anonymous questionnaire administered through REDCap and hosted on the University of Toronto's secure servers. Questionnaire access required two-factor authentication, and researchers were granted role-based access only to the data necessary for their responsibilities. REDCap was selected based on its encryption (in-transit security and at-rest security), functionality to host on institutional servers, restriction of access to data for REDCap or any other third parties, the option for researchers to choose not to collect any personal identifying information on respondents, including IP addresses (REDCap, n.d.), and functionality allowing participants to complete the questionnaire in multiple sessions, which aligned with our duty-of-care commitments to participants.

We further strengthened participant confidentiality through rigorous anonymization procedures. Participants were given the choice of in-person or online interviews and assigned a unique identification code. Any direct identifiers to participants were stored separately from research data in encrypted, access-restricted files. Interviewees were pseudonymized by removing or replacing names, organizational affiliations and other potentially identifying information before analysis. All interviewees were referenced with pseudonyms in subsequent publications unless participants expressed interest and willingness to be named in the publications, which we respected and documented accordingly. Participants' names marked with an asterisk at first mention indicate the use of a pseudonym. Participants were also given the choice to be interviewed in English or their native language, given the linguistic diversity within widely spread diaspora communities.[6] Addressing the emotional and psychological impacts of GDTR, all team members have undertaken training on the research ethical protocol, including data privacy policy, trauma-informed approach in research, and intersectionality and how it shapes the experiences of participants, especially when it intersects with GDTR.

While interviews helped us to explore participant perspectives and experiences in greater depth, we recognized the potential barriers many people from these communities might face, including a lack of childcare, time to participate in an interview, and access to private or safe spaces. This study also recognizes the limitations in fully assessing access to training opportunities and the ways in which queer visibility may be weaponized for the purposes of DTR. To account for these barriers, we designed a questionnaire as an alternative means of participation for those who did not feel sufficiently safe or comfortable to be interviewed. The questionnaire helped our study reach queer women in exile and focus on the experiences and threats they faced as they identified and described them. To avoid epistemic injustice, where the voices of the most vulnerable are excluded from research because they are unable to participate in traditional means, we provide this anonymous questionnaire to create an accommodating and thoughtful alternative. Rather than treating 'queerness' as a variable, we centered participants' agency in defining their own safety and identity within their social and political contexts.

6. We conducted interviews in Arabic, Spanish, German, Russian, Turkish, Azerbaijani, Uyghur, Amhari, or Persian besides English.

4 Assessing Digital Security and Self-Protection Measures

Responses to our questionnaire reveal a gap between queerness and relevant digital security training. Many respondents chose not to disclose their sexual orientation, illustrating a potential *visibility paradox* in which greater visibility may increase exiled queer activists' exposure to threats and identity-based targeting (Fu and Cooper 2022).[7] These findings align with our interviews as several queer participants added that they were not open about their sexual orientation, whether in social or activism settings. While several non-queer respondents reported receiving digital security training in our questionnaire, none of the openly LGBTIQ+ respondents had accessed such support. These findings prompted this article's inquiry into whether current cybersecurity approaches exclude individuals at the intersection of exile, activism, and queerness who face GDTR.

Our questionnaire findings also reveal a disconnect between risk and protection as exiled queer activists face intensive gendered targeting while having the least security support. Crucially, this is not a gap in educational attainment, as the majority of queer respondents who chose to provide written responses hold either a university degree or a postgraduate qualification. Rather, our subsequent interviews suggest a systemic failure of the overgeneralized digital security ecosystem to offer relevant, intersectional, targeted, and human-centric defense mechanisms (Deibert 2018).

Existing cybersecurity practices and threat models must shift toward needs-based design rather than generic frameworks. Currently, existing standard modules fail to address the complex intersectional nature of the threats from state and state-related actors. These identity-based attacks are not merely technical; they weaponize the specific characteristics of exiled queer women's identities, including gender and sexual orientation, legal and socio-economic status, activism and social status. Consequently, mainstream defense mechanisms do not capture the unique risks of GDTR. Cybersecurity practices must account for these vulnerabilities to address an inequitable and insecure digital landscape, especially in the context of GDTR.

5 Protection Paradox: Gaps in Digital Security Training and Institutional Support

Our interviews revealed a paradox of protection: queer activists in exile experience digital repression alongside identity-based attacks, yet they are inadequately equipped to defend themselves against these threats. These attacks involve reputational and social harms specific to their sexual orientation and gender identity, involving doxxing, disinformation, deepfake imagery, and outing of exiled queer activists from state-

7. The visibility paradox in DTR refers to the contradictory statement that in order to effectively engage in activism and build communities, activists must be visible online, yet this same visibility makes them accessible to authoritarian states seeking to silence them (Fu and Cooper 2022).

sponsored attacks, which might be amplified by diaspora groups. Unlike questionnaire respondents, most queer participants in the semi-structured interviews reported having at least one digital security training, with some having attended more. During the 18 interviews with participants, we asked the 12 interviewees who accessed digital security training if there was anything related to gender, queer, or sexuality, but there was a significant consensus that these issues were not covered. They described these trainings as being overgeneralized for defending themselves against GDTR. Despite being employed by organizations and targeted because of their advocacy work, most exiled queer activists described experiences of institutional neglect and insufficient support.

5.1 Lack of Institutional Support

The participants we interviewed expressed a lack of institutional support from the organizations they worked with when they became targets of GDTR. Despite most participants reporting that they were being targeted by their country of origin because of their professional or advocacy work, the organizations they were associated with did not offer adequate support in the majority of cases.

Elif*, a transwoman journalist from Türkiye who is currently exiled in Germany, was the only trans journalist at the media outlet where she worked. She became the target of what she perceived as a massive online harassment campaign, where pro-regime networks targeted her across multiple platforms with death threats and sexualized insults. Offline, authorities in Türkiye interrogated her family members. Elif also described being targeted with queerphobic, racist, and other forms of intimidation within the pro-regime Turkish diaspora community in Germany. Determined to stand up for herself, Elif fought back against her perpetrators and wrote about her experiences and the serious impacts they had on her life. However, she felt that her organization offered no support. Her colleagues neither showed solidarity nor helped share her story to amplify her voice. This institutional abandonment is experienced through the refusal of mental health resources when she requested and not renewing her contract, resulting in the organization pushing Elif out, fulfilling the perpetrators' goal of professional and social isolation. As she observed:

> *"I even tried to make clear to them that I am the most marginalized person in this group, when I found out that the project funds were ending. I asked them for additional support, maybe a small permanent job, but they completely ignored all my requests [...] they started a new format [program] without me."*

This lack of support that Elif experienced was not an isolated incident. Arwa*, a queer human rights defender and artist from Yemen, did not receive legal or mental health support from her organization, despite benefiting from her journalistic contributions. During her position as an investigative journalist, she experienced doxxing, smear campaigns, and death threats, which she believes were sponsored by Yemen and the

UAE. They made her feel that her safety was solely her own responsibility:

> *"It made me very nervous working with organizations that, if something were to happen, I'm the only one that's gonna take care of myself, nobody's gonna be there for me, institutionally."*

Maha*, an exiled Syrian queer journalist, also expressed that she did not receive any support from her organization when she was experiencing Syrian state-sponsored online harassment and GDTR, observing that she "*did not know what to ask for.*"

This disconnection between participants and their organizations reveals a structural failure by institutions to anticipate and respond to identity-based threats against their staff, reflected in an absence of institutional support. Despite the substantial contribution of these activists to their organizations' work, the lack of duty of care reflected an institutional readiness or support. Standard security policies, onboarding, training, or support lack the vocabulary to address gendered and sexualized digital attacks, leaving their team members unprotected.

This pattern of institutional abandonment is demonstrated clearly in Gülnar's* narrative. She's a queer journalist from Azerbaijan exiled in Georgia, and she told us that when she became a target of GDTR, she believed it was sponsored by the Azerbaijani government. Gülnar told her organization but they did not provide any support or even acknowledgment of the burden of such a devastating experience:

> *"They expected me to continue work[ing] while I was facing these threats and harassment."*

Sofia*, an exiled queer researcher and investigative journalist from China, emphasized that threats not only disrupt current employment but also limit future opportunities. After being the target of what she believes was a widely spread gender-based online harassment campaign sponsored by the Chinese Communist Party, several international media outlets expressed interest in publishing her freelance work but hesitated to offer her a full-time position. She felt that she was being viewed as a liability:

> *"They are very interested in publishing whatever I write but they are hesitant to make me [] staff. Because then they will be responsible for my safety."*

When organizations such as Sofia's and Gülnar's prioritize liability avoidance over duty of care, they inadvertently reinforce authoritarian tactics by facilitating the economic and professional precarity of exiled dissidents.

These experiences shared by interviewees highlight a trend of institutional neglect. Exiled queer women's stories illustrate that, regardless of the size, popularity, and funding of these institutions, as well as the presence of cybersecurity policies and frameworks, they often fail to protect vulnerable individuals associated with them, particularly exiled queer activists. This situation places the burden of risk onto individuals rather than ensuring

collective safety.

When institutional support is available, it can significantly enhance the resilience of those targeted. Tala*, a queer journalist from Morocco working with several international and grassroots media outlets, described being targeted by her country of origin when her work, which was critical of the government, began to draw attention. She described being the subject of a spyware attack and extensive state-sponsored online harassment campaigns. Luckily, she did receive institutional support from the organizations, she was affiliated with, such as mental health and legal support:

> *"They were both incredibly supportive. I had access to all their resources, legal team, everything. They were ready at any moment to assist me."*

When exiled queer activists receive institutional support such as Tala, they avoid significant labor risks and are empowered to continue their transnational advocacy work. However, for Elif, Maha, Gülnar, Sofia, and other participants, the limitations within institutional support, such as in emotional, legal, and technical areas, constitute a protection gap rooted in the absence of organizational support, which places the burden of risk onto them rather than ensuring collective safety. These findings point to gaps in institutional duty of care considering exiled queer women's experiences with gendered and sexualized attacks linked to their activism and professional roles.

The experiences of Elif, Maha, Gülnar and Sofia directly intersect with the precariousness of gendered and digital labor, where their online participation, whether for freelance gig work, advocacy and volunteer work, demands tremendous emotional and immaterial labor (Gregg and Andrijasevic 2019). For these exiled queer activists, emotional labor translates into the constant, exhausting regulation of their online expression to meet social, professional, or political expectations and survive the hostile digital spaces. While their immaterial labor encompasses the unpaid roles, such as communication, identity, and social relations, that are required to sustain digital platforms and their activist networks (Arcy 2016). Consequently, exiled queer activists must navigate online spaces with hypervigilance, adjusting their behaviors in anticipation of how digital platforms, states, and their proxies might interpret their actions online. In this insecure environment, labor extends from producing online content to the invisible labor of managing security, reputation and risk (Bucher, Schou, and Waldkirch 2021; Romero 2026). Together, when self-expression carries the constant threat of state surveillance and sexualized and gendered risks, labor becomes intertwined with self-censorship and reputational labor, both of which respond to and reproduce existing structures of power.

5.2 Security without Safety: A Disconnect between Threats & Defense

Few queer participants had access to digital security training, and those who did described these sessions as introductory and general in scope. The workshops typically focused on account protection practices such as two-factor authentication, password

hygiene, encrypted messaging, and the use of VPNs. None of the participants reported that these trainings addressed gender-specific risks, sexualized harassment, disinformation, or reputational attacks. Instead, the curriculum was centered on digital security as protection against surveillance and device compromise.

Researchers from the Citizen Lab found, in their study of transnational grassroots organizations and dissidents, that civil society security support often prioritizes protection of devices, data, and accounts over responses to harassment, disinformation, and reputational attacks (Aljizawi, Böcü, and Lawford 2024). During the interviews, participants shared that these measures may mitigate surveillance risks and reduce the likelihood of account takeover and unauthorized access to targets' information. However, they fail to address the broader range of harm faced by activists, especially exiled women and queer activists, who remain feeling unsafe, even after attending these trainings. While safety is "highly contextual" (Strohmayer, Bellini, and Slupska 2022, 1) this asset-centric definition of security prioritizes the protection of organizations' assets and data, rather than a human at risk, who should be empowered to be safe from "bodily, emotional, and psychological harms" (2).

For example, Tala, the journalist from Morocco, attended several digital security workshops with different organizations. She explained that the sessions focused on preventing surveillance but overlooked the issue of gender-based violence:

> *"I received several cybersecurity training workshops in different places in three different organizations... It was mostly encryption, privacy, how to protect yourself from the threat or risk of surveillance. It was more oriented toward surveillance issue[s] than [] gender-based violence."*

For Tala, protected devices did not equip her against the Moroccan government's state-sponsored online harassment and other gender-based attacks.

Other participants identified a similar distinction between account security and personal safety. After receiving a warning from Google regarding a state-sponsored actor attempting to access her account, Maha, the exiled Syrian journalist, sought expert guidance and implemented the recommended safeguards. These measures relieved her anxiety about potential hacking attempts. However, she identified a more significant threat: coordinated disinformation and hate campaigns that undermined her credibility within her diaspora community. As she stated:

> *"I'm not as ... scared of being hacked as of this systematic misinformation, combin[ed] [with] real information, combina[ed] with hate speech, combinat[ed] with very personal attacks online, which eventually affected the way I'm being seen in my community."*

The attacks Maha faced targeted her credibility and belonging, not her data or devices. She identified the key harm as reputational and social, rather than only technical.

Sasha*, an exiled non-binary activist from Russia, offers a critical perspective on the limitations of digital security training in protecting dissidents from digital threats. Despite their grassroots organization implementing a strict digital security protocol, their data was inadvertently disclosed by other activist groups that were not attuned to the specific privacy and technical needs of exiled queer individuals. Shortly after, Sasha and their organization began receiving threats and messages addressed to them by name. Although Sasha believed that the extensive cybersecurity training they attended would keep them safe, the data leak and subsequent threats left them feeling unprepared for these types of harm:

> *"If we consider serious models of threats which we discussed, my knowledge is not enough. I would like to go deeper into how to minimize threats."*

Sasha's sense of being 'unprepared' originates from digital security training centered on securing organizational data but failed to address the specific vulnerabilities of exiled queer activists, leaving Sasha feeling unsafe and exposed to offline harms triggered by data leaks.

Shirin*, an exiled human rights defender from Iran living in France and a mother, experienced threats that extended to her family. She believes that both pro-Islamic Revolutionary Guard Corps trolls and supporters of Reza Pahlavi[8] employ similar methods of gender-based online harassment against women and queer activists. The attackers discovered her child's account on social media and began sending threatening messages, including threats to harm Shirin if she continued her activism:

> *"From videos of beheadings to sending pictures of knives, to saying they will catch me anywhere, etc., there are plenty of these kinds of things. Even threats are not just a single sentence; they describe what they might do with a knife, for instance."*

Shirin described the digital security training she received as "outdated," explaining that she already knew "basic stuff like two-factor authentication."

Digital security training programs tend to focus on digital threats as purely technical issues (Caramancion 2020; Caramancion et al. 2022). The reality described by participants is that they encountered a broad range of digital threats, including smear campaigns, sexualized harassment, outing, and death threats. These threats impacted their relationships, careers, well-being, migration status, and sense of safety. When applied to digital security frameworks and the capacity for self-protection measures, a feminist intersectional approach reveals that current programmings are generalized, do not capture or address how digital vulnerability is socially constructed and unevenly distributed. For exiled queer activists, vulnerability to GDTR does not only come from technical threats, but also from the violent interplay of their intersectional identities.

8. The exiled son of the last Shah of Iran who has positioned himself as an influential figure in the diaspora opposition to the Islamic Republic of Iran

To effectively *queer cybersecurity frameworks and responses*, these initiatives must move beyond devices security and tool-centric manuals to account for the unique safety needs, accessibility requirements, and gender sensitivities to address significant protection gaps for exiled queer activists. This means expanding the threat horizon to address attacks that disproportionately weaponize identities, including doxxing, outing, targeted disinformation campaigns and more. Digital security programs must fully address the needs of queer activists with a human-centric approach to digital safety and account for both prevalent among vulnerable, exiled, and queer populations. Ultimately, digital security programs and responses must pivot toward a human-centric approach (Deibert 2018), confronting both the protection gap and the "visibility paradox" that shape the lives and experiences of exiled queer dissidents.

Our participants' experiences expose a massive disconnect between the institutional threat models and the actual tactics of digital transnational repression and its gendered dimensions. In a previous study on enhancing cyber resilience, we analyzed several dominant cybersecurity frameworks against the threats we identified in interviews with GDTR targets. Dominant cybersecurity frameworks, such as MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), The National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF), and ISO 27001 operate on the assumption of a universal abstract adversary, overlooking how gender, sexuality, immigration status, and political visibility shape vulnerability (Strohmayer, Bellini, and Slupska 2022; Aljizawi, Böcü, and Lawford 2024), and the unique forms of GDTR they are subjected to (Caramancion 2020; Aljizawi, Böcü, and Lawford 2024; Aljizawi et al. 2024). In the context of GDTR, these harms are contextual; they are identity-based and intentionally designed to surveil, discredit, isolate, and threaten activists within their host countries. Consequently, by focusing exclusively on device-level security measures and securing organizational data, current digital security training and threat responses shift the burden for protection onto individuals, while overlooking how states frequently combine surveillance and technical targeting with intimidation and psychological pressure.

This article identifies two gaps to queer cybersecurity that existing cybersecurity programs must address. First, existing cybersecurity frameworks and responses emphasize technical methods and address the device-level threats. Second, these frameworks largely ignore how vulnerabilities are socially constructed and unevenly distributed. As a result, they fail to account for identity-based attacks and the relational, legal, and psychological harms resulting from digital threats such as defamation, disinformation, doxxing, deepfakes, outing sponsored by a state or state-related actors. These attacks extend beyond an organization's digital assets and target every aspect of a person's life, livelihood and well-being. Third, existing approaches place the burden of protection on exiled queer individuals while overlooking the institutional duty of care owed by organizations for participants engaged in gig, work advocacy, and volunteer labor that they coordinate, facilitate or benefit from. A duty of care approach requires institutions

to assess identity-specific risks and provide access to legal, psychological, and digital safety training. To queer cybersecurity, institutional responsibility is required to address the unequal distribution of risks and ensure that participants are not left to manage these harms alone.

The structural limitations identified by our participants suggest that queering cybersecurity has broader relevance beyond the specific context of exiled queer activists facing GDTR. Existing cybersecurity frameworks prioritize device-level defense, including infrastructural protection, asset defense, and surveillance prevention. While this level of defense is important, it overlooks identity-based attacks and the devastating impacts of social, emotional, and reputational harms. Yet many forms of technology-facilitated gender-based violence similarly rely on mechanisms of humiliation, isolation and reputational damage. These dynamics also extend to other populations whose digital vulnerabilities are shaped by precarity, racism, sexism, institutional dependency and unequal visibility, including migrant workers and Trust & Safety professionals operating under restrictive employment conditions. In such contexts, digital security is experienced not only through exposure to technical threats but also through concerns about social exclusion, professional limitations and psychological harm. A queer and intersectional approach to cybersecurity therefore offers an opportunity for a broader intervention, by addressing how digital harms are mediated through unequal social relations, identity-based vulnerabilities and power asymmetries across different digital environments and contexts.

6 Recommendations: Toward Intersectional Safety

In this article, our interviews and questionnaire reveal a misalignment between existing digital security training and the lived realities of exiled queer women targeted by GDTR. Current approaches to digital security involve general conceptualizations that do not account for authoritarian regimes exploitation of participants overlapping systems of vulnerability related to gender, sexual orientation, immigration, social status and more. We argue that addressing this protection gap requires a queering of cybersecurity in order to reconceptualize security beyond technical parameters to include the intersecting identity-based dimensions of digital threats.

6.1 Institutional Duty of Care

Organizations that employ or host exiled queer activists should move beyond a liability-avoidance approach toward an institutional duty of care that recognizes digital security as a collective organizational responsibility rather than an individual burden. Our findings revealed that exiled queer women are expected to independently manage state-sponsored digital threats in addition to intersecting forms of marginalization, trauma, and resource constraints from freelance, gig work or volunteer roles.

Organizations must adopt the duty of care as a prerequisite for participation in the organization's advocacy. They should invest in structural support, including legal support, psychological services, reputational management, and relocation when necessary for targets. This involves moving beyond cybersecurity toward digital safety and incorporating it as a core of their cultural and organizational practice, rather than an optional technical service, one-off training, or an emergency response.

As a few of our participants shared, when they became targets of DTR, their organizations chose to distance themselves from them, perhaps to minimize reputational risk. However, this neglect reinforces perpetrators' objectives of DTR, to isolate exiled queer women and sabotage the life they are rebuilding in exile. Beyond targeted individuals, this practice gradually empowers the authoritarian regimes to extend their control beyond borders and contribute to shrinking civic spaces in democratic contexts.

6.2 Reimagining the Path from Cybersecurity toward Digital Safety

Our participants' experiences reveal that a *secure device* doesn't equal a *safe* person. This requires adopting a human-centric intersectional safety framework that expands threat modeling to account for the unique risks queer activists in exile face, which devices' protection *alone* can't address. Reimagining the path from cybersecurity toward digital safety is essential for at-risk communities, particularly queer and women dissidents in exile. Through the lens of our participants, we argue that digital security training must move beyond generalized cybersecurity frameworks toward participant-centered, intersectional, trauma-informed and context-specific digital safety approaches. The curriculum should be co-designed with participants with lived experiences of DTR to ensure that training goes beyond abstract digital security models and incorporates the intersectional vulnerabilities that perpetrators weaponize. Training must include peer-to-peer learning networks, collectively interpret emerging threats and reduce isolation, thereby strengthening community resilience and challenging the objectives of DTR perpetrators.

6.3 Host States Responsibilities

In developing policy responses to DTR, host states should in their responses adopt a trauma-informed, intersectional approach, especially for women and queer activists. The intersecting identities of these targets should not prevent them from seeking support of host-country governmental institutions. Nonetheless, with increasing crackdowns on immigrants and queer individuals in the United States and Western democracies, targets of DTR may hesitate to report foreign state-sponsored digital threats, fearing that engagement with authorities in their host state could lead to secondary victimization (Wiggins 2026).

Host states must establish safe, civilian reporting institutions to receive and coordinate reports on TNR & DTR. These bodies should operate independently from immigration

enforcement and security agencies and should take all measures to protect information provided by targets, ensuring that they will be used solely for documenting, investing, and responding to foreign state-sponsored threats. Governments should communicate more across agencies and provide proactive intervention before DTR escalates into offline harm.

6.4 Platforms Responsibilities

As discussed earlier in this article, digital platforms in an age of AI, disinformation campaigns, hate speech, and more have limited their content moderation policies. In response to the disproportionate targeting of exiled queer women these platforms should establish dedicated reporting channels staffed by multilingual personnel trained to recognize the intersection of state-sponsored threats, and transnational repression and understand the cultural context and coordinated nature of these campaigns.

Digital platform's automated content moderation systems fail to recognize coordinated state-sponsored identity-based disinformation campaigns. It further places the burden on targets to submit evidence and proof attribution of coordinated attacks against them to a perpetrating state or state-related actors. This leaves participants without support or follow-up and despite all harmful impacts, allowing the harmful content to remain on their platforms and remain circulated and visible. To address this, platforms must treat these attacks as state-sponsored, rather than fragmented or one-off incidents that do not address the larger state-run repression. This involves tools that capture and preserve digital evidence to allow documentation of state-sponsored coordinated attacks in hopes of pursuing legal action and dedicated channels that reflect the intersectional vulnerabilities experienced by exiled queer women.

7 Conclusion

Our article has argued that for exiled queer activists from the Global Majority, current approaches to digital security training remain misaligned with the needs and lived realities of queer exiled activists. The disconnect between overgeneralized technical advice and the lived experiences of exiled queer activists manifests in a protection gap, whereby technical security and the protection of organizational assets are prioritized over measures that address vulnerabilities resulting from the intersecting identities of targets, such as gender, sexuality, immigration status, ethnicity, and race. When digital security training focuses primarily on device and account security, it risks losing sight of the broader context and conditions that shape targets' safety.

Queering cybersecurity is necessary in order to close this protection gap. This requires moving beyond narrow technical training centered on account and device security toward a framework that addresses identity-based attacks, which values collective resilience,

institutional solidarity, and an intersectional understanding of power. Safety cannot be reduced to the strength of a password, but it is also grounded in the assurance that when an exiled activist is targeted, they are not left unprepared for these unique attacks and must respond alone. As one of our research participants observed, "*solidarity is more than a hashtag*."

References

Acconcia, Giuseppe, Aurora Perego, and Lorenza Perini. 2024. “LGBTQ Activism in Repressive Contexts: The Struggle for (In)visibility in Egypt, Tunisia and Turkey.” *Social Movement Studies* 23 (2): 207–25. https://doi.org/10.1080/14742837.2022.2070739.

Aljizawi, Noura, Siean Anstis, Marcus Michaelsen, Vignesh Arroyo, S. Baran, M. Bikbulatova, Gözde Böcü, et al. 2024. *No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression.* Research report Research Report No. 180. The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto. https://citizenlab.ca/wp-content/uploads/2024/12/Report180-noescape112924.pdf.

Aljizawi, Noura, Gözde Böcü, and Nicola Lawford. 2024. *Enhancing Cybersecurity Resilience for Transnational Dissidents.* Research report. Center for Long-Term Cybersecurity, UC Berkeley. https://cltc.berkeley.edu/wp-content/uploads/2024/09/state-sponsoredCybersecurity_for_Transnational_Dissidents.pdf.

Amnesty International. 2024. *Thailand: “Being ourselves is too dangerous”: Digital violence and the silencing of women and LGBTI activists in Thailand.* Research report ASA 39/7955/2024. Amnesty International. https://www.amnesty.org/en/documents/asa39/7955/2024/en/.

———. 2025. *Poland: Twitter/X facilitated spread of anti-LGBTI hatred and harassment.* Research report EUR 37/0098/2025. Amnesty International. https://www.amnesty.org/en/documents/eur37/0098/2025/en/.

Anstis, Siean, and Barnett. 2022. “Digital Transnational Repression and Host States’ Obligation to Protect against Human Rights Abuses.” *Journal of Human Rights Practice* 14 (2): 698–725. https://doi.org/10.1093/jhuman/huab051.

Anstis, Siean, T. Surman, Noura Aljizawi, Marcus Michaelsen, and Ronald J. Deibert. 2026. *Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the Committee on Enforced Disappearances and the Working Group on Enforced or Involuntary Disappearances Report.* Research report. University of Toronto.

Arcy, Jacquelyn. 2016. “Emotion work: Considering gender in digital labor.” *Feminist Media Studies* 16 (2): 365–68. https://doi.org/10.1080/14680777.2016.1138609.

Ayalew, Yohannes Eneyew. 2025. “A Third-World Critique of the International Human Rights-Based Approach to Content Moderation.” *Transnational Legal Theory* 16 (4): 546–77. https://doi.org/10.1080/20414005.2025.2523184.

Barter, Christine, and Sanna Koulu. 2021. "Digital Technologies and Gender-Based Violence – Mechanisms for Oppression, Activism and Recovery." *Journal of Gender-Based Violence* 5 (3): 367–75. https://doi.org/10.1332/239868021X16315286472556.

Basu, Soumita, and Craig Biddolph. 2025. "Queering cybersecurity: an alternative research agenda." *Critical Studies on Security,* 1–25. https://doi.org/10.1080/21624887.2025.2502716.

Bucher, Eliane L., Peter K. Schou, and Matthias Waldkirch. 2021. "Pacifying the algorithm: Anticipatory compliance in the face of algorithmic management in the gig economy." *Organization* 28 (1): 44–67. https://doi.org/10.1177/1350508420961531.

Caramancion, Kevin Matthe. 2020. "An Exploration of Disinformation as a Cybersecurity Threat." In *Proceedings of the 2020 3rd International Conference on Information and Computer Technologies,* 440–44. https://doi.org/10.1109/ICICT50521.2020.00076.

Caramancion, Kevin Matthe, Yusheng Li, Elizabeth Dubois, and Edward S. Jung. 2022. "The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats." *Data* 7 (4). https://doi.org/10.3390/data7040049.

Chan, Chaddrick D., and Lionel C. Howard. 2020. "When Queerness Meets Intersectional Thinking: Revolutionizing Parallels, Histories, and Contestations." *Journal of Homosexuality* 67 (3): 346–66. https://doi.org/10.1080/00918369.2018.1530882.

Crenshaw, Kimberle. 1989. "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics." *University of Chicago Legal Forum* 1989 (1): 139–67. http://chicagounbound.uchicago.edu/uclf/vol1989/iss1/8.

De Guttry, Andrea, Micaela Frulli, Edoardo Greppi, and Chiara Macchi. 2018. *The Duty of Care of International Organizations Towards Their Civilian Personnel: Legal Obligations and Implementation Challenges.* T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-258-3.

Deibert, Ronald J. 2018. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32 (4): 411–24. https://doi.org/10.1017/S0892679418000618.

Dignity Network Canada. 2025. *Canada's Foreign Policy on Global LGBTIQ+ Rights: A Summary of a 10-Year Assessment (2016–2025).* Research report. Dignity Network Canada. https://dignitynetwork.ca/wp-content/uploads/2026/04/Canadas-Foreign-Policy-on-LGBTIQ-Rights-EN.pdf.

Dunn, Suzie. 2020. *Technology-Facilitated Gender-Based Violence: An Overview.* Research report Supporting Safer Digital Spaces Paper No. 1. Centre for International Governance Innovation. https://www.cigionline.org/static/documents/SaferInternet_Paper_no_1_coverupdate.pdf.

Electronic Frontier Foundation. 2021. "Saudi Human Rights Activist, Represented by EFF, Sues Spyware Maker DarkMatter for Violating U.S. Anti-Hacking and International Human Rights Law." Electronic Frontier Foundation, December 9, 2021. https://www.eff.org/press/releases/saudi-human-rights-activist-represented-eff-sues-spyware-maker-darkmatter-violating.

Elswah, Mona. 2024. *Moderating Maghrebi Arabic Content on Social Media.* Research report Supporting Safer Digital Spaces Paper No. 1. Centre for Democracy and Technology. https://cdt.org/insights/moderating-maghrebi-arabic-content-on-social-media/.

European Commission. 2024. "Digital Services Act Transparency Database." European Union. https://transparency.dsa.ec.europa.eu/.

Fu, Jiayan S., and Kimberly R. Cooper. 2022. "Reconsidering Communication Visibility in Politically Restrictive Contexts: Organizational Social Media Use in China." *Journal of Communication* 72 (5): 540–52. https://doi.org/10.1093/joc/jqac024.

Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media.* Yale University Press. https://doi.org/10.12987/9780300235029.

Gillett, Rosalie, Zara Stardust, and Jean Burgess. 2022. "Safety for Whom? Investigating How Platforms Frame and Perform Safety and Harm Interventions." *Social Media + Society* 8 (4). https://doi.org/10.1177/20563051221144315.

Gregg, Melissa, and Rutvica Andrijasevic. 2019. "Virtually Absent: The Gendered Histories and Economies of Digital Labour." *Feminist Review* 123 (1): 1–7. https://doi.org/10.1177/0141778919878929.

Gupta, S., and Steven Furnell. 2022. "From Cybersecurity Hygiene to Cyber Well-Being." In *International Conference on Human-Computer Interaction,* 103–15. Springer, Cham. https://doi.org/10.1007/978-3-031-05563-8_9.

Haimson, Oliver L., Daniel Delmonaco, Peipei Nie, and Alan Wegner. 2021. "Disproportionate Removals and Differing Content Moderation Experiences for Conservative, Transgender, and Black Social Media Users: Marginalization and Moderation Gray Areas." *Proceedings of the ACM on Human-Computer Interaction* 5 (CSCW2): 1–35. https://doi.org/10.1145/3479610.

Hellerstein, Erica. 2023. "In Nairobi's Silicon Savanna, African Workers Are Taking On Big Tech." *Coda Story,* October 11, 2023. https://www.codastory.com/authoritarian-tech/kenya-content-moderators/.

Henry, Nicola, and Anastasia Powell. 2015. "Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence." *Violence Against Women* 21 (6): 758–79. https://doi.org/10.1177/1077801215576581.

Heydari, Anousha. 2025. "Meta Says New Rules Prioritize Freedom of Expression, but Even Civil Liberty Advocates Have Mixed Feelings." *CBC News,* January 15, 2025. https://www.cbc.ca/news/business/meta-moderation-language-1.7428480.

Human Rights Watch. 2024. *Saudi Authorities Must End Misuse of Administrative and Judicial Measures Against Released Human Rights Defenders Including Loujain al-Hathloul.* Research report. Human Rights Watch. https://www.hrw.org/news/2024/10/31/saudi-authorities-must-end-misuse-administrative-and-judicial-measures-against.

———. 2025. *Russia: Rising toll of LGBT 'extremism' designation.* Research report. Human Rights Watch. https://www.hrw.org/news/2025/06/30/russia-rising-toll-of-lgbt-extremism-designation.

Al-Jizawi, Noura, Siean Anstis, Sharlychan Barnett, S. Chan, N. Leonard, A. Senft, and Ronald J. Deibert. 2022. *Psychological and Emotional War: Digital Transnational Repression in Canada.* Research report Research Report No. 151. The Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto. https://citizenlab.ca/research/psychological-emotional-war-digital-transnational-repression-canada/.

Lim, G., Noura Aljizawi, S. Baran, and Nicola Lawford. 2025. "Avoiding the Kitchen Sink: A Guide to Mixed Methods Approaches within Digital Rights Governance." *Internet Policy Review* 14 (4). https://doi.org/10.14763/2025.4.2044.

Mhajne, Anwar, and Crystal Whetstone. 2024. "A feminist cybersecurity: addressing the crisis of cyber (in) security." *International Affairs* 100 (6): 2341–60. https://doi.org/10.1093/ia/iiae234.

———. 2025. "Redefining (In-) Security in Cybersecurity: An Intersectional Lens." In *Handbook on Gender and Security,* 397–408. Edward Elgar Publishing.

Michaelsen, Marcus. 2020. *The Digital Transnational Repression Toolkit, and Its Silencing Effects.* Research report. Freedom House. https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects.

Michaelsen, Marcus, and Siean Anstis. 2025. "Gender-Based Digital Transnational Repression and the Authoritarian Targeting of Women in the Diaspora." *Democratization* 32 (6): 1518–40. https://doi.org/10.1080/13510347.2025.2476178.

Miller, Gary, and Christopher Parsons. 2023. *Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure.* Research report Report No. 172. The Citizen Lab, University of Toronto. https://citizenlab.ca/research/finding-you-teleco-vulnerabilities-for-location-disclosure/.

Oz, Mustafa, A. Yanik, and M. Batu. 2023. “Under the Shadow of Culture and Politics: Understanding LGBTQ Social Media Activists’ Perceptions, Concerns, and Strategies.” *Social Media + Society* 9 (3). https://doi.org/10.1177/20563051231196554.

REDCap. n.d. “REDCap Mobile App Privacy Policy.” Project REDCap. Accessed June 27, 2026. https://projectredcap.org/software/mobile-app/privacypolicy/.

Romero, G. 2026. “Digital Surveillance Is Breaking Activist Mental Health.” Global Voices, June 23, 2026. https://globalvoices.org/2026/06/23/digital-surveillance-is-breaking-activist-mental-health/.

Schectman, Joel, and Christopher Bing. 2022. “Insight: How A Saudi Woman’s iPhone Revealed Hacking Around The World.” *Reuters,* February 17, 2022. https://www.reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/.

Schenkkan, Nate, and Isabel Linzer. 2021. *Out of Sight Not Out of Reach: The Global Scale and Scope of Transnational Repression.* Research report. Freedom House. https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf.

Shulruff, T., and A. Menking. 2026. ““I tend to run to problems that people run away from”: Emotion as an Essential Asset in Trust and Safety Work.” *Journal of Online Trust and Safety* 3 (2). https://doi.org/10.54501/jots.v3i2.288.

Strohmayer, Angelika, Rosanna Bellini, and Julia Slupska. 2022. “Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety.” *IEEE Pervasive Computing* 21 (3): 61–69. https://doi.org/10.1109/MPRV.2022.3182222.

Torek, B. 2025. “Meta’s New Policies: How They Endanger LGBTQ+ Communities and Our Tips for Staying Safe Online.” Human Rights Campaign, May 20, 2025. https://www.hrc.org/news/metas-new-policies-how-they-endanger-lgbtq-communities-and-our-tips-for-staying-safe-online.

Wiggins, Christopher. 2026. “U.S. Deports Gay Asylum Seeker to Country Where Homosexuality Is Illegal.” Advocate. https://www.advocate.com/news/gay-immigrants-dangerous-deportations.

X. 2024. *DSA Transparency Report, October 2024.* Research report. X. https://transparency.x.com/dsa-transparency-report.html#/.

York, Jillian C. 2024. “The Global Suppression of Online LGBTQ+ Speech Continues.” Electronic Frontier Foundation, June 27, 2024. https://www.eff.org/deeplinks/2024/06/global-suppression-online-lgbtq-speech-continues.

Authors

Noura Aljizawi is a Senior Researcher at the Citizen Lab at the University of Toronto's Munk School of Global Affairs and Public Policy. Her research specializes in the intersection of technology, human rights, and global security, with a focus on digital authoritarianism and transnational repression. Grounded in trauma-informed and intersectional approaches, her work is uniquely informed by her background as a prominent figure in the Syrian uprising and her experience as a survivor of political detention. She is the Chair of Verify-Sy, a leading independent fact-checking and media monitoring platform, and the founder of Start Point, an NGO providing human rights advocacy and psychosocial support for formerly detained Syrian women, and she serves on the board of the Center for Victims of Torture. Aljizawi is a member of the Humanitarian Dialogue expert group and the steering committee of the Just Tech and Migration Community. Her research has been published in peer-reviewed journals and research volumes, including Democratization, Internet Policy Review, and the Center for Long-Term Cybersecurity. She holds a Master of Global Affairs from the University of Toronto. She is the recipient of the University's Excellence Through Innovation Award and the Janice Stein Alumni Leadership Award. Email: noura@citizenlab.ca.

Shaila Baran is a Ph.D. candidate with a background in criminology, sociolegal studies and internet studies, and a researcher at the Citizen Lab, where she explores transnational repression, dis- and misinformation and social movements.

Marcus Michaelsen, PhD, is a researcher studying digital technologies, human rights activism and authoritarian politics. He works as a Senior Researcher at the Citizen Lab based at the Munk School of Global Affairs and Public Policy, University of Toronto, where he focuses on digital transnational repression. Previously he was a Marie-Skłodowska-Curie Fellow in the Law, Science, Technology and Society (LSTS) research group of Vrije Universiteit Brussel and a Senior Information Controls Fellow with the Open Technology Fund, a non-profit organization supporting global internet freedom. From 2014 until 2018, Dr. Michaelsen was a post-doctoral researcher in the project Authoritarianism in a Global Age in the Political Science Department of the University of Amsterdam. His work on transnational repression has been published in Democratization, Globalizations, the European Journal of International Security, and Surveillance & Society, among others.

Siena Anstis is a senior legal advisor at the Citizen Lab. She is a lawyer admitted to practice in Ontario and New York and a researcher in the areas of international law, human rights, technology, and migration. She has worked as a refugee lawyer in Canada, a litigation associate at Morrison Foerster LLP in New York City, and as a judicial clerk at the Supreme Court of Canada (2015-2016) and the Court of Appeal for Ontario (2014-2015). She holds a Master of Law from the University of Cambridge (2020), a Bachelor of Laws and Bachelor of Civil Law from McGill University (2014), and a Bachelor of Arts in journalism and anthropology from Concordia University (2009). She is currently

completing a PhD in Law at the University of Oslo.

Acknowledgments

Parts of the research and interview data for this paper were drawn from a study on gender-based digital transnational repression (GDTR) conducted by the Citizen Lab at the University of Toronto, which was supervised by Professor Ronald Deibert, principal investigator, under the University of Toronto Research Ethics Protocol # 42719, and 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.

We extend our sincere gratitude to the participants who shared their knowledge, lived experiences, and perspectives through interviews for this report. Their contributions reflect diverse experiences and forms of expertise that are central to understanding human rights activism. We recognize the care, trust, and emotional labor involved in sharing these experiences, and we honor the participants' agency and leadership in shaping this research.

We would like to express our gratitude to the guest editors of this special issue, Sujata Mukherjee, Mona Elswah, and Crystal Abidin for their guidance and support throughout the publication process. We also thank the anonymous reviewers for their insightful comments and constructive feedback, which improved the article.

Finally, we thank Claire Posno for her editorial assistance and Emile Dirks for his review of earlier drafts of this paper.

Data Availability Statement

The data supporting the findings of this study are not available due to ethical, security and institutional considerations. This restriction is a core component of our intersectional and trauma-informed methodological and ethical framework, designed to recognize and mitigate the profound risks our research participants face, including state-sponsored online and offline threats, transnational activism, intersectional identities, and precarious immigration or legal statuses in host states. In accordance with the research ethical protocol approved by the University of Toronto Research Ethics Protocol (REB), research data cannot be shared with third parties and are strictly restricted only to the approved purposes of this research.

Funding Statement

This research was supported by the general operating funds of the Citizen Lab at the University of Toronto. No specific grant or outside funding was allocated for this paper. A list of Citizen Lab funders is available at https://citizenlab.ca/who-we-are/.

Ethical Standards

The study from which this article's research and interview data are drawn was conducted under University of Toronto Research Ethics Protocol # 42719.

Competing interests: Noura Aljizawi is Chair of Verify-Sy, an independent fact-checking and media monitoring platform; Founder and Chair of Start Point, a human rights advocacy and psychosocial support NGO; a Board Member of the Center for Victims of Torture; an Expert Group Member of Humanitarian Dialogue; and a Steering Committee Member of the Just Tech and Migration Community. Shaila Baran, Marcus Michaelsen, and Siena Anstis declare no competing financial or non-financial interests. The authors declare no competing financial interests.

Keywords

Digital transnational repression; cybersecurity; digital threats; intersectionality; duty of care.