NO ESCAPE

The Weaponization of Gender for the Purposes of Digital Transnational Repression

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

DECEMBER 2, 2024
RESEARCH REPORT #180

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THE CITIZEN LAB

Copyright

Electronic version first published by the Citizen Lab in 2024. This work can be accessed through https://citizenlab.ca/2024/12/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/

Document Version: 1.0

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Content Warning: This report examines digital transnational repression with a focus on its gendered dimensions and impacts. It includes discussions on topics such as online harassment, targeted surveillance, and intimidation tactics that disproportionately affect women, LGBTQ+ individuals, and marginalized communities. Readers may find descriptions and analyses of these repressive tactics distressing and potentially triggering, especially those with personal or family histories related to such experiences. We encourage readers to approach the report with care and to access support if needed.

Acknowledgements

This project was supervised by Professor Ronald Deibert, principal investigator, under the University of Toronto Research Ethics Protocol # 42719, “The Gender-Dimensions of Digital Transnational Repression.”

We acknowledge and thank all research participants who generously participated in interviews for this report and shared their personal experiences with us. Their stories demonstrate the courage required to engage in human rights activism and we are grateful for their willingness to speak with us.

We also thank Cynthia Khoo, Alice Nah, Alexandra Haché, and Katty Alhayek for their peer review of this report; Adam Senft and Céline Bauwens for copyediting and providing assistance in the publication process; Bill Marczak, Bahr Abdul Razzak, John Scott-Railton, and Alberto Fittarelli for their assistance in digital investigations; Snigdha Basu, Alyson Bruce, and Mari Zhou for their assistance in designing and formatting this report; Ryookyung Kim for the cover and internal illustrations; and Este Orantes Migoya for their assistance with translations.

Suggested Citation

Aljizawi, Noura, 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. “No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression,” Citizen Lab Report No. 180, University of Toronto, December 2024. Available at: https://citizenlab.ca/2024/12/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/

Contents

Contents

Introduction

Background to our Research Program on Digital Transnational Repression

Noushin's story[1]

Noushin works for a news website run by Iranian journalists in the diaspora. She covers the human rights situation in Iran and the regime views her reporting as a threat. She regularly receives phishing messages attempting to hack into her email and social media accounts. Noushin is also frequently subjected to online harassment and sexist insults. She has received threats from hostile accounts that describe raping her, putting her in a bag, and taking her to Iran. Yet, the most chilling attack came when someone found her son's social media profile and sent him explicit images, threatening to assault his mother in front of him.

Noushin believes these attacks – which are sometimes amplified by websites affiliated with the Islamic Republic's hardliners – are orchestrated by the Iranian regime and its supporters. Her parents, who live in Iran, have been threatened too. To Noushin, these digital threats are deeply troubling. "They aim to diminish your self-confidence and push you out of the space you occupy," Noushin told us. When under attack, she reduces her social media presence, struggles to focus, and feels vulnerable. She fears that she may be physically assaulted even in Europe.

Disturbing as it is, Noushin's experience – which has been captured by the term *digital transnational repression* – is unfortunately not unique. Digital transnational repression arises when governments use digital technologies to surveil, intimidate, and silence exiled and diaspora communities. It has emerged as a critical area of concern in the context of digital threats against human rights, shrinking civic space, and authoritarian interference in democratic societies. It is part of the broader practice of *transnational repression*, which refers to states using methods such as harassment, coercion-by-proxy, kidnapping, and extraterritorial killings, in order to control and silence dissent outside their territory.[2]

[1] The participant has been assigned a pseudonym to protect their identity.

[2] See Freedom House (undated), "Transnational Repression," <https://freedomhouse.org/report/transnational-repression>; Nate Schenkkan and Isabel Linzer (2021), "Out of Sight, Not Out of Reach," *Freedom House* <https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf>. On coercion-by-proxy, see Fiona Adamson and Gerasimos Tsourapas (2020), "At Home and Abroad: Coercion-by-Proxy as a Tool of Transnational Repression," *Freedom House* <https://freedomhouse.org/report/special-report/2020/home-and-abroad-coercion-proxy-tool-transnational-repression>.

The Citizen Lab's Research on Digital Transnational Repression

The Citizen Lab's research on digital transnational repression began in 2010 as a four-year study on targeted digital threats against civil society groups, which included Tibetan community organizations in exile.[3] At the time, no term was specifically used to describe the practice of authoritarian states systematically targeting human rights defenders both within and outside the state's territorial borders. In 2018, researchers from The Citizen Lab analyzed the device of Saudi activist Omar Abdulaziz, a Canadian permanent resident whose phone we discovered had been infected with Pegasus spyware while he was studying in Montreal. Abdulaziz, along with other Pegasus targets, described the extensive negative emotional and social repercussions of such digital attacks while in exile.[4]

In the wake of these discoveries, The Citizen Lab initiated a specific research stream to further investigate this practice of cross-border digital targeting, starting with a study on digital transnational repression against exiled and diaspora communities in Canada.[5] In conducting this research, we observed that women, in particular, faced a unique form of targeting that sought to shame and intimidate them through derogatory comments and other threats related to their gender, bodies, and sexuality. The Citizen Lab's interest in pursuing this particular issue – the impact of digital transnational repression on women human rights defenders in exile – inspired the present report.

Examining New Dimensions: Gender-Based Digital Transnational Repression

Building upon our prior research and the contributions of other scholars to this field, the aim of this novel study is to understand the security risks and harms caused by digital transnational repression against exiled and diaspora women human rights defenders. We use the term "women human rights defenders" broadly to describe women in exile or in the diaspora working on any human rights issue in relation to their country of origin. This includes human rights activists and individuals who may not self-identify as human rights defenders *per se*, such as journalists, researchers, or other members of the public.

[3] Masashi Crete-Nishihata, Jakub Dalek, Ronald Deibert, Seth Hardy, Katharine Kleemola, Sarah McKune, Irene Poetranto, John Scott-Railton, Adam Senft, Byron Sonne, and Greg Wiseman (2014), "Communities @ Risk: Targeted Digital Threats Against Civil Society," *The Citizen Lab* <https://targetedthreats.net/>.

[4] Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ronald Deibert (2018), "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," *The Citizen Lab* <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>; Access Now (2020), "From India to Rwanda, the Victims of NSO Group's WhatsApp Hacking Speak Out," <https://www.accessnow.org/nso-whatsapp-hacking-victims-stories/>.

[5] Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ronald Deibert (2022), "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* <https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/>.

The focus of our research is on human rights defenders who identify as women (cis/trans), non-binary, and gender-diverse individuals.

Drawing on the lived experiences of 85 women human rights defenders originating from 24 countries of origin (which we also refer to as home countries in the report) and residing in 23 host countries (which we also refer to as countries of residence or host states), we examine how gender and sexuality play a central role in digital transnational repression. We refer to this specific dimension of transnational repression as *gender-based digital transnational repression*. This study contributes to existing research on transnational repression and authoritarianism by investigating the specific ways in which state and state-affiliated actors deploy digital technologies and weaponize gender as a tool of repression against women human rights defenders residing outside their countries of origin. We shed light on new forms of technology-facilitated gender-based violence against political exiles and diaspora members and the impacts of this practice on targeted individuals and communities.

We find that exiled and diaspora women human rights defenders targeted through digital transnational repression face not only the same digital threats as men human rights defenders, but also gender-specific forms of online harassment, abuse, and intimidation. These threats lead to disproportionate harms that range from professional setbacks, stigmatization, and social isolation to the erosion of intimate relationships, profound emotional distress, and psychological trauma. Gender-based digital transnational repression also frequently involves the amplification and exploitation of entrenched patriarchal norms around women's bodies, sexuality, behaviour, and notions of family honor, potentially leading to further forms of violence and discrimination.

Scholarship on technology-facilitated gender-based violence commonly attributes online violence against women to misogynistic ideas and patriarchal norms in society which are reproduced and extended through digital technologies.[6] Our research highlights how state or state-affiliated actors build on such misogyny and patriarchism to instigate and perpetrate repressive acts with a distinct political purpose: to silence criticism and dissent beyond their borders.

The involvement of state or state-affiliated actors in these practices further exacerbates the power asymmetries between offenders and victims, increasing the risks for the safety, security, and fundamental rights of the targeted women. States have the resources and political will to engage in invasive surveillance or mount coordinated online defamation

[6] See, for example, Henry, Nicola and Anastasia Powell (2015), "Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence," *Violence Against Women* 21(6); Suzie Dunn (2020), "Technology-Facilitated Gender-Based Violence: An Overview," *Centre for International Governance Innovation* <https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/>.

and harassment campaigns that can leave severe impacts on the psychosocial wellbeing and professional career of targets. Further, they are also likely to act upon online threats against an exiled human rights defender, for instance by harassing, detaining, or even killing her family in her home country, inciting regime loyalists and chauvinist groups in the diaspora, or sending hired thugs to physically assault her. Finally, states are harder to hold to account due to the fact that, contrary to individuals or companies engaging in online violence against women, they may benefit from immunity from civil proceedings in domestic courts.

In addition, the intersecting identities of those targeted by gender-based digital transnational repression – namely, their gender, race, ethnicity, immigration status, and socio-economic class in the host country,[7] among others – lead to compounded vulnerability. Exiled and diaspora women human rights defenders often lack robust social networks and support structures in their host societies, leaving them further isolated and exposed to state repression. Their social ties to diaspora communities that may already have restrictive views on the public activity of women, as well as the increasingly hostile migration policies of host states, can further limit protection against the long arm of a repressive home state.

These unique dimensions of gender-based digital transnational repression call for responses that take into account both the intersectional risks to women targeted with online violence and the specific challenges of tackling transnational repression. By examining the interplay between digital technologies, authoritarianism, and gendered threats against exiled and diaspora women human rights defenders, our research sheds light on the dynamics and impacts of gender-based digital transnational repression and will inform the development of more effective strategies for prevention and mitigation.

Report Structure

This report is organized as follows:

- **Section 1: provides an introduction to transnational repression and gender-based digital transnational repression and highlights gaps in research to date**
- **Section 2: describes the research methods and challenges or limitations in undertaking this research project**
- **Section 3: discusses the methods and impacts of gender-based digital transnational repression through an analysis of 85 interviews conducted as part of this project**

[7] We refer to the country in which the research participant lives as their “country of residence,” their “host country,” or their “host state.” We refer to the country in which the research participant was born or where their parents were born as their “country of origin” or “home country.”

- **Section 4: reviews efforts by research participants to seek the support of their host states and developments in how host states have addressed transnational repression**
- **Section 5: describes how participants experienced gender-based digital transnational repression on social media platforms, the lack of assistance from these companies, and reviews selected platform policies and the lack of specific measures addressing digital transnational repression**
- **Section 6: provides a set of policy recommendations to specifically address gender-based digital transnational repression**

Key Findings

In this section, we set out high-level findings from the report that relate to the technologies used in digital transnational repression, perpetrators' potential profiles and motives, the gendered nature of the digital attacks and threats experienced by research participants, and the impacts:

- **Technologies and techniques used in digital targeting:** Activists are digitally targeted using a range of tools and techniques including social media surveillance, hacking of electronic devices or social media accounts, online harassment and disinformation, and the use of false or private information to discredit them.
- **Profile of perpetrators:** Perpetrators, as identified by respondents,[8] included government actors, state-backed trolls, inauthentic accounts, regime supporters, and other diaspora members with chauvinist and misogynistic ideas.
- **Gendered dimensions of online threats and attacks:** Participants were exposed to gendered online attacks and threats that included sexual slurs, harassment, vulgar comments on social media platforms, messages with detailed sexual fantasies, rape threats, and attacks related to targets' personal lives which reflected profoundly patriarchal ideas and attempted to deny women the ability to speak up on political and social issues.
- **Motives and triggers of gender-based digital transnational repression:** Threats typically targeted women human rights defenders who were in a position to mobilize international attention, causing authoritarian governments reputational damage and increased external scrutiny. Many research participants saw a direct connection between the threats they experienced and their work on their home country government's power abuse and human rights violations. Attacks were further directed

[8] The research methods applied in this report focused on collecting data through semi-structured interviews with respondents who self-identified as being attacked by their countries of origin. In most cases, we relied on respondents self-reporting of harm to understand the perceived nature and impact of digital threats they experienced versus conducting an empirical technical investigation of each attack described.

against women who challenged state censorship and patriarchal norms in their country of origin with their online presence and expression.

- **Impacts of gender-based digital transnational repression – mental health, wellbeing, and social relations:** The digital attacks experienced by respondents impacted their mental health and wellbeing. Respondents described feelings of exhaustion, stress and anxiety, burnout, sleeplessness, and depression. The attacks profoundly altered women's sense of security and their social relations. Relationships with family and partners deteriorated under the stress and uncertainty caused by such online harassment, attacks, and surveillance. The mistrust seeping into diaspora communities and online networks led research participants to isolate themselves and withdraw from others.
- **Impacts of gender-based digital transnational repression – activism and professional work:** Research participants exposed to smear campaigns were anxious about the negative impacts of such targeting on their work, in particular in undermining their reputation and credibility. Many started doubting the costs of activism and whether it was worthwhile to continue. Their deteriorating mental health affected productivity and work routines. Some were forced to withdraw, at least temporarily. Other respondents, however, seemed undeterred. These research participants saw the attacks against them as a sign their work was having an effect on the regime and its affiliates. But, even when they persisted in their activism, research participants had to constantly evaluate and navigate the associated risks. Fearing spying and surveillance, some renounced the attendance of larger gatherings with other exiles. Instead of speaking out in public, others engaged in research and writing, behind-the-scenes organizing, or met within smaller, trusted circles.
- **Managing security risks – securing practices and behavioural changes:** Research participants took a number of steps to mitigate the harms of digital attacks. They adapted their online behaviour and relied on different tools and practices of digital hygiene. However, the burden of such "preventive labour"[9] clearly lay on the shoulders of targeted research participants. They were constantly assessing the risks of their online environment and had to invest time and effort to seek out solutions to improve their digital security and other protective measures.
- **Coping with gender-based digital transnational repression:** To deal with the impact of attacks and mitigate psychological harm, research participants came up with different coping strategies. They tried to build mental resilience, took active care of their mental health and wellbeing, and sought support from family, friends, and peers. These responses carried emotional, social, and professional costs, requiring considerable effort and resources.

[9] Sarah Sobieraj (2020), "Constant Calibration (Preventative Labour)," in *Credible Threat: Attacks Against Women Online and the Future of Democracy*, (Oxford University Press).

- **Seeking support from host states:** Host state authorities continue to provide insufficient support to respondents. This protection gap is even larger for women targeted with gender-based threats from state actors in their countries of origin because law enforcement often lacks an understanding of the political motivation for such attacks and the necessary gender and racial sensitivity required to help victims of online abuse. As a result, many research participants doubted the benefits of reporting incidents to the police in their country of residence.
- **Social media platforms and gender-based digital transnational repression:** Research participants rely on large social media platforms for information sharing, advocacy, and activism. As a result, these platforms are also the primary sites of threats and attacks. Perpetrators exploited the technical affordances of platforms, manipulating crowd- and algorithm-driven news feeds for the viral distribution of harassment and defamation. The platforms' content moderation often failed to detect and prevent online abuse, particularly outside the context of English-speaking communities. Some research respondents reported having their accounts taken over or blocked by false mass reports. They often felt left alone as platforms were unresponsive. Overall, activists experienced uncertainty and anxiety over how to safeguard accounts and their content, adding to the psychological burden of digital threats.

Key Recommendations to Address Gender-Based Digital Transnational Repression

Building on existing recommendations to address digital transnational repression and suggestions made by research participants in this study, we focus our recommendations in this report on the gender-based dimensions of digital threats against exiled women human rights defenders.

Recommendations to host states:

- Fund civil society and relevant public sector institutions and agencies to facilitate group and individual counseling services for women human rights defenders in exile or in the diaspora
- Develop community support groups and opportunities for peer-to-peer learning for women human rights defenders in exile or in the diaspora
- Provide tailored digital security training which is specific to the gendered nature of the online threats experienced
- Ensure that relevant agencies (e.g., law enforcement) receive specific training on transnational repression and its digital and gender-based components

Recommendations to social media platforms:

- Enact community policies and guidelines that specifically address digital transnational repression and its gender-dimensions
- Work with civil society organizations that interact with women human rights defenders in exile or in the diaspora to mitigate gender-based digital transnational repression (e.g., receive complaints directly)
- Develop reporting channels that are specific to gender-based digital transnational repression
- Invest in special programs for high-risk targets such as women human rights defenders in exile or in the diaspora
- Research and publish on the surveillance-for-hire industry and how state actors abuse social media platforms and share such data with independent researchers

Recommendations to civil society organizations:

- Facilitate community support networks in order to address social isolation and facilitate peer-to-peer learning and group resilience among women human rights defenders in exile
- Deliver counselling services, provide digital security training, and coordinate legal aid support
- Provide information and offer support when women human rights defenders in exile or in the diaspora decide to report instances of transnational repression to law enforcement or other government bodies in the host state

Section 1: Situating Gender-Based Digital Transnational Repression

Authoritarian states employ transnational repression to extend domestic political controls and coercion in other countries. Digital technologies offer these governments a low-cost means to expand the scope and scale of transnational repression. Digital transnational repression is a specific form of transnational repression that employs digital technologies to surveil, intimidate, and silence individuals living in exile or in the diaspora. It builds on the following technical methods:

- **Surveillance:** Monitoring online communications to gather, analyze, and exploit information on the activities, daily habits, and social networks of human rights defenders, with the aim to expose country of origin contacts or prepare further attacks.
- **Interception:** Hacking of electronic devices, email, and social media accounts to access private information, communications, and contacts. These forms of targeted, invasive surveillance can rely on phishing attacks or the use of spyware.
- **Intimidation and stigmatization:** Using private, false, and distorted information, online harassment, and online threats to silence and discredit human rights defenders.
- **Disruption:** Curtailing expression on blogs, news websites, and social media profiles through distributed denial-of-service (DDoS) attacks, false reports, spam comments, and information manipulation.[10]

Digital threats often set the stage for an escalation into other attacks on exiles and their social networks including threats against family members in the country of origin, kidnappings, or physical assaults. As such, digital transnational repression is a core element of all forms of transnational repression. Digital tools enable authoritarian governments to easily instill fear and uncertainty among exiled human rights defenders, undermine the social relationships within exile and diaspora communities and their countries of origin, and foster self-censorship and withdrawal from activism.

Previous research on digital transnational repression has contributed to our understanding of the methods used and the impacts this practice has on targeted individuals and communities. However, to date there has been limited research on the specific factors, such as the gender or sexual orientation of targeted individuals, that contribute to these impacts. Scholarship on technology-facilitated gender-based violence shows

[10] This can include different forms of disinformation or defamation campaigns to harm the targeted person or negatively shape their public image and perception. See, for example, The U.S. Cybersecurity and Infrastructure Security Agency (undated), "Information Manipulation Infographic," <https://www.cisa.gov/sites/default/files/publications/information_manipulation_infographic_508.pdf>.

that women face unique and disproportionate harms online.[11] As digital technologies permeate everyday routines and communication, they perpetuate and amplify existing forms of discrimination and violence against women. Social scientist Sarah Sobieraj argues that digital hostility and sexism are an expression of men's resistance to women's participation in online publics. In order to sideline and silence women, aggressors typically rely on three overlapping strategies: intimidation, shaming, and discreditation.[12] Violent behaviour and activities that enable such strategies range from cyber-stalking, online harassment, sexist abuse, and slurs to the non-consensual release of private information and intimate images, and online rape and death threats.[13]

Gender-based online attacks and harassment are shown to have a significant negative effect on the psychological and emotional wellbeing of those affected causing fear, distress, withdrawal from social media platforms, and self-censorship.[14] They can also create physical safety concerns and lead to physical attacks. The negative impacts of technology-facilitated gender-based violence can be further exacerbated by the intersecting identities of the targets. LGBTQ+ individuals, women from racial and ethnic minorities, and individuals with lower socio-economic status or living with disabilities face greater risks of both being targeted and disproportionately affected by gender-based online violence.[15]

To date, the insights from the technology-facilitated gender-based violence literature have not been integrated into research on digital transnational repression. Authoritarian regimes typically promote traditional gender roles as a means to secure their hold on power.[16] Upholding patriarchal norms helps to reinforce established social hierarchies

[11] Technology-facilitated gender-based violence describes a range of activities and behaviors that rely on digital technologies for perpetuating violence and causing harm against women. See, for example, Cynthia Khoo (2021), "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence," *Women's Legal Education and Action Fund* <https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf>; Ronald Deibert, Lex Gill, Tamir Israel, Chelsey Legge, Irene Poetranto, and Amitpal Singh (2017), "Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Special Rapporteur on Violence Against Women, Its Causes and Consequences, Ms. Dubravka Šimonović," *The Citizen Lab* <https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf>.

[12] Sarah Sobieraj (2017), "Bitch, Slut, Skank, Cunt: Patterned Resistance to Women's Visibility in Digital Publics," *Information, Communication & Society* 21(11).

[13] Jill Filipovic (2007), "Blogging While Female: How Internet Misogyny Parallels Real-World Harassment," *Yale Journal of Law and Feminism* 19(1).

[14] Suzie Dunn (2020), "Technology-Facilitated Gender-Based Violence: An Overview," *Centre for International Governance Innovation* <https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/>.

[15] Laura Hinson, Jennifer Mueller, Lila O'Brien-Milne, and Naome Wandera (2018), "Technology-Facilitated Gender-Based Violence: What Is It, and How Do We Measure It?," *International Center for Research on Women* <https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/>.

[16] Chenoweth, Erica and Zoe Marks (2022), "Revenge of the Patriarchs: Why Autocrats Fear Women," *Foreign Affairs* 101(2).

and power relations.[17] Many of today's authoritarian and populist leaders rely on hypermasculinity and misogynistic speech to shore up support and silence their critics.[18] Feminist ideas and activism for gender equality and human rights are stigmatized as external corrupting influences. Outspoken women who challenge patriarchal privilege are perceived as threats and targeted with insults, abuse, and physical intimidation.[19] Such forms of violence against women also naturally extend into the online sphere, both domestically and transnationally. Illiberal and authoritarian power holders have deployed gendered disinformation to discredit and tarnish the reputation of women politicians and journalists.[20] Digital threats are also used to intimidate and punish politically active women and other vulnerable groups.[21]

The strategic use of online violence against women by repressive rulers seeking to subdue dissent clearly needs more attention, particularly in its transnational form. Research on digital transnational repression has not yet examined how authoritarian regimes instrumentalize gender and sexuality to extend and amplify digital threats against human rights defenders in exile or in the diaspora. Our report begins to fill this gap by investigating what we refer to as "gender-based digital transnational repression" (i.e., the use of digital technologies for gendered attacks that aim to silence criticism, dissent, and human rights advocacy among exiles or in the diaspora). This research sheds light on the specific vulnerabilities of women fighting for political and societal change from afar and the harms caused by gender-based digital transnational repression.

[17] Amnesty International (2021), "Azerbaijan: Gender-Based Reprisals Against Women Must Stop," <https://www.amnesty.org/en/wp-content/uploads/2021/05/EUR5541032021ENGLISH.pdf>; Naseer, Shirin and Cameran Ashraf (2021), "Gender-Based Violence in Pakistan's Digital Spaces," *Feminist Legal Studies* 30; Marc Owen Jones (2021), "State-Aligned Misogynistic Disinformation on Arabic Twitter: The Attempted Silencing of an Al Jazeera Journalist," *Open Information Science* 5(1).

[18] Nitasha Kaul (2021), "The Misogyny of Authoritarians in Contemporary Democracies," *International Studies Review* 23(4).

[19] Stewart, Abigail J, Shelly Grabe, and Wang Zheng (2024), "Women's Movement Activism in Authoritarian States: Lessons from the Global Feminisms Project," *Signs: Journal of Women in Culture and Society* 49(2).

[20] Lucinda Di Meco and Kristina Wilfore (2021), "Gendered Disinformation is a National Security Problem," *Brookings* (March 8) <https://www.brookings.edu/techstream/gendered-disinformation-is-a-national-security-problem/>.

[21] Amnesty International (2024), "'Being Ourselves is too Dangerous' Digital Violence and the Silencing of Women and LGBTI Activists in Thailand," <https://www.amnesty.org/en/latest/news/2024/05/thailand-state-backed-digital-violence-silence-women-lgbti-activists/>; Rina Chandran and Maya Gebeily (2021), "Analysis: From Middle East to India, Women 'Violated' in Pegasus Hack," *Reuters* (August 10) <https://www.reuters.com/article/business/healthcare-pharmaceuticals/from-middle-east-to-india-women-violated-in-pegasus-hack-idUSL8N2P91KX/>.

Section 2: Data and Methods

2.1 Data Collection and Analysis

The findings in this report are primarily based on a series of semi-structured interviews with 85 research participants from 24 countries of origin and living in 23 different host countries.[22] The most prominent countries of origin of our respondents include Iran (13 participants), China (13 participants, including 10 Uyghur participants from the Xinjiang region), Russia, and Azerbaijan (both 10 respondents). This selection covers important state perpetrators of transnational repression and a variety of authoritarian governments.[23]

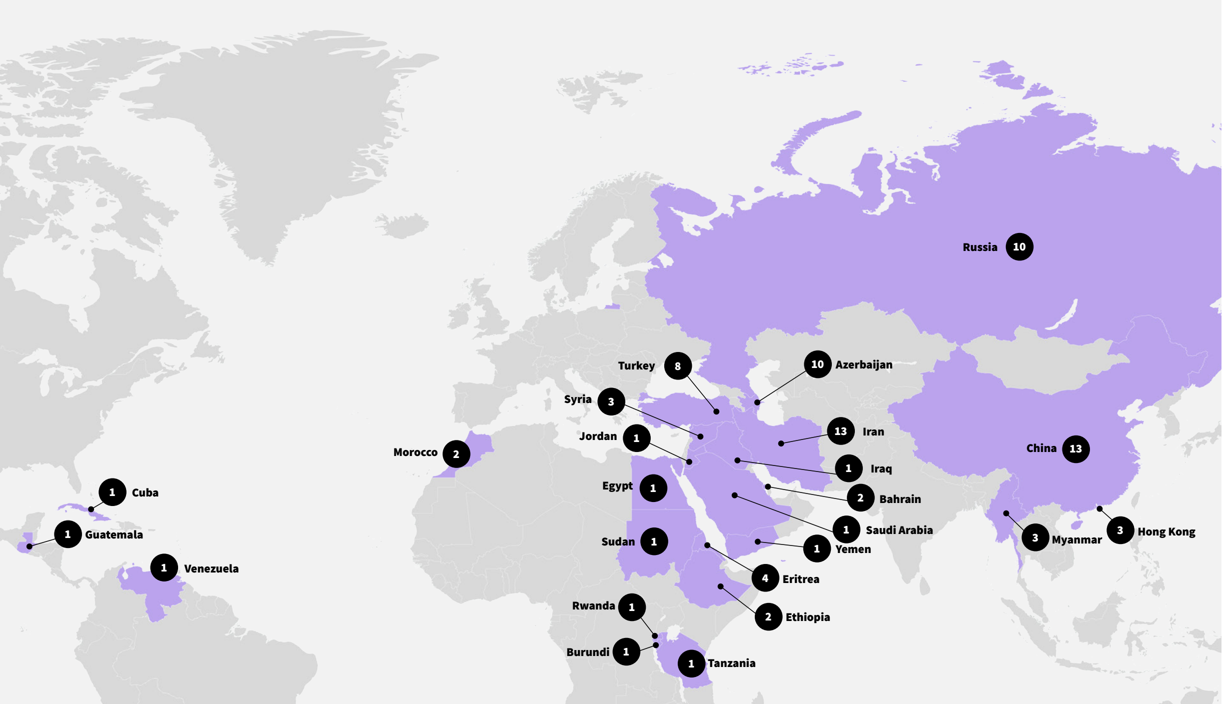

Figure 1: Countries of origin of the participants of this research study.

[22] As noted, we refer to the country in which the research participant lives as their "country of residence" or their "host state" or "host country." We refer to the country in which the research participant was born or where their parents were born as their "country of origin" or their "home country." The country of origin as identified by a participant does not necessarily correspond to a nation state. While we categorized participants according to internationally recognised countries for this overview, throughout the report we rely on their self-description. For example, a respondent from the Xinjiang region in China may identify herself as Uyghur (and not Chinese), while an interviewee of Kurdish origin may indicate Kurdistan as their home country (and not Iraq or Turkey). In addition, migrants with hybrid identities may consider themselves as having origins in one country although they were born and raised in another (e.g., second-generation immigrants from Turkey living in Germany).

[23] Following Marlies Glasius' conceptualization of authoritarianism, we define authoritarianism not exclusively as a regime type tied to a specific territory, but as a set of practices of accountability sabotage with two core components, namely "disabling voice" and "disabling access to information." See Marlies Glasius (2023), *Authoritarian Practices in a Global Age*. (Oxford University Press) at 190.

The most prominent host countries are the U.S. (16 respondents), Germany (15), the U.K. (11), and Canada (8). While the majority of host states covered in this report are democratic, we also interviewed some respondents residing in authoritarian host states (e.g., Thailand and the United Arab Emirates). This has allowed us to learn more about the lack of protection and support from host state authorities in authoritarian regimes.

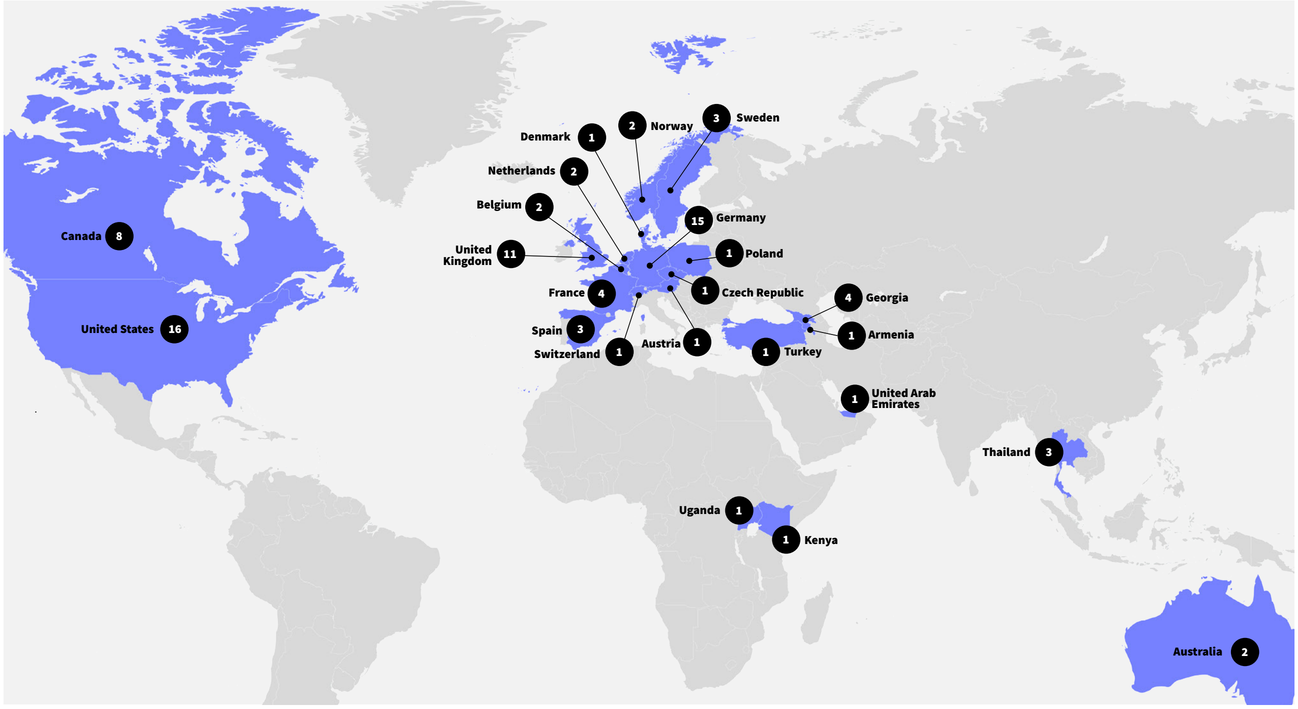

Figure 2: Countries of residence of the participants of this study.

In terms of their occupational background, respondents fell into two broad categories: human rights defenders and journalists. As noted earlier, we consider human rights defenders as any person promoting human rights in a paid or voluntary role, ranging from staff of large nongovernmental organizations to individual activists.[24] This includes human rights activists and individuals who may not self-identify as human rights defenders *per se*, such as journalists, lawyers, or members of the public. We have separately labelled research participants who are journalists for the purpose of this research project because of the significant impact of digital transnational repression on freedom of expression and the operation of the media. Journalists, including citizen journalists, cover news and comment on public affairs in print, online, and on radio and television.[25] Whenever interviewees were active in different fields, we list the activity that occupied most of their time or was the main reason for the attacks against them. Accordingly, 52 research participants were identified as human rights defenders and 30 interviewees as journalists (three study participants fell into neither category).

[24] United Nations Human Rights Office of the High Commissioner (2024), "About Human Rights Defenders Special Rapporteur on Human Rights Defenders," *United Nations* <https://www.ohchr.org/en/special-procedures/sr-human-rights-defenders/about-human-rights-defenders>.

[25] Committee to Protect Journalists (2024), "How Does CPJ Investigate and Classify Attacks on the Press?," <https://cpj.org/about/faq/>.

Research participants were recruited on the basis of the following criteria:

- Over the age of 21
- Identify as a woman (which includes cis and trans women and individuals who identify as non-binary or gender-diverse)
- Engaged in political, social or advocacy work in relation to their country of origin
- Targeted or believe they were targeted through digital technologies by what they suspect was a state or state-affiliated actor in relation to their work or activism
- Left their country of origin and are residing in exile or in the diaspora in a different country (in some cases this also included second-generation migrants)[26]

We established a fellowship program for exiled and diaspora women human rights defenders with ties to different authoritarian contexts to conduct interviews in various languages and deepen our understanding of gender-based digital transnational repression. This program included researchers of Iranian, Uyghur, Ethiopian, Russian, Azerbaijani, and Turkish origin. These fellows, alongside bilingual researchers at the Citizen Lab, conducted interviews in either English or in the research participant's first language if it was Arabic, Spanish, German, Russian, Turkish, Azerbaijani, Uyghur, Amhari, or Persian. Collaborating with women researchers from exile and diaspora communities – some with firsthand experience of gender-based digital transnational repression – helped us improve and enrich our research with the trust and contacts these fellows had established within their own networks. We were thus able to speak with research participants with a broader range of experiences. Furthermore, the diverse lived experiences of researchers working on this project offered a wider lens through which to interpret our findings and understand the political, social, and cultural contexts of different exiled and diaspora communities.

We conducted the interviews for this study between August 2022 and March 2024. Participants were recruited based on existing contacts of The Citizen Lab, referral from previous research respondents, and publicly reported cases of digital transnational repression. The semi-structured interviews included questions on the technologies respondents used in their activism, the type of threats they had experienced, their perception of possible triggers, perpetrators and gender dimensions, the impacts of

[26] The concepts of 'exile' and 'diaspora' certainly overlap. While exile commonly describes the individual experience of being forced to live in a country other than one's own country of origin, the term diaspora tends to emphasize the collective identity of people "with a common origin who reside, more or less on a permanent basis, outside the borders of their ethnic or religious homeland." Exiles typically consider their existence abroad as potentially less long-term and engage in political activities against the home regime in order to return. Although more rooted in their existence abroad, diasporas also organize and mobilize to participate in social and political affairs of their homeland and states have invested growing resources into different strategies that seek to recruit the diaspora (in addition to repressing them). Shain, Yossi and Aharon Barth (2003), "Diasporas and International Relations Theory," International Organization 57(3) at 453; See also Alan Gamlen (2019), *Human Geopolitics: States, Emigrants, and the Rise of Diaspora Institutions*. (Oxford University Press).

threats, participants' coping strategies, experiences in seeking remedies, and what justice and security meant to them in their contexts.

After completing the interviews, we conducted a thematic analysis of the transcripts alongside a list of codes derived from the project's key research questions (e.g., types of digital threats, impacts, and responses). Additional themes and patterns were added as we identified them in the interview material. This approach enabled us to develop a detailed and contextually grounded analytical description of the dynamics of gender-based digital transnational repression and its multifaceted impacts. Throughout the analysis we tried to account for how the intersectional identities of our research participants – including gender, sexuality, race, ethnicity, refugee or immigrant status, socio-economic class, age, disability, and activism status – shaped their experience and coping mechanisms in response to the harms of gender-based digital transnational repression. In addition to the interview material, our analysis incorporated findings from desk research and literature review, drawing on academic articles, policy papers, media reports and publications from non-governmental organizations, and other secondary sources.

Draft versions of this report underwent peer-review by members of The Citizen Lab and three external reviewers who are experts in technology-facilitated and gender-based violence, human rights defenders in high-risk contexts, and the digital security of marginalized communities.

2.2 Research with Participants in High-Risk Situations

The safety, security, and wellbeing of study participants were a core concern throughout the entire project cycle. The research followed an ethics protocol approved and supervised by the University of Toronto's Research Ethics Board.[27] We conducted the study with careful attention to participants' various vulnerabilities, resulting from factors such as their gender, race, refugee or immigration status, and history of trauma. Interviewees provided informed consent, either in writing or verbally, to participate in the research study after being told about the goals and content of the study and the potential risks raised by participation. Verbal consent was used in cases where signing a document risked creating additional security concerns for interviewees or discouraging them from fully participating in the interview.[28] Interviews were conducted over end-to-end encrypted

[27] This research was conducted under research ethics protocol #42719. For more information on Ethics in Human Research at the University of Toronto, see Division of the Vice President, Research & Innovation (undated), "Ethics in Human Research," *University of Toronto* <https://research.utoronto.ca/ethics-human-research/ethics-human-research>.

[28] This is a recommended practice in research with migrants and other sensitive populations. See European Commission (2021), "Guidance Note – Research on Refugees, Asylum Seekers and Migrants," <https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-research-on-refugees-asylum-seekers-migrants_he_en.pdf>; Marlies Glasius, Meta de Lange, Jos Bartman, Emanuela Dalmasso, Aofei Lv, Adele Del Sordi, Marcus Michaelsen, and Kris Ruijgrok (2018), *Research, Ethics and Risk in the Authoritarian Field*. (Palgrave Macmillan) at 100.

communication channels. Audio recordings and interview transcripts were stored on secured servers. Identifying personal information was removed from transcripts and interviewees were cited anonymously or pseudonymously throughout the report.

Given the emotional and psychological impacts of gender-based digital transnational repression, and recognizing that participants may have endured various forms of repression in their country of origin – including imprisonment and gender-based violence – our research team received training in trauma-informed interview approaches. We were conscious of the risks for each of our respondents participating in the interview – both in terms of a possible re-traumatization when talking in detail about the difficult experience of online abuse or harassment as well as a potential exposure to further threats or marginalization against them and their social networks.

Conducting interviews primarily online allowed us to reach a broader range of participants. We prioritized a safe environment for the interview by observing and adapting to the specific needs of each respondent and trying to limit intrusion into their personal and professional lives. We offered an introductory meeting to inform them about the research project and allow for trust-building prior to the interview. The fact that many of our interviewers shared the experience of living in exile or in the diaspora with their interlocutors – and some interviewers had also been the targets of digital threats themselves – helped respondents feel more comfortable and encouraged them to share their experiences more deeply during our conversations. Many participants were interviewed in their mother language, allowing them to express themselves more fully and naturally.

To promote agency and control over their narrative, research participants could request access to the transcript, withdraw from the study, or modify any of their statements. If we doubted our interpretation of participants' views, we sought clarification from the interviewer or research participant directly to avoid misrepresentation or harmful assumptions. In line with standards of qualitative research, participants did not receive any remuneration for their participation in the interview. However, as part of our commitment to digital rights and community empowerment, we provided interested respondents with resources on digital security and the wellbeing of human rights defenders. Many respondents expressed to us that they valued the opportunity to share their experiences and insights in the hope to contribute to improved measures of support and protection for targets of gender-based digital transnational repression.

2.3 Research Limitations

Selecting respondents from our existing networks and further referrals has several limitations. First, such an approach runs the risk of failing to incorporate contradictory or minority opinions as researchers tend to stay enmeshed in their own networks and thus predominantly interview people who share similar experiences, views, or backgrounds. Second, by primarily seeking out respondents who were active as human rights defenders or journalists, we may have included fewer individuals who were actually silenced by digital transnational repression and quit activism as a result of regime pressure or other responsibilities and pressures. Third, our understanding of digital transnational repression and its impacts may have been influenced by the tendency of some participants to downplay how they experienced digital threats, possibly in order to project resilience or strength in the face of adversity. Others may have emphasized the risks they faced in order to potentially stress the relevance of their activities.

We tried to mitigate any distorting effects of these limitations on our analysis and interpretation by maximizing our exposure to different experiences and understandings of gender-based digital transnational repression.[29] As a result, our pool of respondents come from a range of countries of origin. It includes human rights defenders working both as individuals as well as those in larger well-resourced organizations and incorporates the experiences of high-profile activists and those engaged in less public activities. Further, it includes the experiences of individuals coming from different sexual and ethnic backgrounds. Throughout the interview process, we critically re-evaluated and adapted the selection of respondents. In the resulting relatively large collection of in-depth interview material, we were able to identify recurring patterns across different countries and exile/diaspora communities. Finally, together with the research fellows who acted as interviewers, we held a two-day workshop in which we collaboratively discussed and compared our findings and interpretations.

Finally, our research approach prioritizes the insights of digitally targeted individuals over the technical investigation of such threats or attacks. In this report, we do not attribute the described threats or attacks to specific perpetrators or verify particular incidents mentioned by respondents. We build on the descriptions provided by respondents who, for different reasons, believe the threats or attacks they experienced came from state or state-affiliated actors in their country of origin. Whenever possible or relevant we refer to other sources for the behaviour, motivations, and methods of states engaging in digital transnational repression for further substantiation. However, any detailed technical analysis was beyond the scope of this report, which aims to provide a global view on the issue of gender-based digital transnational repression and its impacts. By centering the human experience of online attacks and digital (in-)security, this report aims to bring forward a perspective that often gets lost in more technical research.

[29] Peregrine Schwartz-Shea and Dvora Yanow (2012), *Interpretive Research Design: Concepts and Processes*. (Routledge) at 84-89.

Section 3: The Experiences of Women Targeted with Gender-Based Digital Transnational Repression

In this section, we provide a summary of the prevalent tactics of digital transnational repression described by the exile and diaspora women human rights defenders we interviewed. Next, we turn to the gendered dimensions of digital threats and detail the online harassment, abuse, and insults that the women in this study experienced. We use the observations of these research participants to discuss the identity of some of the potential aggressors as well as likely motives and triggers for the attacks. We also examine the impacts of digital attacks, showing how constant harassment, abuse, and threats affected the mental health, social relations, activism, and professional development of targeted women.

Despite these experiences, many respondents displayed persistence in their activism. They adopted digital security practices and changed their online behaviour, developed mental resilience and coping strategies, and built networks and communities of mutual support and allyship. All of these responses came with emotional, social, and professional costs, requiring considerable effort and resources on the part of the targeted individuals.

While these responses reveal the creativity and resistance of the women we interviewed, they also illustrate the power dynamics and structural inequalities that drive gender-based digital attacks from, as identified by respondents, authoritarian state and state-affiliated actors. Tackling this imbalance would require a dedicated intervention and support from host states and social media platforms, both key players in the protection of human rights defenders in exile or in the diaspora against digital transnational repression.

3.1 The Repertoire of Digital Threats Across Borders

Starting from monitoring, surveillance, and attempts to break into email and social media accounts up to online harassment and defamation campaigns, research participants were confronted with a paradigmatic selection of digital transnational repression methods. These digital attacks occasionally escalated into physical threats, such as when state agents harassed activists' family members in the country of origin or regime affiliates stalked and even assaulted women human rights defenders in their host country.

Among our respondents, we observed a widespread assumption of ongoing **monitoring and surveillance** by state authorities from the country of origin. They perceived that online abuse and other attacks were closely linked to their activities on social media, often in immediate reaction to posts on a social media platform. An Iranian women's rights defender in the U.K. felt the Iranian government was closely observing people in the diaspora to "assess personalities, exploit dependencies and emotional ties to plan threats and harassment." But monitoring not only prepared the ground for further attacks, it also served as an instrument of control in and of itself in the form of performative surveillance. An Iranian and an Azerbaijani journalist, both working from the U.S., reported that they overheard breathing and other noises during calls with contacts in their countries of origin. To the Azerbaijani journalist, this was not just a technical glitch, but a deliberate gesture to signal that surveillance was ongoing, in particular when she was talking to contacts about sensitive issues such as politically motivated arrests and police torture. The Iranian journalist believed that the Iranian authorities tried to showcase and exaggerate their surveillance capabilities to create an image of 'big brother' and intimidate diaspora members.

Attempts at more **invasive surveillance** included the self-reported digital infiltration of online meetings and communities, phishing messages, and the use of spyware. A feminist activist from Russia explained how her group scrupulously avoided linking any personal information to email accounts and social media profiles they used for their activism. Yet, when they started to coordinate anti-war activities with other exiled organizations that did not follow similarly strict protocols, she explained that some of her personal details were leaked from a chat and as a consequence she was threatened by Russian security agents. Two other Russian activists coordinating efforts to help their fellow citizens escape army recruitment and leave the country were frequently contacted by people who pretended to seek support, but apparently tried to gather information on their location and contacts. A Myanmar activist based in Thailand described how the Myanmar military used the devices and accounts of activists arrested inside the country to contact others outside and infiltrate the opposition's Zoom meetings.

Phishing emails were reported by the majority of women we interviewed. They described how these attacks often used information on the target that perpetrators had previously gathered through profiling. In particular, the Iranian respondents reported elaborate scenarios of social engineering to get them to open compromised links or attachments. An Iranian activist based in Germany explained that she and other fellow panelists from a conference were contacted for an interview by a journalist claiming to work for a well-known American think tank. "When I looked at her Twitter [X] posts, I was certain this person opposed the Islamic Republic. She particularly covered the Baha'i community, claiming to be a Baha'i herself. This gained trust, especially since many of us do not know prominent figures in the Baha'i community well." Shortly before the scheduled interview, the person sent her a link for an online meeting that contained malware. After she clicked on it, she temporarily lost access to her email account and could only log in again after resetting the password. She then decided to no longer use the account.

A report by an Iranian digital security organization later attributed this attack to threat actors close to the Islamic Revolutionary Guard Corps.[30]

Three research participants reported how they were impacted when **spyware** was used against them. An activist from Rwanda whose phone was infected with Pegasus spyware described how she felt more vulnerable, including to physical threats, after being targeted with this technology. She explained: “I think that was the scariest for everyone in my family, when they realized which spyware tools [the government of Rwanda had access to] and what kind of transnational repression the government can perpetrate and…the ability for them to locate me.” The case of Loujain Al-Hathloul, a prominent women's rights defender from Saudi Arabia, exemplifies how the targeting of women activists with spyware can lead to increased risks of physical acts of transnational repression. According to litigation materials filed in the U.S., Al-Hathloul’s device was infiltrated by the Abu Dhabi-based cybersecurity company Dark Matter while she was living in the United Arab Emirates.[31] This surveillance helped local authorities determine her geographical location and led to her arrest. Al-Hathloul was later extradited to Saudi Arabia, where she was imprisoned and tortured.[32]

The fear of being targeted with spyware also stayed with those respondents who experienced invasive surveillance before moving into exile or came from countries with governments known for their use of surveillance tools. A Venezuelan activist acknowledged that leaving Venezuela had reduced her risks but noted that the use of spyware against her remained a latent fear. "It’s a constant concern; if you’re working against this kind of technology, it can be used against you.” Similarly, a participant from Bahrain, who was targeted with spyware in her home country, shared how, even in exile, the fear of being monitored has not left her: “I constantly feel watched, monitored everywhere, and at all times throughout my day.” She added, "Who knows? If they are not using Pegasus, they may be using other spyware.” Describing the emotional toll of surveillance, she said: “I felt completely exposed, I felt naked. It was as if they stripped me of my privacy when they hacked my device.”

[30] See Factnameh (2023), “Tactics, Techniques and Procedures of Malicious Hacking Groups Affiliated with the Government of the Islamic Republic of Iran [in Persian],” (June 17) <https://factnameh.com/fa/fact-checks/2023-06-08-iran-cyber-threat-actors-ttps>.

[31] Chrisopher Bing and Joel Schectam (2019), “Inside the UAE’s Secret Hacking Team of American Mercenaries: Ex-NSA Operatives Reveal How They Helped Spy on Targets for the Arab Monarchy – Dissidents, Rival Leaders and Journalists,” *Reuters* (January 30) <https://www.reuters.com/investigates/special-report/usa-spying-raven/>; Loujain AlHathloul v. Darkmatter Group, Marc Baier, Ryan Adams, and Daniel Gericke (2021), *3:21-cv-01787-IM* <https://www.courthousenews.com/wp-content/uploads/2023/03/alhathloul-v-darkmatter-complaint.pdf>.

[32] Loujain AlHathloul (undated), “Timeline of Arrest, Torture, and Charges,” <https://www.loujainalhathloul.org/arrest-torture-charges>.

Other than hacking and spying attempts, the abuse of social media platforms' reporting and content moderation mechanisms for **blocking or limiting the reach of social media profiles** was widely mentioned. Respondents described how attackers would typically coordinate the mass reporting of a profile for alleged violations of the community guidelines. Once the profile was flagged or even blocked for allegedly spreading hate speech or pornography, it took the targeted individuals time and effort to deal with the platform's automated user services and get the profile reinstated to normal functioning (see Section 5, below). Other platform features were also manipulated for the silencing of human rights defenders. Two Iranian respondents were among the targets of a broader attack in which the number of followers on their Instagram pages was suddenly increased by tens of thousands of fake profiles. The discrepancy between the high number of followers and comparatively low engagement from the audience led to the profile's downgrading in news feeds so that its content was no longer visible to its actual followers.[33]

Activists described **defamation campaigns** launched against them to undermine their credibility and isolate them within their own communities. The campaigns that respondents experienced followed three patterns: 1) distorting the position of activists; 2) portraying them as foreign agents; and 3) exacerbating divisions in the diaspora. Participants described how their interviews, articles, or statements were taken out of context to misrepresent their views and smear their reputations. Using old photos and interview snippets, several Azerbaijani respondents stated they were framed as traitors, both online and in state-affiliated media, for their previous contacts with Armenian colleagues after hostilities between the countries escalated in 2020. A Russian anti-war activist described being accused of selling information about the location of Russian soldiers to the Ukrainian Army that caused higher casualties. A high-profile human rights campaigner and direct witness of the detention camps in the Xinjiang region mentioned an attack by anonymous accounts that she believed were likely tied to the Chinese government. The attackers tried to use her Uzbek roots against her by questioning her legitimacy to speak out on behalf of Uyghurs and spreading rumours that she was a Chinese spy.

In addition to these digital attacks, many respondents described facing threats of physical harm to themselves or their relatives, especially their children. In particular, threats against family members still living in their country of origin were reported as a widespread tactic for escalating digital threats: research participants' close relatives were threatened, summoned to the police, or lost their jobs in retaliation for their activism abroad. Such proxy punishment (coercion-by-proxy) was particularly frightening for Uyghur activists who risked seeing their loved-ones disappear into China's dystopian system of internment camps. Some reported they had received calls from government agents who

[33] Qurium The Media Foundation (2022), "Weaponizing Instagram Against the Iranian #MeToo Movement," (June 16) <https://www.qurium.org/alerts/iran/weaponizing-instagram-against-the-iranian-metoo/>.

pressured them in the presence of family members to stop speaking out about human rights or to spy on other activists in the diaspora.

In other cases, respondents described how perpetrators combined digital methods with physical threats to increase pressure. Two Uyghur human rights advocates highlighted how online surveillance was linked to broader intimidation and harassment. When they travelled for advocacy events or prepared for interventions at the United Nations headquarters in Geneva, they described being followed, photographed, and filmed by individuals they believed were affiliated with the Chinese government. A human rights defender from Ethiopia was similarly filmed and threatened in Geneva before giving a statement at the United Nations. Two Eritrean activists described how online smear campaigns ended in harassment and physical assaults by regime loyalists in public places and at events in their countries of residence, the U.K., and Sweden. The husband of an Azerbaijani activist living in the Czech Republic was attacked by three assailants armed with a knife; another Azerbaijani journalist in the U.S. had her car tires slashed by unknown perpetrators. While respondents were unable to establish a direct link between these physical threats and their home state, the timing of the attacks and/or their correlation with ongoing online hate campaigns against the respondents, which repeated regime narratives, led them to believe the threats were directly or indirectly instigated by government actors from their country of origin.

Arwa: An Activist From Yemen[34]

Arwa – who spent over a decade in public activism work in Yemen – played a crucial role in the 2011 Yemeni uprising. She attended protests, spoke at conferences, and participated in women's marches, often using digital platforms to reach a broader audience. Digital technology was central to her activism, enabling her to communicate with fellow activists through encrypted apps like WhatsApp and to share her views publicly on platforms such as Facebook, Twitter, and Instagram. Yet, as a woman activist, her public visibility drew relentless attacks and criticism. "I really didn't like being a public figure," she reflects. "It's not for me." The pressure grew exhausting, and, in 2015, she sought refuge in the E.U., hoping for a safer environment to continue her work in a more discreet way.

[34] The participant has been assigned a pseudonym to protect their identity.

Despite facing political repression and gender-based threats both online and offline, Arwa refused to abandon her activism. Instead, she adapted her approach, shifting her focus toward broader human rights and democracy through artistic advocacy. “What I want is for people to really understand and connect on an emotional, personal level,” she explains, describing how art allows her to challenge authoritarian and patriarchal systems without risking the severe reprisals that come with public activism. Yet, even her creative efforts bring risk. Publishing her artwork under a pseudonym to protect her identity, she faces ongoing threats that leave her in fear for her safety — even in the E.U.

Arwa’s belief that her attackers are connected to her country of origin’s government is grounded in painful experiences. She has faced repeated digital threats including the hacking of her computer and the leak of her wedding photos, intended to shame her as a “hypocrite” for not adhering to traditional expectations. “I still get emails, messages, DMs,” she says, revealing the ongoing psychological burden of these intrusions. The leaked photos, where she was not wearing a headscarf, provoked accusations and violent comments, some of which threatened rape. “It’s a real fear,” she shares, understanding the personal and familial consequences should these threats ever get carried out. Her extended family, distressed by the public shaming, has urged her to withdraw from activism to “protect the family’s honour.”

The persistence of misinformation, perpetuated even by credible sources like Arabic Wikipedia, has compounded the emotional toll. This circulation of false narratives serves not only to undermine Arwa’s reputation but to isolate her from her community. In response to these attacks, she has developed a heightened sense of caution, exercising self-censorship and second-guessing her choices. "I’m more careful about who I socialize with," she explains, fearing that someone might be working for the regime and seeking to infiltrate her social circles. Over time, the vigilance and isolation have diminished her confidence. "It’s just sucking my energy," she admits, describing the toll of maintaining her safety.

Even within Europe, Arwa’s concerns persist. She is wary of harassment from Yemeni agents and continues to face a flood of messages from online trolls. Her frustration is compounded by the lack of support from institutions while in exile; organizations she has collaborated with – including those advocating women’s rights – have offered little in terms of digital security or protective measures. Despite their awareness of her situation, Arwa feels these institutions have “zero concern for us and our safety.”

Looking forward, Arwa envisions a platform where women facing similar forms of digital harassment can confront their perpetrators in a protected space. "They need to understand all the harm they’ve done," she says, “not just [on] one person, but an entire society.” Resilient and determined, Arwa continues to navigate the delicate balance between her advocacy and the high personal costs it exacts.

3.2 The Gendered Dimensions of Digital Threats and Attacks

In addition to the threats outlined above, many respondents were exposed to sexual slurs, harassment, and vulgar comments on social media platforms. They received messages with detailed sexual fantasies and rape threats. Several women had unsolicited pictures of male genitalia sent to their accounts. Others mentioned that photoshopped fake nude pictures of themselves were circulated online.

An Iranian human rights activist recounted: “I receive so many messages that only talk about sexually assaulting me, saying that I'm only good for that. I try to protect myself, but it's not easy. You can't filter everything.” A Uyghur human rights defender recalled being targeted with sexual insults in Chinese that she could not even understand despite her fluency in the language because she had never heard such words before. “I felt embarrassed and ashamed that it was publicly shown to many other people. I think that this is a strategy. Smearing someone's body, like sexually assaulting someone, is the one way to hurt women the most. I think they know this exactly.”

This activist stressed that male human rights defenders were not exposed to comparable attacks. For men, “they would say stuff to their mother. They would be like I'm going to do something to your mother, to your sister, or to your daughter. But they wouldn’t say I'm going to do something to you, to the male person. So it’s still targeted at the female person in that human rights advocate’s family.” Many other participants made similar comparisons, highlighting that their male colleagues or fellow activists were never attacked on the basis of their gender identity whereas women almost automatically became a target for abusive and sexualised comments related to their appearance and behaviour.

An Iranian journalist based in France observed that “anything related to your body and your sexuality becomes the target of attack.” She had experienced extensive abuse degrading her as a sexual object and shaming her for her body from both regime-affiliates and opposition members. A Kurdish activist from Germany observed that online abuse often targeted women’s bodies as if to reassert patterns of dominance in the digital sphere: “They want to bring you back into that physical, even kind of animalic space, where it’s just like, ‘You think you’re in a civilized world where thoughts and discussions can change things. Let me bring you back to the jungle of reality where I could do whatever I wanted.’” Another Kurdish respondent reported that she had received violent rape threats and threats to put her in a “yellow body bag” of the type used by the Turkish military when Kurdish militia fighters are killed.

Abuse and defamation targeting the personal lives of activists often reflected profoundly patriarchal ideas, denying women the ability to speak up on political and social issues. Several respondents mentioned attacks against them focused on their alleged rejection of traditional gender roles such as not having children, or not taking care of their children or husbands. A human rights defender from Tanzania said that in addition to labelling her a “whore” and “sex-deprived,” there was a whole discussion “about whether I should be in the kitchen or having sex with my husband.” Assailants sought to undermine the credibility of research participants with false statements about women’s sexual relationships and promiscuity. A U.S.-based Azerbaijani journalist remembered a smear campaign in which a journalist supportive of the government accused her of cheating on her husband, even though she did not have a partner at the time. Similarly, an Iranian journalist working with a media outlet in the U.S. pointed out that online mobsters regularly accused her of having reached that position only because of an alleged affair with the chief-editor.

Gendered abuse and threats of sexual violence were also aimed at the parents or children of exiled activists. Some respondents noted that certain campaigns against them reinforced patriarchal norms and weaponized the notion of men's guardianship. For instance, they pointed out how their husbands were bullied for failing to "control" their wives. Male family members were also shamed for not being able to silence their rebellious female relatives. In other cases, male partners were confronted with some of the sexualized threats that were also being directed at women. Respondents married to foreigners said that defamation campaigns sought to discredit them as foreign agents or questioned their credibility to speak on behalf of their community.

Several participants noted that in some communities, women who behaved and dressed in non-conformist ways could face harsh attacks on their morality with male commenters policing their actions and telling them "how to behave." These types of derogatory remarks did not only come from likely regime affiliates, but also from within the women's own diaspora communities. A Uyghur journalist working for a media organization in the U.S. explained how an anonymous Facebook account posted private photos from her personal Instagram account with degrading comments: "They used these photos and shamed me on Facebook, saying how I dress and where I go with my friends. Just to falsify the work that I do and my credibility by attacking my personal life, rather than what I actually report as a journalist." She felt more vulnerable to this type of attack because of the Uyghur community's traditional values, which imposed restrictions on how she should express her personality in public. These intersecting pressures from both the diaspora community and the repressive state illustrate the broader power dynamics in which regimes are able to build on and manipulate predominant patriarchal norms and gender stereotypes to amplify attacks, tarnish the reputation of outspoken women activists, and undermine their position.

Mariam AlKhawaja: A Human Rights Activist From Bahrain[35]

Exiled and living under constant surveillance, Mariam continues her relentless fight against the Bahraini government's repression. Her father has been a political prisoner for over a decade, and while she advocates for his release, her activism has made her a high-profile target. Since she left Bahrain under threat of arrest, Mariam has faced state-sponsored digital and physical harassment, even while in exile in Denmark.

In Bahrain, platforms like Twitter became indispensable for coordinating protests and documenting human rights abuses during the 2011 uprising. "[We tweeted] in

[35] Mariam has consented to publicly sharing her identity.

real time about what was happening when we were getting attacked by the police. It was also for communication between us," she explains. But digital freedom quickly turned dangerous as the government also adapted its strategies to exploit these digital tools – deploying phishing attacks and throttling internet speeds in protest zones. She finds herself in a familiar paradox as many other human rights defenders face when using digital platforms: "I started realizing that the tools we are using as activists, as a method of trying to make change in the country, [were] also being used by the government against us." Yet, despite the risk, she continues to use these tools, knowing they help her connect with defenders back home and raise awareness.

As a woman tirelessly advocating for human rights while in exile, Mariam has faced explicitly gendered threats. Sexualized rumors, accusations of promiscuity, and claims of abortions circulate online to tarnish her reputation. This kind of gender-based digital repression is not new for Mariam. In one instance, she was the subject of a degrading Twitter poll asking whether her breasts were real or fake, with photo edits exaggerating her chest — a campaign disturbingly launched as she spoke about Bahrain's political prisoners, particularly on the plight of detained women. "[When they target women], it's sexually explicit," she notes. Gender-based attacks have compounded attacks on other aspects of her identity, including religion: "And because I am Muslim, that's the way they target me." Her male peers, by contrast, are often accused of homosexuality. These smear campaigns have also affected her family, with her parents targeted as a tactic to pressure her into silence.

Even offline, the attacks persist. Stalkers have followed her, often with cameras. During advocacy trips, she has been followed by people attempting to capture photos to create rumours of "immoral behaviour" that fuel the defamation campaigns flooding the internet. These campaigns run in parallel to her policy engagement and public appearances.

Mariam refrains from reporting these online and offline threats to law enforcement, believing the system is not on her side. Diaspora communities face systemic discrimination, and she feels Western governments and institutions are complicit in ignoring, or even enabling, attacks on exiled activists, especially when the regimes targeting them are political allies. "[The police] were never a symbol of protection for me, but one of threat," she explains.

Mariam's challenges extend beyond attacks sponsored by her country of origin. In Denmark, she faces racist hostility and Islamophobic abuse. "Some days I get as much, if not more, abuse from racist Danish people than from pro-government trolls," she says, recounting comments suggesting she "should go home." Even her advocacy for her father's release, who is a Danish citizen, invites backlash and doubts about her belonging in Danish society. "I don't feel safe in the West either," she admits.

While she has managed to avoid physical imprisonment in Bahrain, Mariam still lives in constant anxiety, strained by the possibility of surveillance. She fears her devices are compromised by spyware, making her vulnerable to monitoring and tracking.

Her activism now extends to training other exiled activists in digital security, a responsibility she views as essential. "Governments go after the weakest link.

If you're the weak link, you put everyone else at risk," she emphasizes. Yet, the threat landscape continues to evolve, with spyware like Pegasus exemplifying the advanced technologies authoritarian regimes deploy. "This technology creates constant anxiety. It's not only about access to devices but about making you fearful that they could access them at any time."

The burden on Mariam has been psychological, social, and professional. Despite her talents, Mariam has lost confidence that she could secure employment with international human rights organizations due to "constant targeting" and security threats from the Bahraini government. Yet, amid her tireless advocacy, Mariam remains undeterred yet critical of the systemic injustices that allow regimes to repress activists like her with impunity, the complicity of Western institutions, and the exploitation of digital platforms by authoritarian governments. To her, justice is more than freedom of speech – it is about building a digital space where voices from the global majority are truly heard.

Several study participants described the intersectionality of gender and race in the threats they received. As representatives of marginalized ethnic groups, the public presence and outspokenness of these women challenged dominant power structures on multiple fronts provoking a strong backlash. An anti-war activist from Russia who hailed from the Tartar minority recalled how her video statement for a project exposing the violent history of Russian colonialism went viral on Instagram and X. In return, a barrage of online bullying took aim at her ethnic origins with comments about her "Asian backwardness," "uneducated savagery," and that she should "be grateful we brought civilization." The perpetrators escalated these racist attacks over the gender-based abuse. As if reminiscing about the medieval conquests the activist had highlighted in her video, one of the attackers wrote that "all Tatar women should be raped and murdered." The respondent recalled: "There were threats to find where I live, threats of rape, comments about appearance…beautiful or not beautiful, rapeable or unrapeable—I think most women go through this."

Kurdish participants as well as a respondent from the Arab minority in Iran shared similar experiences. They were accused of separatism and faced fierce gender-based and racist attacks.

Fatima: A Journalist From Syria[36]

Fatima, a Syrian journalist, has been relentlessly harassed, threatened, and blacklisted for her work. She can hardly bear to think about Syria now, let alone continue writing about the never-ending tragedy of the conflict. After years of covering anti-regime groups, freedom of expression, and gender issues, Fatima fled her home country due to the threats she faced. But even in exile in the U.K., the attacks have not stopped. Online and offline harassment continue to haunt her across borders.

[36] The participant has been assigned a pseudonym to protect their identity.

As a woman who speaks out against both dictatorship and patriarchy, Fatima has faced ongoing digital attacks since 2011, when she began writing critically against the regime. Disinformation spread through posts and messages discrediting her, and groups on Facebook and WhatsApp circulated false claims about her political affiliations, along with a flood of sexist abuse aimed at silencing her. The attacks intensified not only because of her activism, but also because she is a woman. For example, she has been accused of being a “Western agent” for not wearing a hijab. She was also shamed for her working-class background and called a “whore” and “troublemaker” in numerous online comments.

Even in the U.K., the harassment follows her. She has been physically stalked and her social media and email accounts have been repeatedly targeted by hackers. Despite being in exile, Fatima receives warnings of state-sponsored digital attacks, a reminder that repression knows no borders. The threats have come from all sides – both the regime and anti-regime groups she criticized. “One of the main attacks against me,” she explains, “is that I criticize the rebels more than the regime.” This has left her distrustful of fellow Syrians she meets, wary of their potential ties to the regime.

Fatima’s family, including her daughter and uncle, was also attacked. Social media comments specifically mentioned her young daughter, a chilling reminder of how women’s families are often used as leverage to silence them. “It’s easier to silence women,” Fatima says. “They use your family to pressure you, and it works.” Fatima’s close family members urged her to stay quiet, making it not only the regime’s supporters who pressured her into silence, but also her family.

Fatima's working-class background has amplified the pressure and harassment she faces. Her socioeconomic status has not only been weaponized in the attacks against her, but has also shaped the responses from her community, which might have been more supportive of an elite member facing similar harassment. “Being from an unprivileged family, poor background,” she reflects, “I think if I was of such a high class or whatever, or Bourgeoisie, or just influential, or have an influential parent, it wouldn't have been the same.” These class dynamics add another layer to her struggle, as she continues to feel the weight of both societal and systemic marginalization.

These attacks have taken a toll on her mental health and daily life. Fatima has become suspicious of every email, message, or online contact, wondering if they might be part of the ongoing harassment. When she realized that writing about Syria led to intensified online attacks, she stopped. Now, if she does write about her home country, she only publishes in English, refusing to translate her work into Arabic to avoid the backlash. “Being scared of expressing my opinion is the main cause of my trauma,” she says.

To protect her family, Fatima asked them to deactivate their social media accounts and avoid responding to harassing messages. The fear for their safety has distanced her from her loved ones, including her parents in Syria, with whom she has not spoken in years.

Despite all these challenges, Fatima continues to advocate for greater accountability from social media platforms, particularly for Arabic-speaking women. She recalls how platforms like Facebook have been slow to remove harmful content, leaving her and others vulnerable to coordinated disinformation campaigns. Fatima dreams of a future where platforms have "a board of feminists" to advise on how to act when such incidents happen. She believes this would increase her sense of safety online and allow women like her to express their thoughts without fear of retaliation.

3.3 An Array of Perpetrators

Authoritarian regimes do not necessarily engage in transnational repression through centrally coordinated tactics and actors. Rather, research suggests that regimes rely on different configurations of facilitators and affiliates, including government-sponsored media outlets, loyalist diaspora groups, government-affiliated trolls, and even organized criminal groups, who enable and amplify threats against human rights defenders in other countries.[37] Such decentralized structures obfuscate the actual perpetrators making it difficult to attribute attacks to a specific government. Confirming these insights, the respondents in this study perceived the attacks to come from various aggressors whose abuses often built on and reinforced one another, not only intensifying the impact of online attacks but also occasionally crossing from digital to non-digital threats. The diffuse and anonymous nature of online attacks made it difficult for the targeted activists to attribute them to specific offenders. Social media, in particular, allowed government supporters to take initiative independently from any central authority whenever an activist appeared to challenge the political interests and values of the regime. Moreover, when authoritarian rulers tie their power to the preservation of traditional gender hierarchies, women speaking out about politics readily spark a backlash from groups and individuals that are not necessarily linked to the regime but still act in its interest on the basis of patriarchal and chauvinist ideas, sometimes simply because they feel provoked by the public presence of women activists.

In some cases, the link between an attack against research participants and their country of origin seemed more obvious. A prominent Uyghur human rights advocate recalled how an X account that she believed was run by the Chinese Foreign Ministry had amplified a defamation campaign against her. An exiled journalist from Azerbaijan explained how a defamatory video, originally posted on a Facebook profile associated with the youth branch of the ruling party, was then broadcast on state media. Similarly, an Eritrean human rights defender described how Eritrean embassy staff had spread disinformation against her and incited members of the Eritrean diaspora to attack her. An Iranian

[37] Marlies Glasius (2023), "Extraterritorial Authoritarian Practices: People of Turkish and Iranian Descent in the Netherlands," in *Authoritarian Practices in a Global Age*, (Oxford University Press).

journalist observed how coordinated online abuse and defamation typically starts on some anonymous X accounts and is then taken up by government-affiliated Telegram groups before appearing on the news websites of Iran's hardliners and the Revolutionary Guard. "Then these reports circulate again on social media networks and after that, threats and destruction start […] aiming to silence and to create a safe environment for the Islamic Republic," she said.

In addition to threats perceived as directly linked to regime actors and institutions, many respondents also mentioned government-organized trolls and inauthentic accounts engaging in coordinated attacks against their social media posts. An activist exiled from Tanzania observed a pattern where waves of abusive comments flooding her social media posts were initiated in the early morning, as if the attackers "had just started their shift." She suspected the attacks from these "lice" – as they are called in Tanzania – emanated from a troll farm run by the Tanzanian government. Two Uyghur human rights activists shared that they were targeted by smear campaigns from fake accounts using identical message templates and automated translations from Chinese into English. These attacks also intensified in accordance with working hours in China and usually stopped on weekends. These inauthentic timing patterns in the attacks against women critical of the Chinese government have been documented and visualized by researchers in other work.[38] Two activists originating from federal republics in Russia's Far East described how they were attacked for their anti-war activism by different groups of trolls organized, as they recounted, both by the local authorities in their respective home regions and the central government in Moscow. One of the women explained that comments denigrating her social media posts would appear in the comment section around the same time and with similar content. While one group of trolls posted in the local language, others commented in Russian and repeated the narrative of the Putin regime.

In addition to direct attacks by state or state-linked perpetrators, many of our respondents mentioned attacks by diaspora government supporters. These attacks were particularly problematic as they came with a higher perceived risk of physical threats in the host country. These risks seemed even more intense for women, and were further amplified for those belonging to ethnic minorities, because of existing patterns of gendered and racial discrimination. Reports of potential infiltrations and spying within diaspora groups further intensified feelings of uncertainty and distrust. For example, research participants originating from Turkey felt especially threatened by loyalists of President Erdoğan and right-wing nationalists who responded aggressively to any form of dissent. Attacks by these groups appeared to be self-initiated rather than directly linked to, and organized by, a state

[38] Albert Zhang and Danielle Cave (2022), "Smart Asian Women are the New Targets of CCP Global Online Repression," *ASPI The Strategist* (June 3) <https://www.aspistrategist.org.au/smart-asian-women-are-the-new-targets-of-ccp-global-online-repression>; Danielle Cave and Albert Zhang (2022), "Musk's Twitter Takeover Comes as the CCP Steps up Its Targeting of Smart Asian Women," *ASPI The Strategist* (November 6) <https://www.aspistrategist.org.au/musks-twitter-takeover-comes-as-the-ccp-steps-up-its-targeting-of-smart-asian-women/>.

actor. While not necessarily state-linked, respondents explained that these groups threatened to report government critics to authorities in Turkey in order to have them arrested if and when they returned for a visit. A woman living in Germany from the Alevi community, a religious minority in Turkey, said that she was afraid whenever she or fellow activists travelled back home. “I am always worried, because I know that there are reporting mechanisms for the government. There are apps and websites and people can easily report back to the government and make accusations,” she said. In a comparable case, a Saudi student at a British university was sentenced to 34 years in prison in Saudi Arabia for retweeting posts of Saudi women rights activists when she returned home for a visit.[39]

Other respondents of Turkish and Kurdish origin living in Germany, which hosts the largest diaspora from Turkey worldwide, shared that after being attacked online they feared someone would recognise them in the street or find out where they lived. Such fears were not unwarranted as shown by the case of an Eritrean human rights defender in Sweden. Following calls to attack her on Facebook, members of the Eritrean diaspora harassed and assaulted her eight times in places that included the supermarket, the gym, and the subway. Eventually, she stopped using public transport. Both the governments of Eritrea and Turkey rely on large sections of government supporters in their diasporas to function as levers of control and punishment against critical voices.[40]

Meron Estefanos: An Activist from Eritrea[41]

Meron is Swedish-Eritrean who grew up in Sweden, where her parents were deeply involved in the Eritrean liberation movement. She moved back to Eritrea in 2002 and stayed for two years. At the time, she did not know much about the situation in her country of origin. When she arrived she was shocked to learn about the forced military service and other restrictions that the state imposes on its population. “There is no such thing as freedom of expression or movement,” she says. After her return to Sweden she began engaging in human rights activism opposing the Eritrean government. Meron currently lives in East Africa where she continues to advocate for Eritrean refugees.

Communication and digital tools are key for Meron’s activism. She uses phone calls to connect with refugees during their dangerous journeys. She relies on Proton Mail, Signal, and other channels to securely share information on human traffickers with law enforcement and human rights groups in different countries. Social media platforms like X and Facebook help her raise awareness and pressure decision makers to better protect the human rights of Eritreans. With her reporting on human trafficking and advocacy for Eritrean refugees, she feels

[39] Stephanie Kirchgaessner (2022), “Saudi Woman Given 34-Year Prison Sentence for Using Twitter,” *The Guardian* (August 16) <https://www.theguardian.com/world/2022/aug/16/saudi-woman-given-34-year-prison-sentence-for-using-twitter>.

[40] Baser, Bahar and Ahmet Erdi Ozturk (2020), “Positive and Negative Diaspora Governance in Context: From Public Diplomacy to Transnational Authoritarianism,” *Middle East Critique* 29(3); Hirt, Nicole and Abdulkader Saleh Mohammad (2017), “By Way of Patriotism, Coercion, or Instrumentalization: How the Eritrean Regime Makes Use of the Diaspora to Stabilize Its Rule,” *Globalizations* 15(2).

[41] Meron has consented to publicly sharing her identity.

she has stepped on the feet of various governments, including Ethiopia, Rwanda, and Israel. But it is mostly her criticism of the Eritrean government that exposes her to gendered threats and digital transnational repression.

Ever since becoming an activist, she has been attacked by trolls who she believes are organized by the Eritrean government. After media appearances, Meron regularly faces hundreds of racist and misogynistic attacks. She is repeatedly called "a prostitute," "an animal," and "ugly." Meron also noticed that, after attackers target the international journalists who interview her, they appear less willing to cover her activism and Eritrea. To mobilize the diaspora against her, she says, Eritrean government figures have spread false claims that she would receive part of the ransom paid to human traffickers and decide over the fate of refugees who risked crossing the Mediterranean. "When they make such accusations, it really harms you," she says, referring to the thousands of Eritreans who died after fleeing their home country.

The online assailants never challenge Meron's ideas, rather they attack her as a woman and question her parental ability. As she recounted: "They call me a drug addict and that I lost my kids through social services even though I live with my kids." These constant attacks and accusations on social media leave Meron feeling tired and depressed. She has also been subject to physical attacks. After a Facebook post was circulated in Sweden that incited the Eritrean diaspora to break her bones, she was assaulted by eight people in a nightclub. Other attacks happened at the gym, in the supermarket, and on public transport.

To protect herself Meron constantly updates her digital security knowledge. Activist support groups on digital safety and mental support have helped her the most. She also takes breaks from social media and blocks perpetrators. Still, Meron questions if online safety measures are worthwhile given the resources repressive governments have at their disposal. Meron believes that social media companies have neglected Eritrean communities as they fail to capture how hate speech and bullying in local languages violates platforms' guidelines.

China also leverages members of its large, globally distributed diaspora to pressure and silence critics.[42] Certain Uyghur respondents shared suspicions that the government incites Chinese students on government-sponsored study-abroad programs to disrupt events and protests in Western countries that raise awareness about the genocide against

[42] Amnesty International (2024), "China: Overseas Students Face Harassment and Surveillance in Campaign for Transnational Repression," <https://www.amnesty.org/en/latest/news/2024/05/china-overseas-students-face-harassment-and-surveillance-in-campaign-of-transnational-repression/>; Freedom House (2021), "China: Transnational Repression Origin Country Case Study," <https://freedomhouse.org/report/transnational-repression/china>.

the Uyghur population. A Uyghur human rights advocate recalled a presentation she gave at a university in the U.S. where a Chinese student constantly tried to interrupt and distract her. One of the organizers later told her it was as if "an internet troll was taken from the cyber world and put in our classroom." In addition to such direct disruption, respondents shared how the Chinese government tries to infiltrate and instrumentalize the Uyghur diaspora. Threats against families in the country of origin are used to blackmail diaspora members to spy on others.[43] The same human rights defender also explained how social media accounts of Uyghur individuals shared fake photoshopped photos of her naked and spread rumours about how she had destroyed her husband's previous marriage, which led to her isolation within the diaspora community. Because the language and narrative of these allegations resembled the Chinese Communist Party (CCP)'s broader strategy of using patriarchal norms to suppress politically active women,[44] she suspected these individuals were backed by Chinese authorities or forced to post this content.

Even in cases where the majority of emigrants shared an opposition to the home regime, participants reported attacks from other exiles. According to interview participants, the Iranian regime appeared to be particularly adept in manipulating divisions within the diaspora to pit groups against one another.[45] For example, several respondents described how regime-affiliated social media accounts disseminated information that helped portray them as "regime apologists," stirring up harassment and abuse from hardline opposition groups. An Iranian journalist in exile explained that someone – she suspected government agents – managed to access and leak her confidential communication with contacts in Iran. The way the leaked information was framed spoke to existing conflicts in the diaspora. As a result, she explained that she was not only attacked as a "traitor" and "regime collaborator," but also faced gendered threats and abuse on a massive scale.

3.4 The Motives and Triggers of Gender-Based Digital Transnational Repression

When authoritarian regimes repress across borders, they aim to strengthen their position both domestically and on the international level.[46] Autocrats seek to silence human rights defenders who can mobilize international attention, causing reputational damage and external pressure. They also try to contain diaspora activists who might influence

[43] David Tobin and Nyrola Elimä (2023), "We Know You Better than You Know Yourself": China's Transnational Repression of the Uyghur Diaspora," *The University of Sheffield* <https://www.sheffield.ac.uk/seas/research/we-know-you-better-you-know-yourself-chinas-transnational-repression-uyghur-diaspora>.

[44] Leta Hong Fincher (2018), "Xi Jinping's Authoritarian Rise in China Has Been Powered by Sexism," *The Washington Post* (March 1) <https://www.washingtonpost.com/news/global-opinions/wp/2018/03/01/xi-jinpings-authoritarian-rise-in-china-has-been-powered-by-sexism>.

[45] See also Reporters Without Borders (2024), "Watch Out Because We're Coming for You: Transnational Repression of Iranian Journalists in the UK," <https://rsf.org/en/watch-out-because-we-re-coming-you-rsf-report-unprecedented-transnational-repression-iranian>.

[46] Alexander Dukalskis (2021), *Making the World Safe for Dictatorship*. (Oxford University Press).

domestic audiences by spreading alternative views or supporting the organization of political discontent.[47] Cross-border repression often targets figures with a certain visibility and outreach in transnational information flows who are perceived to contest the power and control of the home state regime.[48] Exiled women human rights defenders, especially those who successfully leverage their position in transnational advocacy networks and influence public opinion and decision-making in Western democracies, challenge not only the authority of the authoritarian regimes in their home country, but also the patriarchal norms that undergird their rule.

Attacks against targets in exile or in the diaspora are not random, but often appear to be triggered by specific events or occasions. Many study participants drew a direct line between the threats they experienced and their work to raise awareness and expose their country of origin's abuse of power and human rights violations. Two exiled Azerbaijani journalists were threatened for reporting on police torture and government corruption. An Iranian journalist was attacked for exposing disinformation by the Revolutionary Guard that aimed to cover up the killing of protesters in 2019. Uyghur human rights advocates were harassed and smeared as they tried to raise international awareness on the genocidal persecution of their people in the Xinjiang region in northwestern China.

Respondents also tied the attacks against them to their criticism of government authorities and their public visibility in doing so. For example, a participant from Turkey's diaspora gave interviews on German television in which she questioned the policies of President Erdoğan, while a Russian activist published a viral TikTok video lambasting Putin and the war against Ukraine. A Hong Kong activist commented on the apparent link between digital harassment and her media visibility: "if I go on media…I get a bunch of attacks the day after." Similarly, a Rwandan activist observed a pattern of attacks in conjunction with her public appearances and meetings with policy makers in the U.S. and Europe: "It's clearly aligned with the day and time of my engagements." Likewise, a Chinese activist faced a surge in trolling after a high-profile speech in the Australian Senate, noting that "the trolls were really active after that."

Other respondents mentioned speaking out during sensitive political events in their country of origin, such as during protests, elections, or armed conflicts, as a catalyst for heightened abuse and harassment. Two Chinese activists described escalated threats during the National Congress of the Chinese Communist Party (CCP). One also observed that the Chinese national day "was a big day for the Chinese communists. So they have a lot of people on Twitter to attack their enemies." She noted that the attacks also increased around other special dates, such as the anniversary of Tiananmen Square.

[47] *Ibid*; Dana Moss (2022), The Arab Spring Abroad: Diaspora Activism Against Authoritarian Regimes. (Cambridge University Press).

[48] Marcus Michaelsen (2018), "Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State," *Globalizations* 15(2).

In all these examples respondents demanded accountability: they posed critical questions, revealed information that was hidden by those with power, and challenged governments to justify their conduct. The threats targeted at respondents sought to mute their voices, a core practice of authoritarian rule.[49] For offenders, gendered abuse and misogyny served as tools to subvert and punish criticism and dissent against the home state from abroad.

In other cases, attacks on research participants were clearly tied to speaking out about issues of gender equality and women rights. Topics such as intimate partner violence, femicide, sexual harassment, female sexuality, divorce, and abortion rights consistently triggered extensive threats and abuse. Some respondents said that simply being present in public would trigger an increase in insults and threats against them. The range of potential perpetrators was also broader including regime actors and their affiliates as well as members of the same diaspora community, opposition groups, and even colleagues and friends. In these types of attacks, the gender-identity of the targeted women, in addition to their opposition to patriarchal power structures, appeared to motivate the attacks and threats they experienced.

When asked about the underlying intent of the attacks they were exposed to, research participants unanimously believed the purpose was to intimidate and silence, humiliate, and discredit them. Their experiences showed that assailants sought to inhibit women's political participation in public space by reinforcing gendered hierarchies. These findings highlight that, for authoritarian rulers, patriarchal ideas and chauvinism running through certain communities often conveniently align with their goal to suppress demands for transparency, justice, and political rights. Authoritarian states rely on such structures to fuel hostility towards women human rights defenders and, consequently, bolster their own unaccountable and oppressive regimes.

3.5 The Impacts of Gender-Based Digital Transnational Repression

3.5.1 Stress and Anxiety—Impacts on Mental Health and Wellbeing

The digital threats, insults, and harassment experienced by respondents deeply impacted their mental health and wellbeing. Respondents described feelings of exhaustion, stress, anxiety, burnout, sleeplessness, and depression as a result of attacks and threats they received. The abuse and hate that would inevitably follow any of their posts caused dread

[49] Marlies Glasius (2018), "What Authoritarianism is… and is not: A Practice Perspective," *International Affairs* 94(3).

and doubts, paving the way towards self-censorship and withdrawal. Others described the ways they engaged with their attackers, for example by investigating and blocking profiles or countering allegations, to the point that they had no energy left for their actual work.

An Iranian singer and feminist activist said she found herself in a constant dilemma. She debated whether to post online and witness unfolding attacks against her, or simply to live with the uncertainty that her profile might have been taken down again. As she explained: “something you've built, the audience you’ve gained, and the relationships you’ve formed through your page […] disappear at any moment.” Another Iranian participant, a women’s rights advocate in the U.K., recalled how the mental pressure and damage resulting from the smear campaigns against her became so severe that she “preferred not to exist at all” and contemplated suicide.

Dounia Filali: A Journalist from Morocco[50]

Dounia Moustaslim (also known as Dounia Filali), a journalist in exile, was among the first to expose the Moroccan security apparatus’ use of spyware against political figures and journalists. Through her newspaper and YouTube channel, she also reported on political repression and human rights abuses, including torture. Her work gained attention, but also brought her under dangerous scrutiny.

In 2020, while living in China, Dounia uploaded a teaser for an interview with a political activist. Soon after, her pictures were plastered across Moroccan newspapers linked to the state’s security agencies. These outlets, in collaboration with the government, launched a smear campaign that quickly shifted from attacking her work to targeting her personally and sexually – tactics often used against women dissenters. As Dounia recounts: “[i]f the target is a woman, false charges related to prostitution, immorality, and the like are immediately fabricated against her.”

The harassment initially targeted her family, falsely accusing her mother of “forbidden relationships.” These stories spread through Moroccan media and social media platforms. Soon, the attacks turned on Dounia, labelling her a “corrupt prostitute” and accusing her of selling sex toys. The accusations escalated to claims of arms trafficking, drug smuggling, and money laundering, particularly as her reporting covered sensitive political issues. Videos mocking her were produced in multiple languages and shared with Chinese authorities triggering an investigation into Dounia and her family.

One day, a Moroccan agent filmed her home in Shenzhen and threatened her by sharing a video with online groups of the local Moroccan diaspora community in China. Recognizing the imminent risk Dounia faced from the Moroccan regime while she was abroad, the UNHCR determined that she was a refugee under international law.

However, the harassment she faced from Morocco, even in China, forced Dounia and her family to flee to France in 2021. The disinformation followed. She believes that new waves of disinformation campaigns alleging that she had hidden assets

[50] Dounia has consented to publicly sharing her identity.

and evaded taxes influenced French authorities to suspend her access to accommodation and assistance. Dounia felt abandoned by the system that should have protected her: "[When] will this psychological torture practiced by the French government and, behind it, the Moroccan government, end?"

The disinformation did not just damage her reputation – she also believes it jeopardized her refugee claim in France. She observed that Morocco adjusted the content of its disinformation campaigns based on Dounia's host state, aiming to create complications for her within each political context. "Hundreds of articles started circulating false accusations, claiming we supported Iran and Hezbollah," she recalls. These lies were based on a fabricated Facebook post that was falsely attributed to her husband.

Fearing further attacks, Dounia cut off communication with her family in Morocco and avoids sharing personal information online. Despite the toll this constant pressure and threat to her safety has taken on her health, she remains determined to continue her human rights work. She hopes her story will inspire other journalists and activists to resist repression.

The threats and attacks experienced by respondents also profoundly altered their sense of security. Respondents were particularly troubled by messages threatening to find them or harm their children. Similar to Noushin, the Iranian journalist whose story we presented in the introduction, several participants said they were afraid to leave their homes and venture freely on the streets after experiencing a sustained wave of online abuse. A few participants, notably of Iranian, Uyghur, and Azerbaijani origin, said they preferred living in buildings with increased security measures, such as CCTV surveillance or guarded condos. The anxiety was even more pronounced in host countries that were easily accessible to agents from the country of origin. A Tartar activist, who was exposed to a massive online attack and rape threats for her video statement on Russia's violent colonial history, lived in Serbia at the time the video was released. As Serbia still maintained close ties to Russia even after the start of the full-scale war against Ukraine, she became concerned about possible assaults. "You start to think…do the people who write to you on Telegram know where you are?", she said, pointing out how easy it was to find someone to simply beat her up. Even when she moved to the Netherlands, her sense of security was not fully restored. Referring to the attempts to poison several Russian exiled journalists in European countries she added: "Nowhere is safe actually and you cannot really hide from Russian security services."

For many respondents, residing in a Western democracy did not necessarily allay fears raised by transnational threats. A Uyghur human rights defender leading a diaspora association based in the U.S. explained how she had tried to ignore the slurs and rumours spread by those seeking to undermine her credibility. However, the attacks became more serious for her when Chinese trolls posted her home address on social media and in the comments section of a public online event. “I have kids, I got scared. I don't want to lie. At night, I had a hard time sleeping. I tell myself that I live in the U.S. so what could they do…But at the same time, you never know.” She also found out about attempts to infiltrate her social circles with spies and she felt observed by unknown persons in her neighbourhood. The pressure of these threats and the advocacy work exposing her daily to the trauma of the genocide against her own people culminated in a panic attack that sent her to the hospital.

While some participants felt they were up against a powerful state, others, who believed they were targeted by regime loyalists in the diaspora, felt that any of their online attackers could be living right next door. A young German journalist of Assyrian descent from Turkey described being attacked by the social media accounts of the Grey Wolves, a group of Turkish right-wing extremists, after she reported on the oppression of ethnic minorities in Turkey. She also received a direct message on X from one of these profiles bullying her with surprisingly intimate information about her. Deeply unsettled about how the sender had obtained such personal detail, the journalist became anxious that her phone had been hacked or people were spying on her: “I was terribly scared. […] I didn't know at all who was doing what behind my back or whether someone in my environment or some of my friends were playing a false game.”

3.5.2 Distrust and Isolation—Impacts on Social Networks and Relationships

Digital threats also affected the social relations of the respondents in this study. Relationships with families and partners deteriorated under the stress and uncertainty caused by online harassment, attacks, and surveillance. The mistrust seeping into diaspora communities and online networks led to isolation and withdrawal.

Many research participants were forced to limit connections to family members in their country of origin to protect them from harm. They kept conversations with loved-ones to generalities and small talk, avoiding politics and their activist work. Some cut ties with family members on social media, deleting photos and even unfollowing their siblings. Others sacrificed contact entirely and stopped communicating with their relatives. Most Uyghur respondents had not heard from their families for years.

In other cases, respondents’ family members still residing in their country of origin were harassed and threatened in retaliation. This pressure naturally transferred to the activists, confronting them with feelings of guilt and a dilemma over how to continue their work. An Iranian journalist and human rights defender explained how her parents had asked her to stop giving interviews to Persian-language media abroad because of the possibility of putting them at risk. Her mother once told her that she would mute the sound when she saw her daughter on television. “My mom said, I just want to see your face, but I do not care about what you are saying. What consequences do these words have other than threatening your brother?"

The risks and mental costs associated with diaspora activism also strained respondents’ relationships with their partners. The same Iranian journalist explained how her husband, seeing her depressed and anxious under the weight of online attacks, tried to convince her to quit activism. “It has been very difficult for me when everyone...my family, my husband, mom, dad…all tell me to stop my activities,” she said. Other participants shared that partners urged them to abandon activism in order to prevent further harm to themselves and their families. An Indigenous activist from the Far East of the Russian Federation who engaged in anti-war activism reported how the daily routines of her engagement put her relationship under pressure, even though her husband was generally supportive. In addition to her regular job, she was busy into the evening organizing protests and writing social media posts, whereas her husband took over household chores and childcare. Under these circumstances, she found it difficult to expect sympathy when dealing with the anxiety and depression caused by online abuse and threats.

The relationships of other respondents collapsed under the pressures resulting from their activism. An Iranian activist based in Canada mentioned that her Iranian partner broke up with her after she received threats likely coming from the Iranian regime or its affiliates. Similarly, a Moroccan human rights defender living in the U.S. said that her partner had left her because her struggle against the Moroccan government and its supporters was “taking such a big part” of her life.

As a consequence of online harassment and surveillance many respondents became more cautious in their overall social relations, especially to other diaspora members. Several women said they were distrustful whenever they met new people. Worried that the other person might have been sent to spy on them, they examined new acquaintances for suspicious behaviour. Other participants avoided places and events frequented by other members of the diaspora or exile community or switched to another language whenever they heard someone speaking in their first language.

The experience of seeing online defamation and rumours amplified by ordinary people also undermined some respondents’ trust and openness to others. An Eritrean human rights defender said she had become cynical and reduced her socializing because “people don’t deserve my time.” An Iranian journalist based in France recalled how another person living in exile, whom she had met in person, later shared social media posts smearing her reputation. As a result she was constantly ruminating about how others could cause her harm and kept to herself even more: “It’s like I’m building a wall around myself.”

A human rights defender from Rwanda shared that she avoided dating men out of fear they were sent by the Rwandan government to harm her. Because of the risks of physical threats from Turkish government supporters, two Kurdish participants in Germany also said that they had adapted their dating behaviour. While one of them avoided publishing her photo on dating apps, reducing her likelihood of meeting anyone at all, another respondent carefully scanned the online profiles of potential candidates, restricted the amount of personal details she shared, and prudently chose the location for her first meeting. A journalist of Chinese origin living in Australia described that her profiles on dating apps had been repeatedly suspended as a result of coordinated complaints that she suspected came from government-affiliated trolls.

Repression targeted at research participants also led to other diaspora or exile community members distancing themselves. An Eritrean human rights defender recalled attending a wedding in her community and hearing other guests whispering that she was considered part of the opposition. For Uyghurs abroad, even an association with a person speaking out about the camps and the genocide can have grave consequences.[51] Out of fear for their own relatives in Xinjiang, most diaspora members avoided being seen with human rights advocates in public or sharing their social media posts. Several Uyghur participants reported they had been excluded from community events and gatherings. A prominent human rights activist in the U.S. said she was uninvited from a wedding after Chinese police officers from her home town contacted the hosts and mentioned her by name as an unacceptable guest. A camp witness in the Netherlands explained that others in the diaspora talked to her only in private, but avoided adding her on social media or being seen together with her in public. “Even taking a picture with me is a crime. Being around me is also a crime. People keep a distance from me.”

3.5.3 Navigating Risks—Impacts on Activism and Professional Work

The exhaustion, distrust, and uncertainty that came with the digital threats against research participants also affected their activism and professional relationships. Respondents who were exposed to smear campaigns were anxious of the extent to which the allegations would undermine their reputation and credibility. They worried that colleagues or fellow activists might believe the rumours, at least in part. Some pointed out that even distanced family members had inquired whether the most egregious

[51] Amnesty International (2020), “Nowhere Feels Safe,” <https://www.amnesty.org/en/latest/research/2020/02/china-uyghurs-abroad-living-in-fear/>.

accusations were true. An Iranian journalist explained that people actually seemed to accept the propaganda about sexual harassment and rape in her media organization which spread online. “That is the bitter part of the story: the initial spark for these accusations is set by the cyber army of the Islamic Republic, but those who turn this spark into a fire are ordinary users, the very people around us.”

As a consequence of the attacks they experienced, many research participants started doubting their own willingness to bear the costs of activism and whether it was worthwhile to continue. Their deteriorating mental health affected productivity and work routines. Some were forced to withdraw, at least temporarily. Like several other respondents, an Eritrean human rights activist found that attacks which involved ordinary diaspora members took a particular toll on her and nourished her skepticism. “I am not an activist because I think I am the smartest person alive. I hope my work reflects the desires of the majority of Eritreans. When I see people overwhelmingly respond against my work I wonder if I am doing the right thing and it takes away from me.” She had taken breaks from activism to recover and mentioned fellow women activists who had quit entirely because they could no longer handle the harassment and insults. An Azerbaijani human rights defender also said that the need to protect her health and family from the fallout of massive online attacks left her no choice but to give up her work which she had pursued for two decades.

Even research participants who continued with their activism work had to constantly evaluate and navigate the associated risks. Fearing spying and surveillance, some stopped attending larger gatherings with other exiles. Instead of speaking out in public, others engaged in research and writing, behind-the-scenes organizing, published their work anonymously, or met within smaller, trusted circles. A Russian activist explained that she avoided openly collecting donations for Ukraine or writing about Russia as a “terrorist state” because such activities could be used to build a criminal case against her. The permanent possibility of being exposed to another wave of online harassment reminded an exiled Iranian journalist of the “red lines” that limited news publishing inside Iran. As she described, “unconsciously in your mind, you think if I write this sentence, they might attack me again.”

In addition to eliciting varying degrees of self-censorship and restraint, digital transnational repression also raised the costs of activism for research participants. Several respondents said they spent hours filtering through comments full of insults to block and report profiles on social media platforms. The time and energy they invested in this disheartening labour could have been easily directed to more positive work. A Kurdish activist who lost her Instagram profile with 4000 followers after coordinated attacks explained how she had to rebuild her community network from scratch.

Other constraints went beyond the digital realm. When her brothers were arrested in retaliation for her activities, an Azerbaijani journalist based in Norway went into financial debt to cover the expenses for the legal proceedings and to sustain the family. A few respondents said that due to criminal cases opened against them, they had to carefully consider travel routes to avoid getting detained and extradited by authorities in countries cooperating with the government in their country of origin.

Finally, the impacts of online threats, defamation, and heightened security concerns also affected the professional careers of some respondents in the host country. A Syrian activist in the U.K. said that because of the traumatizing impacts of violent threats against her she had stopped working on Syria-related projects and shifted her focus to other countries. An Iranian women rights defender in Canada thought that an international company in the health development sector which was about to hire her retracted the offer at the last minute because they had learned about her activism and imprisonment in Iran and feared that potential working relations with the country could be negatively affected. A Chinese journalist based in Australia explained that massive trolling and threats from other diaspora members made it difficult for her workplace to guarantee her safety and impeded her development within the organization. Similarly, a well-known Bahraini human rights defender thought that not all human rights organizations had the willingness and resources to do the extensive risk assessments that were necessary before working with her.

3.6 Digital Security Practices and Behavioural Changes

Research participants took a number of steps to mitigate the harms of digital attacks. They adapted their user behaviour and relied on different digital hygiene tools and practices. It was the targeted women who clearly bore the burden of such "preventive labour."[52] They were constantly assessing the risks of their online environment and invested time and effort to seek out digital security solutions to better protect themselves.

Two-factor-authentication and strong passwords – including the use of password managers – to access email and social media accounts were among the most commonly mentioned security practices used by participants. Signal and Proton Mail were frequently brought up as the communication tools that respondents perceived as the most secure. In contrast, Facebook Messenger, Telegram, and to some extent WhatsApp were considered less safe for sensitive communications. Many respondents only used these latter platforms when there was no other option. A Russian anti-war activist based in Poland said that on occasion she still uses Telegram because of contacts who could not be reached otherwise. She treated these communications "as if somebody definitely reads our correspondence."

[52] Sarah Sobieraj (2020), "Constant Calibration (Preventative Labour)," in Credible Threat: Attacks Against Women Online and the Future of Democracy. (Oxford University Press).

Meryem: A Human Rights Activist From Xinjiang, China[53]

Meryem and her family left the Xinjiang region in China for Turkey in the early 1990s, before settling in North America. As a child, Meryem's first exposure to the Chinese government's attempts to tightly control information about the rapidly intensifying oppression of the Uyghur culture and community in northwestern China was from family members engaged in human rights journalism. This instilled in her a determination to advocate for her homeland and people. She now works as a human rights defender in a nongovernmental organization.

Meryem has experienced various digital threats in response to her activism. She is frequently attacked by what she believes to be Chinese state-backed trolls on X, Facebook, and in the comment section on public Zoom meetings. Meryem's home address was posted on these platforms and, in turn, she received waves of threatening and hostile messages. She tried to mitigate the impacts of this type of harassment by turning off the comment section during virtual events. Unfortunately, while this approach blocks trolls, it also prohibits engagement with genuine participants who are interested in her activism work.

Offline threats and harassment have caused Meryem "reputational and psychological harm." For example, Meryem explains that Chinese government supporters attend Uyghur human rights conferences with the intent to humiliate, discredit, and shame her work. Meryem says that because she is a woman, perpetrators believe her activism is less impactful than a man's activism. But Meryem responds to these perpetrators by explaining that "I am being attacked [...] because I am speaking the truth [...] no matter what my gender is." Meryem knows she sacrifices her safety, but she will not let anyone stop her from being an activist.

Still, Meryem's wellbeing is compromised by the Chinese government's online harassment. She explains that, despite being an optimistic person, she suffered a panic attack because of the surveillance tactics launched against her. Meryem also experiences paranoia, engages in self-censorship, and refrains from communicating with friends and family members to "limit the information accessible to the attackers." In the face of constant online harassment, Meryem tries to stay positive by telling herself, "maybe I scared them, that's why they want to scare me." But more tangible action is needed. Meryem calls on social media platforms to better identify authoritarian-regime backed accounts that perpetrate gender-based digital transnational repression so they can be reported and blocked.

[53] The participant has been assigned a pseudonym to protect their identity.

Respondents highlighted the importance of having a first point of contact with knowledge on digital security. Often this person was a fellow activist, friend, or family member with some tech expertise who was readily available to give urgently needed advice on how to protect sensitive data and communications. The trust in these relationships also helped respondents to overcome the gendered dynamics often built into interventions for digital security education and support. Not only was available training mostly held by men but some participants also found it difficult to admit gaps in their knowledge on digital security because they did not want to contribute to stereotypes about women's inability to use technology.

Several respondents described their knowledge on digital security as poor, minimal, or beginner level. They had attended only one or no training at all. Often these participants saw themselves as powerless vis-à-vis resourceful government actors relying on invasive surveillance and coordinated defamation campaigns. In particular, the increasingly widespread use of commercial spyware added to these feelings of helplessness. A Russian activist who had never received training but tried to keep herself updated on digital security said that seeing all the recent cases of Pegasus spyware infections made her think that "everything I do to secure myself is not enough at all."

In contrast to these individual efforts to protect themselves, respondents who worked at large media organizations – with audiences in their countries of origin – received regular training on digital security. These organizations often had dedicated staff for technical and security support. Uyghur and Iranian journalists, in particular, mentioned these types of resources presumably because China and Iran are widely recognised as persistent perpetrators of digital transnational repression.

These differences in the digital security knowledge and skills of our respondents highlight that the process of mitigating the risks of digital threats is also marked by issues of inequality and privilege. Factors such as age, digital literacy, organizational ties, and the political backing of the host state clearly shape access to information and support on matters of digital security. As a result, some are exposed to more risks of digital threats than others. However, in the transnational networks of diaspora human rights defenders, any attack against the weakest link could lead to severe consequences for all involved. In the struggle against resourceful state actors, the unequal distribution of digital security resources and knowledge can introduce unforeseen risks and compound the vulnerabilities of all activists.

In addition to learning about the tools and practices of digital security, respondents also carefully considered the risks of their online environment and adapted their behaviour. They separated personal and professional accounts, scanned messages for phishing attempts, and trimmed their followers on social media. To limit their exposure to threats and insults, some respondents made their X and Instagram accounts private so that only accepted followers could reply to their posts, or send a direct message.

Respondents also avoided posting personal information on social media or photos that might expose families, friends, and other contacts. Several respondents said they were reluctant to write about their emotions as they thought perpetrators would exploit such information. An Iranian feminist said she stopped short of describing how much she missed the cooking of her grandmother as regime agents would understand that she had a special relationship they could use for insults and pressure. Others did not use geolocation or post about their movements in real time. An Iranian journalist in London said that when the threats against Persian-language media in the U.K. intensified and there were credible warnings about potential physical attacks, she became cautious to even share a photo of her balcony view out of fear it might help to locate her apartment. “I do not even feel safe sharing a picture of a blooming rose,” she explained.

Some respondents also stopped using social media altogether, or at least for longer periods until they found the emotional strength to face new potential attacks. A human rights activist from Eritrea said she had not used Facebook for four years and since then “life has been more peaceful.”

As a consequence of abuse and harassment, some participants carefully controlled their own online appearance. A young Kurdish activist in Germany conceded that the attacks on her looks had made her think preemptively about what dress or make-up to wear in her online videos, saying, “how I appear online, whether I look good and what I wear has an impact on how serious people take me.” A Uyghur human rights advocate said she avoided posting photos of herself and her friends going out because in the Uyghur diaspora community she believed such images could easily be used to smear her reputation.

3.7 Facing Gender-Based Digital Transnational Repression

Digital security practices and changes in individual online behaviour had a limited impact on respondents’ ability to prevent attacks and abuse. They still had to deal with a considerable amount of harassment, insults, and other threats. To mitigate psychological harm and insulate themselves from their assailants, respondents came up with different coping strategies. They actively reframed the attacks and built mental resilience, took care of their mental health and wellbeing, and sought support from family, friends, and peers.

A few respondents brushed aside the impacts of online threats, stressing they could not be affected. Some saw the attacks against them as a positive sign their work was having an effect on the regime and its affiliates. Respondents from different countries of origin said that, as a result of online harassment, they had received more support for their work and were taken more seriously. In particular, Uyghur respondents considered the decision to engage in human rights advocacy as a point of no return and they often felt a strong moral obligation to continue speaking out. An activist in the Netherlands who was consistently targeted with digital and physical threats said: “Despite all these difficulties, I never regret that I joined this line of work. I always tell myself that I’m doing the right thing, I’m on the right side. I can face my dignity in this world and next.” Another outspoken Uyghur campaigner based in the U.S. pointed out that the attacks would even push her to go further: “I want to show them that it’s not going to work. […]. We are human beings, you know, we get tired, we get sleepy, we get jet lag, and after all these troubles, we just want to take a week off and rest. But when we see those attacks, we will think: let's just make them go crazy!”.

Others compared their digital risks to the hazards faced by activists inside the country of origin who were in the direct reach of repressive state agents. An Ethiopian journalist who left her home country after enduring a period of detention said, when she embarked on her professional career, she had prepared for “prison and death” – a reality for journalists in Ethiopia. This experience helped her reframe the online attacks.

Several research participants recounted similar trajectories where initially they engaged with the attackers but eventually built immunity against their attacks. These respondents described how they initially tried to respond to insults and defamation in the often futile attempt to dispel the rumours and counter accusations that were spreading against them on social media. An Azerbaijani women’s rights activist recalled her learning process: “Reacting to trolls was a mistake. The more you react, the more trolls write back and blow up their opinions. I was giving them the platform to keep writing.” A Uyghur human rights defender remembered that insulting language used against her made her so angry that she replied in the same genre: “I shouldn’t have done that, I realized later. But I wasn’t doing well mentally back then and never in my life have I been attacked by someone in that way.”

Eventually these respondents came to disregard the attacks, setting other priorities and preserving resources. The Uyghur human rights activist said she “numbed” herself against the harassment. Another Uyghur respondent tried to draw strength from the thought that she was not alone: “I think I've built a Chinese wall around me, trying to ignore all these online threats and bots. I told myself I’m not the only one, everyone is experiencing the same thing.” Participants often came to realize that the perpetrators wanted to see them weak and they turned their focus to persisting in the long run.

Recognizing the need to take care of their mental health and wellbeing, a number of participants resorted to therapy and counselling. They used these sessions to process the online threats they experienced as well as broader issues linked to their identity as migrants with ties to repressive contexts. However, some respondents mentioned that therapists in Global North countries sometimes had difficulty providing advice on how to deal with authoritarian repression. A Venezuelan activist based in the U.S. even feared that online therapy sessions could be intercepted by agents from her country of origin. Other than therapy, respondents also mentioned activities such as yoga, meditation, walks and time spent with friends, or going out as deliberate choices to disconnect from the online world.

The majority of respondents turned to family, friends, and fellow activists for support in coping with the harms of digital threats. They considered these safe circles as important sanctuaries for solace and recovery. In particular, the connection with other women who were confronted with similar threats was seen by many as helpful to learn about different coping strategies and the evolving tactics of the attackers, and to not feel isolated. Several participants highlighted the "sisterhood" of like-minded women activists as a key source of solidarity and advice when facing online abuse and harassment. An Eritrean human rights defender said she was in a Signal group that provided a space for moral encouragement and discussions about how to deal with trolls.

Yet, the support of the respondents' close circles also had limits. Several respondents said they were hesitant to share their experiences of sexual harassment with their partners to protect them from distress and embarrassment. Others did not want to cause their family members additional concerns about their safety. Two respondents from Iran and Russia also pointed out that the resources for peer support were not endless. As each person individually coped with the stress and uncertainty of living in exile and being the target of transnational repression, they sometimes lacked the energy to help others who might be going through a particularly intense online attack or mental crisis. At times, these women said, it was necessary to draw boundaries to protect their own wellbeing.

In addition to seeking comfort and strength within their immediate environment, several respondents spoke out publicly about the attacks they were facing, drawing support from a broader online audience of followers. After announcing that she was being threatened by numerous anonymous accounts, a Russian anti-war activist recalled that many people sent messages of support encouraging her to continue her activities. An Azerbaijani journalist said that going public about the abuse and harassment she experienced helped her realize that she was not the only one going through this torment. It also connected her with organizations that work to raise awareness of online safety risks for women journalists.

Furthermore, exposing perpetrators' actions also represented a form of resistance. Several participants mobilized their social media networks to report accounts involved in attacks against them to the relevant social media platforms. After she exposed some of the manipulation tactics she had experienced when being targeted by a coordinated defamation campaign on social media and government-affiliated television programs, an

Azerbaijani journalist recalled her social media channels had gained thousands of new followers – which she considered a positive development for her advocacy work. This interviewee considered publicizing the attacks as a strategy to build immunity: “Once it’s public, they go back and review and realize they haven’t achieved anything.”

Respondents actively fought back against gender-based digital transnational repression with various coping strategies, including developing mental resilience, building networks of solidarity and peer support, and speaking out openly about the abuse they endured. They found ways to defend their space, overcoming the fear, paralysis, and isolation that perpetrators sought to instill in them. However, respondents’ resourcefulness could not offset the power imbalances at the root of these threats. In their struggle against the actions of repressive state actors that mobilize patriarchal structures and misogynistic ideas against them, women human rights defenders require the support and protection of the authorities in their countries of residence and the digital platforms on which most of the attacks unfold. We turn to these two key actors in the next sections.

Section 4: The Role of Host States in Protecting Against Digital Transnational Repression

In Section 3, a theme emerged from participants who repeatedly conveyed the sense that they were left alone to defend themselves against the threats of gender-based digital transnational repression. Although research participants displayed resilience, the protection mechanisms available to them could be considered woefully inadequate to match the scale and far-reaching nature of the threats and abuse they experienced – let alone prevent gender-based digital transnational repression from occurring in the first place.

In exploring this absence of protection mechanisms, we bring our attention to the governments in the host states where exiled and diaspora women human rights defenders reside. Under international human rights law, host states have an obligation to curtail digital transnational repression and protect human rights defenders and journalists within their borders against cross-border repression by authoritarian actors. In this section, after highlighting examples of respondents' interactions with host state authorities, we discuss selected initiatives undertaken by the U.S., Canada, the U.K., and some E.U. governments to address transnational repression and more specifically digital transnational repression.[54] If these states are to live up to their own domestic standards of human rights protection, then they must implement more decisive measures to protect the fundamental rights of targeted individuals and communities.

4.1 Seeking Support from Host State Authorities

Our interviews confirm findings from previous research indicating shortcomings in support from host state authorities for targets of digital transnational repression.[55] This protection gap is even bigger for women targeted with gender-based threats from state actors in their countries of origin because, according to some respondents, law enforcement authorities often lack an understanding of the political motivation for such attacks and the necessary sensitivity for dealing with victims of online abuse. As a result, many respondents doubted the benefits of reporting incidents to the police in their host state.

[54] An exhaustive list of such initiatives across all host states is beyond the scope of this report. However, the following summary shows that, while host states are increasingly active on the issue of transnational repression, there remains a lot of work to be done.

[55] Yana Gorokhovskaia and Isabel Linzer (2022), "Defending Democracy in Exile: Policy Responses to Transnational Repression," *Freedom House* <https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf>; Anstis, Siena and Sophie Barnett (2022), "Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses," *Journal of Human Rights Practice* 14(2).

A Russian activist based in the Netherlands expressed her skepticism as follows: “There is this kind of indifference towards online harassment, it is not commonly considered as stepping stone for something more horrifying.”

Activists based in authoritarian host states with limited rule of law had no expectations of support from authorities. Three respondents from Tanzania, Burundi, and Sudan living in Kenya, Uganda, and Tanzania, respectively, said they would not bother to report threats to the police. In other cases, respondents believed that potential ties between authorities in the host state and their country of origin meant that any encounter with security forces entailed significant risks. Three study participants from Myanmar, who fled military oppression to Thailand from where they continued to be involved in activism, explained that exiles often had to bribe local Thai authorities to avoid deportation to their country of origin. One of these respondents explained that, at checkpoints in the border region, the Thai military would check the phones of individuals from Myanmar for photos and other evidence of their participation in the resistance against military rule in their origin country. “If someone cannot pay any money, they are deported back to the Myanmar side of the border and sent to the Myanmar military.” Activist groups also had knowledge of a list of high-profile exiles shared by the military leadership from Myanmar with security agencies in Thailand demanding their extradition.

When participants based in democratic host states reported attacks to the police, they were frustrated by the limited response. Especially in cases of online abuse, the evidence presented was often not considered sufficient to initiate an investigation. One research participant was a journalist from Turkey’s diaspora in Germany who had been targeted with sexualised threats from social media accounts linked to the Grey Wolves, a transnationally active group of Turkish right-wing nationalists. She recalled with embarrassment presenting screenshots to two women police officers of threats containing highly intimate details. The officers were neither familiar with the background of the organization nor could they provide any advice on possible protection measures or emergency support. She was eventually told that they could not do anything because the accounts had been deactivated. She described the futility of the exercise: “and then you’re left alone with that. In the end it was useless.” Similarly, an Iranian women rights defender in Canada experienced online threats and sexual harassment originating from the social media accounts of other Iranians, some of whom she believed were based in the same city. She reported this to the police, who made her feel dismissed when they explained that these posts would be protected under Canadian human rights law.

Other respondents were hesitant to report threats to police because they feared their race, religion, or immigration status might cause additional problems and not bring the expected protection. A human rights defender from Bahrain summarized how growing up in Scandinavia influenced her view on the authorities: “[t]he police were never a symbol of protection for me, they are always a symbol of threat. And to me as a Muslim brown woman in the West, I don't think the system is on my side. So, it doesn’t come to mind that I could potentially go to the police and report on things!” An Iranian activist based in France suspected that the interaction between law enforcement agencies and diaspora members would also be influenced by the security interests of the host government. Even in cases with a recognised risk of transnational repression, such as Iran, authorities might approach potential target groups to seek information for their own investigations rather than to provide protection.

In contrast, some respondents did receive police support from their host states. Uyghur human rights defenders working in established diaspora and advocacy organizations in the U.S. benefited from access to and protection from law enforcement authorities. These women explained that they were in regular communication with the U.S. Federal Bureau of Investigation (FBI) and were given direct contact information in case of emergency. Some had also received advice on how to secure their apartments. In addition, they had been able to raise the issue of threats from Chinese regime actors with government policy-makers. These support networks clearly contributed to their feelings of safety.

The perception of China (and, in other cases, Iran) as a persistent perpetrator of transnational repression and geo-political rival of the U.S. has likely worked to the advantage of these communities. Working for well-connected organizations with the political backing of the host government has likely given these human rights defenders better support than members of other diaspora or exiled communities. This suggests that the protection of targets at risk of transnational repression may depend on their positionality in the host country context – which means that numerous individuals and communities are likely to find insufficient protection even in a host state that is actively working on transnational repression. Further, even where host state authorities provide support against the general threats of transnational repression, such support mechanisms and interventions are not specifically tailored to the gender-based aspects of such attacks. In this next subsection, we examine various responses to digital transnational repression from a selection of host states to better understand gaps in protection.

4.2 Host State Policies in Response to Digital Transnational Repression

With the experiences of respondents in mind, we review a selection of host state policies addressing transnational repression.[56] While not exhaustive, our analysis suggests that

[56] There have also been some multilateral efforts. For example, the G7 Rapid Response Mechanism includes transnational repression as an area of concern. See Global Affairs Canada (2023), “G7 Rapid Response Mechanism Annual Report 2022,” *Government of Canada* <https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2022-annual-report-rapport-annuel.aspx?lang=eng>; Freedom House (2023), “Declaration of Principles to Combat Transnational Repression,” <https://freedomhouse.org/2023/summit-for-democracy-transnational-repression>.

although states are increasingly aware of the issue of transnational repression (including its digital dimensions), there are significant deficiencies in their responses and more efforts need to be made to prevent such attacks. This section is primarily based on desk-research analyzing public statements, documents, and other sources regarding state responses to transnational repression.

4.2.1 Host State: United States

Under the Biden Administration, the U.S. emerged as a leader in responding to transnational repression. However, it remains to be seen how these policies will play out in practice, whether they will remain in effect under subsequent administrations, and whether they can provide sufficient protection for women human rights defenders based in the U.S. who are targeted with digital or other forms of transnational repression.[57] In particular, reforms around digital transnational repression (and transnational repression more generally) are not explicitly sensitive to the unique effects experienced by women human rights defenders as targets of digital transnational repression.[58] Further, some reforms – such as encouraging targets of digital transnational repression to report to law enforcement – may prove ineffective unless broader systemic changes ensure that targeted persons have lawful status in the U.S., there is a shift in law enforcement culture to be more sensitive to the particular needs of targets of transnational repression, and there are assurances that reporting such incidents will not negatively impact asylum seekers' refugee status.[59]

That being said, under the Biden Administration, the U.S. did make significant efforts to "mainstream" an understanding of the practice of transnational repression in federal agencies and in international fora. For example, the FBI undertakes awareness-raising regarding the threat of transnational repression through various public-facing mechanisms and runs a tip-line for individuals to report acts of transnational repression.[60] The U.S. Department of State includes coverage of transnational repression as an issue in its

[57] Freedom House has also summarized and described U.S. responses to transnational repression with observations regarding additional gaps in the country's response to transnational repression. See Freedom House (2022), "Unsafe in America: Transnational Repression in the United States," <https://freedomhouse.org/report/transnational-repression/united-states>.

[58] GAO (2023), "Human Rights: Agency Actions Needed to Address Harassment of Dissidents and Other Tactics of Transnational Repression in the U.S.," *United States Government Accountability Office* <https://www.gao.gov/assets/D23106183.pdf>; U.S. Department of State (2024), "United States Guidance for Online Platforms on Protecting Human Rights Defenders Online," <https://www.state.gov/wp-content/uploads/2024/03/United-States-Guidance-for-Online-Platforms-on-Protecting-Human-Rights-Defenders-Online-1.pdf>.

[59] Freedom House (2022), "Unsafe in America: Transnational Repression in the United States," <https://freedomhouse.org/report/transnational-repression/united-states>.

[60] Federal Bureau of Investigation (2024), "Transnational Repression," <https://www.fbi.gov/investigate/counterintelligence/transnational-repression>.

country reports.[61] The U.S. Department of Justice (DOJ) has issued indictments against several individuals, characterizing the alleged underlying acts as transnational repression.[62] Legislative measures have also been taken and/or are being debated at the time of publication of this report. In 2021, the U.S. Congress passed the *Transnational Repression Accountability and Prevention Act* ("TRAP Act") intended to help address the abuse of Interpol.[63] Further, several bills addressing transnational repression are also pending, one which proposes to criminalize the practice (the "*Schiff Bill*")[64] and another which proposes specific policy responses (the "*Merkley Bill*").[65]

These U.S. responses to transnational repression have included a specific concern for digital transnational repression. The *Merkley Bill* proposes to develop and refine inter-agency responses to transnational repression including addressing the "access, use, and storage of personal digital data by governments and technology companies for the purposes of transnational repression"[66] as well as proposing assistance to civil society organizations which includes digital security installation and support, emergency response to cyberattacks, and the development of "enhanced capacity to deter surveillance and monitoring by malicious actors."[67]

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) announced the creation of a Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression ("Strategic Dialogue on Transnational Repression"), along with Australia, Canada, Denmark, Estonia, France, Japan, New Zealand, and the U.K., with the goal of information-sharing regarding actions and best practices in response to transnational repression, the threat landscape, and opportunities for protecting the cybersecurity of civil society actors.[68] CISA has also implemented a High-Risk Community Protection

[61] See, for example, US Department of State (2023), "Iran 2023 Human Rights Report," *Bureau of Democracy, Human Rights, and Labour* <https://www.state.gov/wp-content/uploads/2024/02/528267_IRAN-2023-HUMAN-RIGHTS-REPORT.pdf>.

[62] *Ibid.*

[63] Sen. Rick Scott (2021), "National Defense Authorization Act for Fiscal Year 2022," *Senate - Energy and Natural Resources* <https://www.congress.gov/bill/117th-congress/senate-bill/1605/text>. Regarding the abuse of Interpol, see, for example, Edward Lemon (2019), "Weaponizing Interpol," *Journal of Democracy* 30(2).

[64] Rep. Adam Schiff (2023), "Stop Transnational Repression Act," *House - Judiciary; Foreign Affairs* <https://www.congress.gov/bill/118th-congress/house-bill/5907>.

[65] Sen. Jeff Merkley (2023), "A Bill to Address Transnational Repression by Foreign Governments Against Private Individuals, and for Other Purposes," *Senate and House of Representatives - 118th Congress* <https://www.congress.gov/bill/118th-congress/senate-bill/831/text>.

[66] *Ibid* at 9.

[67] *Ibid* at 13.

[68] Cybersecurity & Infrastructure Security Agency (2023), "Joint Statement on the Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression," *America's Cyber Defense Agency* (March 30) <https://www.cisa.gov/news-events/news/joint-statement-strategic-dialogue-cybersecurity-civil-society-under-threat-transnational-repression>.

Initiative to respond to transnational repression and a Joint Cyber Defense Collaborative (JCDC) intended to bring together technology companies, civil society groups, and government to "strengthen the cybersecurity of civil society organizations in the U.S. under threat of transnational repression."[69] CISA and other internationally-based cybersecurity agencies have developed a guide for civil society groups to mitigate the risks of digital transnational repression perpetrated by states.[70] Suggestions are targeted towards civil society organizations, civil society individuals, and software manufacturers.

The U.S. response to digital transnational repression under the Biden Administration also sought to curb the activities of the mercenary spyware industry. Spyware is not only used by governments to target and surveil perceived domestic opponents, but also to reach across borders and engage in the transnational surveillance of diaspora and exile communities.[71] Efforts have included: an Executive Order prohibiting the use of spyware by the U.S. government where it poses counterintelligence or security risks to the U.S. or the improper use (such as targeting human rights defenders) by a foreign government or person;[72] adding spyware companies to the Commerce Department's Bureau of Industry and Security Entity Control List;[73] revising export controls; and implementing visa restrictions,[74] among other initiatives.[75]

[69] Homeland Security (2023), "Secretary Mayorkas Discusses New U.S. Efforts to Counter the Misuse of Technology and the Spread of Digital Authoritarianism at Summit for Democracy," *Homeland Security* (March 30) <https://www.dhs.gov/news/2023/03/30/secretary-mayorkas-discusses-new-us-efforts-counter-spread-digital-authoritarianism>.

[70] Canadian Centre for Cyber Security (2024), "Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society," *Government of Canada* (May 14) <https://www.cyber.gc.ca/en/news-events/mitigating-cyber-threats-with-limited-resources-guidance-civil-society>.

[71] Stephanie Kirchgaessner (2021), "Hotel Rwanda Activist's Daughter Placed Under Pegasus Surveillance," *The Guardian* (July 19) <https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance>.

[72] The White House (2023), "Executive Order on the Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security," (March 27) <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/#:~:text=Therefore%2C%20I%20hereby%20establish%20as,foreign%20government%20or%20foreign%20person>.

[73] U.S. Department of Commerce Office of Congressional and Public Affairs (2023), "Commerce Adds Four Entities to Entity List for Trafficking in Cyber Exploits," *Bureau of Industry and Security* <https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3297-2023-07-18-bis-press-package-spyware-document/file>.

[74] Antony Blinken (2024), "Announcement of a Visa Restriction Policy to Promote Accountability for the Misuse of Commercial Spyware," *U.S. Department of State* (February 5) <https://www.state.gov/announcement-of-a-visa-restriction-policy-to-promote-accountability-for-the-misuse-of-commercial-spyware/>.

[75] Industry and Security Bureau (2022), "Information Security Controls: Cybersecurity Items," *Federal Register* (May 26) <https://www.federalregister.gov/documents/2022/05/26/2022-11282/information-security-controls-cybersecurity-items>.

4.2.2 Host State: Canada

In Canada, transnational repression falls within the departmental portfolio responsible for addressing foreign interference.[76] In September 2023, the Canadian government launched a Public Inquiry into Foreign Interference.[77] This process began after the June 2023 killing of Hardeep Singh Nijjar, a Sikh separatist leader in Canada, and the Canadian Prime Minister's subsequent allegation that the Indian government may have been involved.[78] While the inquiry primarily focused on interference in Canadian elections, the Commission's initial report, published in May 2024, identifies the targeting of diaspora communities as "one of the primary ways in which countries carry out foreign inference in Canada."[79] The Commission process, however, has been riddled with controversy. For example, a Uyghur human rights group pulled out "claiming the process could put victims at risk."[80] Others note that the Commission lacks the ability to help and protect targets who had already complained about transnational repression to Canadian law enforcement.[81] The failure to protect victims of transnational repression while asking them to provide testimony to a government commission effectively illustrates how out of touch Canadian government officials are with the risks faced by diaspora and exile communities in Canada.

Prior to these developments, in October 2023, the Standing Committee on Access to Information, Privacy and Ethics published a report on "Foreign Interference and the Threats to the Integrity of Democratic Institutions, Intellectual Property and the Canadian State."[82] This report stated that the definition of foreign interference includes the targeting of "diaspora communities in relation to homeland issues."[83] The Committee recommended that the Government of Canada "ensure that any legislative mechanisms developed to counter foreign interference take into account how they might affect individuals and communities already victimized or targeted by foreign interference in Canada, and that

[76] Freedom House (2022), "Canada: Transnational Repression Host Country Case Study," <https://freedomhouse.org/report/transnational-repression/canada>; Government of Canada (2024), "Addressing Foreign Interference," <https://www.justice.gc.ca/eng/cons/fi-ie/form-formulaire.html>.

[77] Government of Canada (2023), "Government of Canada Launches Public Inquiry Into Foreign Interference," (September 7) <https://www.canada.ca/en/democratic-institutions/news/2023/09/government-of-canada-launches-public-inquiry-into-foreign-interference.html>.

[78] Jessica Murphy (2024), "Three Arrested and Charged Over Sikh Activist's Killing in Canada," *BBC* (May 4) <https://www.bbc.com/news/world-us-canada-67836968>.

[79] Foreign Interference Commission (2024), "Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions," *Government of Canada* (May 3) <https://foreigninterferencecommission.ca/fileadmin/user_upload/Foreign_Interference_Commission_-_Initial_Report__May_2024__-_Digital.pdf>.

[80] Catharine Tunney (2024), "Uyghur Group Withdraws from Foreign Interference Inquiry, Says Victims Won't be Protected," *CBC* (February 1) <https://www.cbc.ca/lite/story/1.7100381>.

[81] Marie Lamensch (2024), "As Foreign Interference Takes Hold, Ottawa Looks Away," *The Walrus* (August 5) <https://thewalrus.ca/as-foreign-interference-takes-hold-ottawa-looks-away/>.

[82] House of Commons (2023), "Foreign Interference and the Threats to the Integrity of Democratic Institutions, Intellectual Property and the Canadian State," *Standing Committee on Access to Information, Privacy and Ethics* <https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/report-10>.

[83] *Ibid* at 9.

it include these communities in developing measures to counter the impacts of interference on them."[84] The National Security and Intelligence Committee of Parliamentarians (NSICOP) has also published analysis on foreign interference, which included references to transnational repression.[85]

However, recognition of the problem of transnational repression within Canadian borders is a far cry from taking specific measures that effectively protect targets – particularly women human rights defenders in exile or in the diaspora – and evaluate this issue from a human-rights centred perspective. For example, in June 2024, Bill C-70, *An Act Respecting Countering Foreign Interference*, was enacted. While intended to strengthen "Canada's ability to detect, disrupt and counter foreign interference threats to all people in Canada, including members of diaspora communities, through a series of new measures and legislative amendments to national security and criminal laws,"[86] this legislation has been the subject of extensive criticism from human rights organizations as being in breach of Canadian constitutional and human rights law.[87]

Canada has also engaged in multilateral action to address transnational repression. It is among the signatories of the U.S.-led Strategic Dialogue on Transnational Repression and the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware.[88] It was also a participant in the drafting of a set of Guiding Principles on Government Use of Surveillance Technologies, and a member of a multilateral Code of

[84] *Ibid* at 19.

[85] The National Security and Intelligence Committee of Parliamentarians (2024), "Special Report on Foreign Interference in Canada's Democratic Processes and Institutions," at 13 <https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf>.

[86] Public Safety Canada (2024), "Legislation to Counter Foreign Interference Receives Royal Assent," Government of Canada (June 21) <https://www.canada.ca/en/public-safety-canada/news/2024/06/legislation-to-counter-foreign-interference-receives-royal-assent.html

[87] British Columbia Civil Liberties Association (2024), "Joint Statement: Organizations Urge MPs to Extend Study of Bill C-70," (June 6) <https://bccla.org/policy-submission/joint-statement-organizations-urge-mps-to-extend-study-of-bill-c-70/>; Centre for Free Expression (2024), "Charter Rights Under Threat if Senate Fails to Fix Foreign Interference Bill: If They Don't Act, We Will, Say CFE and 9 Other Civil Society Groups," (June 19) <https://cfe.torontomu.ca/news/charter-rights-under-threat-if-senate-fails-fix-foreign-interference-bill-if-they-dont-act-we>; *Canadian Civil Liberties Association* (2024), "CCLA Reaction to the Introduction of Bill C-70," (May 14) <https://ccla.org/criminal-justice/ccla-reaction-to-the-introduction-of-bill-c-70/>; Shakir Rahim, Anaïs Bussières McNicoll, and Noa Mendelsohn Aviv (2024), "Submission to the Standing Committee on National Security, Defence and Veterans Affairs Regarding Bill C-70, An Act Respecting Countering Foreign Interference," Canadian Civil Liberties Association (June 10) <https://ccla.org/wp-content/uploads/2024/06/CCLA-Submission-to-SECD-on-Bill-C-70-An-Act-Respecting-Countering-Foreign-Interference.pdf>.

[88] Cybersecurity & Infrastructure Security Agency (2023), "Joint Statement on the Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression," *America's Cyber Defense Agency* (March 30) <https://www.cisa.gov/news-events/news/joint-statement-strategic-dialogue-cybersecurity-civil-society-under-threat-transnational-repression>; Cybersecurity & Infrastructure Security Agency (2023), "CISA and UK NCSC Hold Inaugural Meeting of Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression," *America's Cyber Defense Agency* (September 29) <https://www.cisa.gov/news-events/news/cisa-and-uk-ncsc-hold-inaugural-meeting-strategic-dialogue-cybersecurity-civil-society-under-threat>.

Conduct for Enhancing Export Controls of Goods and Technology That Could Be Misused and Lead to Serious Violations or Abuses of Human Rights.[89] It remains to be seen how much of an active participant Canada will be in these processes, or whether it takes a backseat to these primarily U.S.-led policy interventions around transnational repression and remains passively aware, but ultimately unmoved, in tackling the issue.

Canada does employ some practices that recognize how members of specific exile or diaspora communities are targeted by foreign states.[90] For example, it shares information about transnational repression with foreign governments and dedicates a "stream for resettling human rights defenders as refugees in Canada."[91] But members of diaspora and exile communities living in Canada share that digital transnational repression remains an "everyday problem for many Canadians" that the government has failed to adequately address.[92] In short, Canada's limited policy interventions to date regarding transnational repression, including its digital forms, have been lacking and such communities remain without effective protection.

4.2.3 Host States in Europe

The European Union (E.U.) and its member states as well as other European countries show varying degrees of awareness of the issue of transnational repression. A lack of a shared problem definition and diverging political priorities have delayed any coordinated response. As in Canada, within the E.U., transnational repression is often subsumed under initiatives seeking to counter foreign interference which is perceived as a growing threat to democratic institutions and processes.[93]

In May 2023, the Committee on Legal Affairs and Human Rights of the Council of Europe's Parliamentary Assembly published a draft resolution that was one of the first documents at the European level dedicated specifically to transnational repression, providing a definition and a set of broad recommendations for countermeasures.[94] The E.U. Parliament

[89] The White House (2023), "Fact Sheet: Advancing Technology for Democracy," (March 29) <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/29/fact-sheet-advancing-technology-for-democracy-at-home-and-abroad/>.

[90] Freedom House (2022), "Canada: Transnational Repression Host Country Case Study," at 1 <https://freedomhouse.org/sites/default/files/2022-08/TransnationalRepressionReport2022_CaseStudy_Canada.pdf>.

[91] *Ibid*.

[92] Marie Lamensch (2024), "As Foreign Interference Takes Hold, Ottawa Looks Away," *The Walrus* (August 5) <https://thewalrus.ca/as-foreign-interference-takes-hold-ottawa-looks-away/>; Marie Lamensch (2023), "Ottawa Can Do More to Stop Transnational Repression," *Centre for International Governance Innovation* (March 4) <https://www.cigionline.org/articles/ottawa-can-do-more-to-stop-digital-transnational-repression/>.

[93] Clothilde Goujard (2024), "Barbarians at the Gate: Von der Leyen Makes Foreign Influence a Key Campaign Topic," *Politico* (May 14) <https://www.politico.eu/article/von-der-leyen-proposes-new-eu-disinformation-law-to-counter-foreign-meddling/>.

[94] Parliamentary Assembly (2023), "Transnational Repression as a Growing Threat to the Rule of Law

adopted two resolutions in March 2022 and in June 2023 with recommendations regarding steps that need to be taken to address foreign interference, including addressing the role of online disinformation.[95] The European Parliament has also adopted a recommendation in 2022 regarding the negotiation of a cooperation agreement between the E.U. and Interpol limiting the institution's abuse by repressive regimes targeting critics abroad.[96]

More specific to digital transnational repression, the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent spyware (the PEGA Committee) has outlined a set of proposed reforms to curb the abuse of spyware.[97] Further, the E.U. *Digital Services Act* provides a set of measures intended to update and harmonize the legal framework in the E.U. around the regulation of illegal content, including disinformation.[98] Transparency provisions in the *Act* have been identified as an important mechanism for better understanding how platforms apportion resources to deal with online content, particularly in languages other than English.[99] Efforts to combat violence against women and domestic violence, which include proposals for addressing online content, could further curb digital transnational repression.[100]

It is also worth noting that, to the extent that measures like the *Digital Services Act* (or the U.K.'s *Online Safety Act*, mentioned below) are compliant with international human rights law and are able to effectively protect against technology-facilitated gender-based violence, such legislation will likely also have a positive effect on protecting women from being the target of digital transnational repression. However, such legislation is likely insufficient in and of itself unless it specifically addresses state or state-related actors as primary perpetrators of digital transnational repression and that this requires a unique set of policy responses.

and Human Rights," *Committee on Legal Affairs and Human Rights* (June 5) <https://rm.coe.int/transnational-repression-as-a-growing-threat-to-the-rule-of-law-and-hu/1680ab5b07>.

[95] European Parliament (2022), "Foreign Interference in All Democratic Processes in the European Union," (March 9) <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html>; European Parliament (2023), "Foreign Interference in All Democratic Processes in the European Union, Including Disinformation," (June 1) <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0219_EN.pdf>.

[96] European Parliament (2022), "Negotiations for a Cooperation Agreement Between the EU and Interpol," (July 5) <https://www.europarl.europa.eu/doceo/document/TA-9-2022-0275_EN.html>.

[97] European Parliament (2023), "Spyware: MEPs Call for Full Investigations and Safeguards to Prevent Abuse," *News European Parliament* (June 15) <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse>.

[98] European Commission (2024), "The Digital Services Act," <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en#new-rules-in-a-nutshell>.

[99] European Commission (2024), "DSA Transparency Database," *Directorate-General for Communications Networks, Content and Technology* <https://transparency.dsa.ec.europa.eu/>.

[100] European Union (2022), "Proposal for a Directive of the European Parliament and of the Council on Combating Violence Against Women and Domestic Violence," EUR-Lex <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0105>.

Host State: Germany

Germany is an important European host country for exiles targeted by transnational repression. According to the Freedom House dataset on physical acts of transnational repression, at least 12 foreign governments have targeted their nationals on German territory since 2014.[101] Germany's domestic intelligence agency regularly documents selected incidents of transnational repression committed by countries such as China, Russia, Turkey, and Iran in its annual reports.[102] In August 2023, the agency published a warning about an ongoing phishing campaign against Iranian regime critics in Germany.[103] Among our study participants, human rights defenders of Palestinian-Jordanian, Russian, Iranian, Azerbaijani, Uyghur, Turkish, and Kurdish backgrounds living in Germany were targeted with digital threats from what they described as state or state-affiliated actors in their country of origin. Although several parliamentary inquiries have raised this issue[104] and the current government has committed to improving protection for civil society actors at risk of cross-border persecution, Germany still does not have a dedicated response to transnational repression. Particularly in cases of digital transnational repression, police often fail to recognize the political background and thus cannot provide the appropriate support.[105]

Host State: U.K.

The U.K., another key destination for perpetrators of transnational repression, established a Defending Democracy Task Force in 2022 to "protect the democratic integrity of the U.K. from threats of foreign interference" and specifically includes transnational repression as one of the threats to be addressed.[106] The U.K. has engaged in legislative reform, implementing a new Foreign Influence Registration Scheme and adopting the *National Security Act 2023*. The Act introduces the offence of foreign interference,[107] which

[101] Freedom House (2022), "Germany: Transnational Repression Host Country Case Study," <https://freedomhouse.org/report/transnational-repression/germany>.

[102] Bundesministerium des Innern und für Heimat (2023), "Verfassungsschutzbericht 2023," <https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2024-06-18-verfassungsschutzbericht-2023.pdf>.

[103] Bundesamt für Verfassungsschutz (2023), "Warnhinweis zu Cyberspionage gegen Kritiker des iranischen Regimes in Deutschland," <https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-01-bfv-cyber-brief.pdf?__blob=publicationFile&v=2>.

[104] See, for example, Deutscher Bundestag (2021), "Schutz von Menschenrechtsverteidigern und Menschenrechtsverteidigerinnen in Deutschland," <https://dserver.bundestag.de/btd/19/325/1932565.pdf>; Deutscher Bundestag (2024), "Transnationale Repression gegen ausländische Staatsbürger in Deutschland," <https://dserver.bundestag.de/btd/20/115/2011508.pdf>.

[105] Hakan Tanriverdi, Max Zierer, Ann-Kathrin Wetter, Kai Biermann, and Thi Do Nguyen (2020), "Lined Up in the Sights of Vietnamese Hackers," *Interaktiv: BR24* (October 8) <https://interaktiv.br.de/ocean-lotus/en/index.html>.

[106] Home Office, Cabinet Office, and The Rt Hon Tom Tugendhat MBE VR (2022), "Ministerial Taskforce Meets to Tackle State Threats to UK Democracy," *Government of United Kingdom* (November 28) <https://www.gov.uk/government/news/ministerial-taskforce-meets-to-tackle-state-threats-to-uk-democracy>.

[107] Government of United Kingdom (2024), "Foreign Interference National Security Bill Factsheet," *Home Office* (May 3) <https://www.gov.uk/government/publications/national-security-bill-factsheets/foreign-interference-national-security-bill-factsheet>.

includes “interfering with the exercise by a particular person of a Convention right in the United Kingdom” such as freedom of speech.[108] In October 2023, the U.K. adopted the *Online Safety Act 2023*, which designates foreign interference offences as a priority offence under the legislation.[109] The *Act* also contains specific provisions regarding steps to protect women and girls online.[110]

The U.K. is also participating in various initiatives to tackle transnational repression led by the U.S., including efforts to strengthen the cybersecurity of civil society organizations targeted by transnational repression. For example, in September 2023, CISA and the U.K. National Cyber Security Centre (UK-NCSC) held the first Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression.[111]

4.3 Growing but Insufficient Responses by Host States

A review of host state policies addressing transnational repression and its digital dimensions demonstrates an inadequate response. One overarching concern in state responses to date has been the misguided integration of transnational repression into broader policies addressing foreign interference. Transnational repression raises a unique set of human rights violations of diaspora individuals and communities, while foreign interference has been (at least initially) conceptualized as threats that are directed against the national security interests of a state or democratic processes such as elections.

By prioritizing the foreign interference paradigm to deal with transnational repression, host states may fail to recognize and specifically address the entire range of transnational repression practices as a series of human rights violations that they are obliged to protect against and remedy. The lens of foreign interference is too narrow to address this range of harms. It focuses on competition between states and the targeting of a state’s territory and institutions by a foreign actor rather than on the expansion of domestic repression to enclose individuals in the diaspora or in exile who simply happen to reside in another state. Transnational repression gives rise to a complex interagency issue that requires collaboration between authorities responsible for areas as diverse as foreign

[108] Legislation.gov.uk (2023), “National Security Act 2023,” <https://www.legislation.gov.uk/ukpga/2023/32/part/1/crossheading/foreign-interference/enacted>.

[109] Legislation.gov.uk (2023), “Online Safety Act 2023,” <https://www.legislation.gov.uk/ukpga/2023/50/enacted>.

[110] Department for Science, Innovation and Technology and The Rt Hon Michelle Donelan (2023), “Britain Makes Internet Safer, as Online Safety Bill Finished and Ready to Become Law,” *Government of United Kingdom* (September 19) <https://www.gov.uk/government/news/britain-makes-internet-safer-as-online-safety-bill-finished-and-ready-to-become-law>.

[111] Cybersecurity & Infrastructure Security Agency (2023), “CISA and UK NCSC Hold Inaugural Meeting of Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression,” America’s Cyber Defense Agency (September 29) <https://www.cisa.gov/news-events/news/cisa-and-uk-ncsc-hold-inaugural-meeting-strategic-dialogue-cybersecurity-civil-society-under-threat>.

policy, security, migration, platform regulation, and violence against women, among others. Therefore, it is critical that the dominant framework in driving future policy is that of rights-protection. Only with such an approach can host states avoid creating further harms by, for example, enacting legislation that ends up securitizing and punishing the same communities that require protection.

It is also worth underlining that host state responses to transnational repression will require broader, more systematic reforms. For example, law enforcement agencies have historically and notoriously failed to address, or even take seriously, gender-based violence, routinely re-victimizing women while also being a major source of such violence.[112] Finally, host states' immigration policies which prevent individuals at risk from receiving lawful status within the host country in a timely manner (or at all) and engaging in rights-violating extraditions or deportations back to perpetrating states also form part of a policy fabric that facilitates transnational repression.[113] Without addressing these larger issues, policy initiatives around transnational repression will be limited in their possible positive impacts.

[112] Htun, Mala and Francesca R. Jensenius (2020), "Fighting Violence Against Women: Laws, Norms & Challenges Ahead," *Daedalus* 149(1).

[113] Lily Sparks and Kate Weine (2024), "We Will Find You: A Global Look at How Governments Repress Nationals Abroad," *Human Rights Watch* (February 22) <https://www.hrw.org/report/2024/02/22/we-will-find-you/global-look-how-governments-repress-nationals-abroad>.

Section 5: The Role of Social Media Platforms in Supporting Targets of Digital Transnational Repression

This section reviews the experiences of research participants with social media platforms which were considered a significant site of digital transnational repression. We review, at a high-level, the practices and policies of a subset of social media platforms and conclude that these companies do not appear to have specific policies or resources dedicated to preventing digital transnational repression. Further, the implementation of existing community guidelines and policies has been an abject failure, as reflected in the experiences of research participants who highlighted numerous ways in which their accounts have been compromised and the lack of responsiveness from these platforms.

5.1 "Soulless Machines": Seeking Support from Social Media Platforms

Research participants continued to rely on big social media platforms for information sharing, advocacy, and activism. Instagram and X were the most mentioned communication tools used by participants to showcase their work and connect to others. As a result, these platforms were also the primary sites for threats and attacks against these women. Perpetrators exploited the technical affordances of these platforms, to manipulate crowd- and algorithm-driven news feeds for the viral distribution of harassment and defamation. The platforms' content moderation tools often failed to detect and prevent online abuse, particularly outside the context of English-speaking communities. Respondents expressed feelings of abandonment by platforms whenever their posts came under attack from regime-affiliated mobs leading to their accounts being taken over, or their posts being muted by false mass reports. Platforms remained unreachable and mechanisms for redress proved unresponsive.

Several respondents used the available mechanisms to block and report attackers in response to insults and harassment on social media. Some of them consistently engaged in this procedure as a means of self-defence and drawing boundaries. A Uyghur journalist exposed to persistent harassment and defamation from Chinese trolls said she reported on every platform of the accounts that attacked her: "Whether it's Twitter, Facebook, Instagram, it doesn't matter. I also block these individuals because when you don't see them, you won't get triggered. I immediately report individuals who are engaged in harassment and it reduces their visibility, but also sends a clear message that their behaviour is unacceptable."

However, other participants were skeptical about the use of reporting. The sheer number of accounts involved in threats and trolling made it impossible for individual activists to flag everything to the platform, given the limits on their time and energy for dealing with abusive posts. One respondent reflected on the burden on targets to document and prove the connection between harmful content and state actors to the platform. Further, reporting threats in languages other than English, such as Uyghur, Persian, Arabic, Turkish, Mandarin, or Azerbaijani, sometimes required translations which is an additional burden: "Re-reading or re-watching harsh messages is difficult, and most of the time, the content of these messages is not easily translatable," said an Iranian women's rights activist and musician.[114] Further, social media terminology surrounding breaches have been inconsistent across platforms, making it difficult for content moderators and activists to control the onslaught of harassment.[115]

Moreover, perpetrators also learned to exploit the reporting mechanisms against activists. A number of study participants said their profiles on Instagram or X had been blocked or shut down as a result of mass reporting by their adversaries. The procedures and decisions behind the blocking of profiles remained opaque. To an Australia-based activist from the Russian Federation it seemed as if a quota was set for complaints that would automatically lead to the blocking of a profile, which she viewed as a form of platform-facilitated censorship that attackers were abusing systematically. A respondent from Turkey's diaspora in Germany pointed out that users needed more transparency: "We need to learn more about why certain posts are removed or profiles deleted. What kind of profiles have the power to report? Which server engaged in reporting? Maybe there are a lot of people who create a lot of fake accounts to systematically report posts. There should be clearer rules as to how and why certain things are removed online."

Automated content moderation algorithms remained obscure to study participants. A U.S.-based activist from Russia observed that her Instagram posts depicting examples of the threats and hate speech directed against her were blocked, while the original posts were not. She suspected that accounts with a greater number of followers were monitored more closely. Another Russian anti-war activist based in Poland was uncertain about the actual practices of content removal: "If I post something offensive against the Russian government or Russian army, will it be considered as hate speech?" As a result, these activists had begun to self-censor their Instagram posts, carefully considering words

[114] Article 19 (2022), "Iran: Meta Must Overhaul Persian-Language Content Moderation on Instagram," (June 9) <https://www.article19.org/resources/iran-meta-persian-language-content-moderation-instagram/>; Maggie Fick and Paresh Dave (2019), "Facebook's Flood of Languages Leave it Struggling to Monitor Content," *Reuters* (April 23) <https://www.reuters.com/article/us-facebook-languages-insight-idUSKCN1RZ0DW>; Fiona R. Martin and Aim Sinpeng (2021), "Facebook's Failure to Pay Attention to Non-English Languages is Allowing Hate Speech to Flourish," *The Conversation* (July 4) <https://theconversation.com/facebooks-failure-to-pay-attention-to-non-english-languages-is-allowing-hate-speech-to-flourish-163723>.

[115] Quintais, João Pedro, Naomi Appelman, and Ronan Ó Fathaigh (2023), "Using Terms and Conditions to Apply Fundamental Rights to Content Moderation," *German Law Review* 24(5).

and phrasing to avoid triggering the content moderation system or giving a pretext to report their profile.

Respondents stressed the difficulties of getting profiles reactivated once they had been shut down as a consequence of mass reporting. Russian activists compared these platforms to corrupt systems in which inside contacts are needed to obtain some form of redress and accountability. A Poland-based respondent said that, although she had the support of Access Now's Digital Security Helpline,[116] it took three months to develop an effective engagement with Instagram and have her account reinstated. As she described: "There is just a feeling that Instagram is a soulless machine which does not take into account the real needs of activists." An Iranian women's rights defender also felt ignored by Instagram after her number of followers was massively increased with artificial accounts, thereby reducing the visibility of her posts. "You can't establish any communication into the organization. I've sent many messages, mentioned them, but there was no reaction."

As a result of the seemingly arbitrary practices of content moderation and algorithmic decision making, activists experienced uncertainty and anxiety over how to safeguard accounts and their content. The prospect of losing a profile with an outreach and network of contacts built over years was discouraging, especially without any specific customer service contacts within the platform available to assist. Some attempted to get their accounts verified in the hopes it would give them better protection against mass reporting; however, getting the blue checkmark often turned out to be another opaque process in which rejections came without any explanation from the platforms.

5.2 Social Media Platform Policies on Digital Transnational Repression

Based on a review of the community guidelines and policies of X, Facebook, and Instagram, it appears that these companies do not explicitly address digital transnational repression or its gender dimensions.[117] Social media guidelines and policies can, in theory, capture some of the activity that constitutes this practice by addressing issues like bullying and harassment, adult sexual exploitation, inciting violence, hate speech, misinformation, coordinated inauthentic behaviour, doxing, the use of hacked content or other material containing personally identifiable information that could lead to physical harm, and dangerous organizations and individuals.

[116] Access Now (undated), "Digital Security Helpline," <https://www.accessnow.org/help/>.

[117] An exhaustive review of platforms' content moderation policies is beyond the scope of this report. However, the following section highlights some areas of concern with respect to DTR.

However, there is no specific category within these policies that fully captures digital transnational repression. Further, these existing policies come hand-in-hand with a broadly acknowledged failure by social media platforms to enforce them and copious evidence that technology-facilitated gender-based violence, among other harms such as the silencing of human rights defenders, is rampant in these forums.[118] Research points to a multitude of causes. For example, content moderation teams may lack native or fluent speakers of the language or dialect which they moderate.[119] This results in inconsistent enforcement of guidelines, over-removal of non-harmful content, and the under-removal of speech with linguistic variations and coded language, or which requires cultural context to interpret.[120] A lack of sensitivity to regional differences has been recognized as particularly harmful to women in the Global South, as women in the Middle East and Central and South America report higher rates of experiencing and/or witnessing online violence.[121] Demoralized by the lack of follow-up on reported content by social media platforms, many women do not report harmful content, instead blocking the person making the post.[122]

[118] On technology-facilitated gender-based violence on social media platforms, see, for example, Dragiewicz, Molly, Jean Burgess, Ariadna Matamoros-Fernàndez, Michael Salter, Nicolas P. Suzor, Delanie Woodlockm, and Bridget Harris (2018), "Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms," *Feminist Media Studies* 18(4); Barker, Kim and Olga Jurasz (2019), "Online Misogyny: A Challenge for Digital Feminism?," *Journal of International Affairs* 72(2); 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). On the targeting of human rights defenders on social media, see, for example, Kargar, Simin and Adrian Rauchfleisch (2019), "State-Aligned Trolling in Iran and the Double-Edged Affordances of Instagram," *New Media & Society* 21(7); and American Bar Association Center for Human Rights (2019), "Invisible Threats: Mitigating the Risk of Violence from Online Hate Speech Against Human Rights Defenders in Guatemala," <https://www.americanbar.org/content/dam/aba/administrative/human_rights/invisible-threats-guatemala-may-2019.pdf>.

[119] Alice Doyle (2021), "Lost in Translation: How the Facebook Oversight Board's Limited Language Capabilities Undermine Human Rights," *UCI Law International Justice Clinic* <https://ijclinic.law.uci.edu/2021/05/25/lost-in-translation-how-the-facebook-oversight-boards-limited-language-capabilities-undermine-human-rights/>. 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 less than 100 staff members having language capabilities in Arabic, French, Polish, and German. See DSA Transparency Database (2024), "DSA Transparency Report," *Twitter International Unlimited Company (TIUC) and Digital Services Act (DSA)* <https://transparency.twitter.com/dsa-transparency-report.html#/>.

[120] See, for example, Richard Ashby Wilson (2022), "The Anti-Human Rights Machine: Digital Authoritarianism and the Global Assault on Human Rights," *Faculty Articles and Papers* <https://digitalcommons.lib.uconn.edu/cgi/viewcontent.cgi?article=1614&context=law_papers>; Isabel Debre and Fares Akram (2021), "Facebook's Language Gaps Allow Terrorist Content and Hate Speech to Thrive," *PBS News* (October 25) <https://www.pbs.org/newshour/world/facebooks-language-gaps-allow-terrorist-content-and-hate-speech-to-thrive>.

[121] The Economist Intelligence Unit (2021), "Measuring the Prevalence of Online Violence Against Women," (March 1) <https://onlineviolencewomen.eiu.com> (see regional differences in the percentage of women who experience and/or witness online violence: 98% and 91% for the Middle East and Central and South America respectively, as opposed to 76% and 74% for North America and Europe). See also Marc Owen Jones (2021), "State-Aligned Misogynistic Disinformation on Arabic Twitter: The Attempted Silencing of an Al Jazeera Journalist," *Open Information Science* 5(1).

[122] Viktorya Vilk and Kat Lo (2023), "Shouting into the Void: Why Reporting Abuse to Social Media Platforms is so Hard and How to Fix It," *Pen America* (June 29) <https://pen.org/report/shouting-into-the-void/>. Indeed, as Nicolas Suzor et al. note, at page 95, "[m]ost digital media platforms rely primarily on relatively simple systems to moderate content–flagging systems that allow users to identify content

Platform design is another aspect of social media that contributes to digital transnational repression and its gender dimensions.[123] Women's experiences with harmful content and inadequate reporting mechanisms can contribute to the retraumatization and the "responsibilization" of victims (i.e., targets of online abuse "are held accountable for the perpetrator's online behaviour and, consequently, are forced to take ownership of the task of avoiding, preventing, and responding to the abuse perpetrated against them").[124] Platforms lack functions that would enable targets of online harassment to easily report to the platform itself or external authorities.[125] As one researcher summarized:

> In the current techno-social environment, targets of online abuse are required to navigate a complex (and often inaccessible) network of ‘‘solutions" to effectively address their abuse, creating a Frankenstein-type response. To effectively and holistically address the abuse, targets must stitch together a variety of insufficient do-it-yourself responses that rely on the inconsistent support from institutions like the government, the legal system, and social media platforms. They must focus primarily on personal resiliency and resourcefulness and rely on the help of family and friends. In some cases, exasperated by the roadblocks they face, targets of abuse have taken matters into their own hands, with varying degrees of success.[126]

This reliance on personal resourcefulness underlines the wider failure of social media

for review...and a limited set of blocking and filtering tools that help users manage the material they are exposed to. These systems have so far proven to be deeply inadequate to the task of addressing online abuse at any serious scale." See also Suzor, Nicolas, Molly Dragiewicz, Bridget Harris, Rosalie Gillett, Jean Burgess, and Tess Van Geelen (2019), "Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online," *Policy & Internet* 11(1); Crawford, Kate and Tarleton Gillespie (2014), "What Is a Flag for? Social Media Reporting Tools and the Vocabulary of Complaint," *New Media & Society* 18(3); Matias J. Nathan, Amy Johnson, Whitney Erin Boesel, Brian Keegan, Jaclyn Friedman, and Charlie DeTar (2015), "Reporting, Reviewing, and Responding to Harassment on Twitter," *Women, Action, and the Media* <https://arxiv.org/pdf/1505.03359>; and Jessica Vitak, Kalyani Chadha, Linda Steiner, and Zahra Ashktorab (2017), "Identifying Women's Experiences with and Strategies for Mitigating Negative Effects of Online Harassment," *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* <https://doi.org/10.1145/2998181.2998337>.

[123] See, for example, Caroline Are (2020), "How Instagram's Algorithm is Censoring Women and Vulnerable Users but Helping Online Abusers," *Feminist Media Studies* 20(5); Marie Lamensch (2022), "In Saudi Arabia, Digital Repression has a Uniquely Gendered Aspect," *Centre for International Governance Innovation* (August 17) <https://www.cigionline.org/articles/in-saudi-arabia-digital-repression-has-a-uniquely-gendered-aspect/>; Suzor, Nicolas, Molly Dragiewicz, Bridget Harris, Rosalie Gillett, Jean Burgess, and Tess Van Geelen (2019), "Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online," *Policy & Internet* 11(1); and Sarah Myers West (2018), "Censored, Suspended, Shadowbanned: User Interpretations of Content Moderation on Social Media Platforms," *New Media and Society* 20(11).

[124] Due to the barriers and the lack of support from online platforms, targets of digital transnational repression are often forced to block, report, or address the harassment they experience online to avoid gender-based digital transnational repression. This trend is documented in how women respond to online abuse. See, for example, Chandell Gosse (2022), "'Don't Take on the Responsibility of Somebody Else's Fu**ed Up Behavior': Responding to Online Abuse in the Context of Barriers to Support," *Canadian Journal of Law and Technology* 19(1).

[125] Viktorya Vilk and Kat Lo (2023), "Shouting into the Void: Why Reporting Abuse to Social Media Platforms is so Hard and How to Fix It," *Pen America* (June 29) <https://pen.org/report/shouting-into-the-void/>.

[126] Chandell Gosse (2022), "'Don't Take on the Responsibility of Somebody Else's Fu**ed Up Behavior': Responding to Online Abuse in the Context of Barriers to Support," *Canadian Journal of Law and Technology* 19(1) at 252.

platforms.

Further, in-platform reporting mechanisms are leveraged by government and other malicious actors against women human rights defenders to stifle their work, notably through mass reporting campaigns resulting in account and page removal, impersonation with the goal of reporting the activist's real account as "fake," and the incorrect memorialization of human rights defenders' accounts.[127]

Platforms have been seen to comply with government requests that are not compliant with international human rights law, while failing to act upon requests by human rights defenders.[128] For example, while Meta purports its compliance with international human rights principles,[129] the company has previously obeyed government requests by removing content posted by human rights defenders[130] and minority groups.[131] Similarly, X has complied with requests by removing government criticism in India[132] and Turkey.[133] Yet, X has refused to abide by government requests in content moderation intended to make the platform safer for vulnerable communities.[134] Despite the pressure for human content moderation by the E.U.,[135] X laid off half of its workforce in 2022 including teams

[127] See, for example, Viktorya Vilk and Kat Lo (2023), "Shouting into the Void: Why Reporting Abuse to Social Media Platforms is so Hard and How to Fix It," Pen America (June 29) <https://pen.org/report/shouting-into-the-void/>; James Pearson (2021), "Facebook Says It Removes Accounts which Targeted Vietnamese Activists," *Reuters* (December 1) <https://www.reuters.com/technology/facebook-says-it-removes-accounts-which-targeted-vietnamese-activists-2021-12-01/>; Samaya Anjum (2022), "Concerted Attacks Against Bangladeshi Activists on Facebook," *AdVox* (February 8) <https://advox.globalvoices.org/2022/02/08/concerted-attacks-against-bangladeshi-activists-on-facebook>; Yasin Isse (2023), "Somalia: Facebook "Remembering" Activists While Still Alive," *SMEX* (March 3) <https://smex.org/somalia-facebook-remembering-activists-while-still-alive/>.

[128] Mackenzie Common (2023), "Beyond the Usual Suspects: A Taxonomy of Social Media Regulations in Countries with Human Rights Issues," *International Review of Law, Computers & Technology* 37(1); Brian Dooley (2023), "Time to Compel Social Media Companies to Protect HRDS," *Human Rights First* (June 8) <https://humanrightsfirst.org/library/time-to-compel-social-media-companies-to-protect-hrds/>.

[129] Meta (2024), "How We Assess Reports of Content Violating Local Law," *Meta Transparency Center* <https://transparency.fb.com/data/content-restrictions/content-violating-local-law/>.

[130] Dien Luong (2020), "Facebook: Vietnam's Fickle Partner-in-Crime," *The Diplomat* (July 9) <https://thediplomat.com/2020/07/facebook-vietnams-fickle-partner-in-crime/>.

[131] David Greene, Paige Collings, and Christoph Schmon (2022), "Online Platforms Should Stop Partnering with Government Agencies to Remove Content," *Electronic Frontier Foundation* (August 12) <https://www.eff.org/deeplinks/2022/08/online-platforms-should-stop-partnering-government-agencies-remove-content>.

[132] Krutika Pathi and Sheikh Saaliq (2021), "Twitter Suspends More India Accounts Amid Free Speech Debate," *AP News* (February 10) <apnews.com/article/media-social-media-india-7769b9fb470e552f5dee877ac8aaea55>.

[133] Megan Cerullo (2023), "Twitter Under Fire for Restricting Content Before Turkish Presidential Election," *CBS News* (May 16) <https://www.cbsnews.com/news/twitter-censoring-content-recep-tayyip-erdogan-turkish-presidential-election/>.

[134] Aljazeera (2023), "Australia Gives Twitter 28 Days to Sort Out 'Toxicity and Hate,'" (June 22) <https://www.aljazeera.com/economy/2023/6/22/australia-gives-twitter-28-days-to-sort-out-toxicity-and-hate>.

[135] Reuters (2023), "EU Tells Elon Musk to Hire More Staff to Moderate Twitter - FT," (March 7) <https://www.reuters.com/technology/eu-tells-elon-musk-hire-more-staff-moderate-twitter-ft-2023-03-07/>.

responsible for content curation, communications, human rights, and machine learning ethics.[136] Similarly, Meta has made severe cuts to teams working in trust and safety issues dedicated to misinformation and foreign influence campaigns in an effort to downsize across Facebook, Instagram and Whatsapp.[137]

While platforms have in the past refused to yield to government requests citing human rights concerns,[138] this trend appears to be acquiescing to censorship demands in exchange for market access at the expense of freedom of expression.[139] Platforms have been placing government-affiliated individuals in decision-making positions[140] and employees of social media companies have been known to be bribed to gain insider access.[141] Finally, upon legal request and review, both X and Meta share certain data with governments, or, in an emergency context, when required to avoid imminent harm.[142] Over-compliance with such requests and without proper consideration for the practice of digital transnational repression can lead to further harm.[143]

5.3 Insufficient Responses by Social Media Platforms

[136] Sheila Dang, Katie Paul, and Paresh Dave (2022), "Twitter Lays Off Staff, Musk Blames Activists for Ad Revenue Drop," *Reuters* (November 4) <https://www.reuters.com/technology/twitter-start-layoffs-friday-morning-internal-email-2022-11-04/>.

[137] Hayden Field and Jonathan Vanian (2023), "Tech Layoffs Ravage the Teams That Fight Online Misinformation and Hate Speech," *CNBC* (May 26) <https://www.cnbc.com/2023/05/26/tech-companies-are-laying-off-their-ethics-and-safety-teams-.html>.

[138] For example, WhatsApp, which belongs to Meta, stopped fielding Hong Kong government requests for content removal following the enactment of the National Security law. See, for example, Selina Cheng (2021), "Facebook Refused All 202 Hong Kong Gov't User Data Requests Since Onset of Security Law," *Hong Kong Free Press* (June 8) <https://hongkongfp.com/2021/06/08/facebook-refused-all-202-hong-kong-govt-user-data-requests-since-onset-of-security-law/?fbclid=IwAR207gJ8IY09ii0yVThA_pBxL10RYStbTXvV3BcIs4l7Upegw523OTBc10w>.

[139] See, for example, Josh Taylor (2023), "Twitter Accused of Responding 'To Tyrants Quickly' but Ignoring Australian Government," *The Guardian* (May 25) <https://www.theguardian.com/technology/2023/may/25/australias-esafety-commissioner-criticises-twitters-inconsistent-response-to-government-requests>; Jeb Su (2019), "Confirmed: Google Terminated Project Dragonfly, Its Censored Chinese Search Engine," *Forbes* (July 19) <https://www.forbes.com/sites/jeanbaptiste/2019/07/19/confirmed-google-terminated-project-dragonfly-its-censored-chinese-search-engine/>.

[140] See, for example, Isabel Debre and Fares Akram (2021), "Facebook's Language Gaps Allow Terrorist Content and Hate Speech to Thrive," *PBS News* (October 25) <https://www.pbs.org/newshour/world/facebooks-language-gaps-allow-terrorist-content-and-hate-speech-to-thrive> ("Former Facebook employees also say that various governments exert pressure on the company, threatening regulation and fines. Israel, a lucrative source of advertising revenue for Facebook, is the only country in the Middle East where Facebook operates a national office. Its public policy director previously advised former right-wing Prime Minister Benjamin Netanyahu").

[141] Julian Borger (2022), "Ex-Twitter Employee Found Guilty of Spying on Saudi Dissidents," *The Guardian* (August 10) <https://www.theguardian.com/us-news/2022/aug/09/twitter-saudi-arabia-dissident-spying>.

[142] X Help Center (2024), "Legal Request FAQs," <https://help.twitter.com/en/rules-and-policies/x-legal-faqs>; Meta (2024), "Government Requests for User Data," *Meta Transparency Center* <https://transparency.fb.com/reports/government-data-requests/further-asked-questions>.

[143] Naomi Nix (2023), "Meta to Begin Fresh Layoffs, Cutting Heavily Among Business Staff," *The Washington Post* (May 23) <https://www.washingtonpost.com/technology/2023/05/23/meta-layoffs-misinformation-facebook-instagram/>.

Our desk review of social media platform policies suggests that these companies have not directed significant attention to the issue of digital transnational repression. While platforms have implemented community guidelines and policies that address certain facets of digital transnational repression (e.g., gender-based violence), they have not succeeded in protecting vulnerable communities and individuals from abuse. This failure is reflected in the observations of research participants that perpetrators of digital transnational repression exploit the technical affordances of these platforms to manipulate crowd- and algorithm-driven news feeds for the viral distribution of harassment and defamation, while online abuse and account take-overs and muting through false mass reports, among other issues, is not detected by the platforms' content moderation tools (particularly outside the context of English-speaking communities). At the same time, participants expressed that platforms remained unreachable and mechanisms for redress were unresponsive.

Section 6: Policy Recommendations

The past few years have been marked by a growing – albeit insufficient – response to transnational repression, including digital transnational repression, from host states. To the extent that host states have enacted some specific policy measures, these positive developments suggest an emerging understanding of the negative impact of transnational repression on human rights, democracy, and rule of law. However, significant work remains to be done. As reviewed in the prior section, host states prioritize strategic, economic, and other interests above human rights. There have been insufficient efforts to address transnational repression in law and policy, particularly from a human-rights perspective. Further, social media companies do not directly address digital transnational repression in community guidelines and policies and are riddled by enforcement issues that suggest greater interest in complying with state demands than in a meaningful collaboration with human rights and civil society organizations on the protection of exile, diaspora, and other vulnerable communities.

Researchers have put forward a series of recommendations to address transnational repression, including its digital dimensions and the proliferation of spyware.[144] These recommendations address various actors in the transnational repression framework, including host states, social media and technology companies, and civil society organizations. Other research gives substantive recommendations on tackling technology-facilitated gender-based violence, equally focusing on the role of governments, social media platforms and civil society in preventing and mitigating the harms of digitally-enabled gender inequality and violence.[145] In this section, we build on these existing recommendations by focusing more specifically on how to begin to address gender-based digital transnational repression, partly drawing on proposals made by research participants.

[144] See, for example, Freedom House (undated), "Policy Recommendations: Transnational Repression," <https://freedomhouse.org/policy-recommendations/transnational-repression>; Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ronald Deibert (2022), "Psychological and Emotional War: Digital Transnational Repression in Canada," *The Citizen Lab* <https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf>; Siena Anstis, Ronald J. Deibert, and John Scott-Railton (2019), "A Proposed Response to the Commercial Surveillance Emergency," *Lawfare* <https://www.lawfaremedia.org/article/proposed-response-commercial-surveillance-emergency>; Noura Aljizawi, Gözde Böcü, and Nicola Lawford (2024), "Enhancing Cybersecurity Resilience for Transnational Dissidents," *Center for Long Term Cybersecurity* <https://cltc.berkeley.edu/publication/cyber-resilience-for-transnational-dissidents/>.

[145] Cynthia Khoo (2021), "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence," *Women's Legal Education and Action Fund* <https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf>; Suzor, Nicolas, Molly Dragiewicz, Bridget A. Harris, Rosalie Gillett, Jean Burgess, and Tess Van Geelen (2018), "Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online," *Policy & Internet* 11(1).

6.1 Host States

Women human rights defenders targeted through gender-based digital transnational repression have repeatedly emphasized the lack of resources and support from host states in the face of transnational repression and gender-based digital transnational repression. Their experiences are particularly marked by social isolation and a lack of institutional or individual support to mitigate the negative effects of this practice. Host state responses so far have often lacked an understanding of the complex social and political context in which gender-based digital transnational repression takes place and the specific vulnerabilities that arise from intersecting identities that engage issues of race, gender, ethnicity, immigration status, and activism. With this background in mind, host states must take the following measures to address gender-based digital transnational repression.

- Explicitly distinguish transnational repression and its digital dimensions from foreign interference and, in any policy enacted going forward, specifically recognize and respond to the distinct gendered harms experienced by women human rights defenders in exile or in the diaspora, in particular as targets of this rights-violating practice.
- Ensure that government agencies adopt a “whole-of-government” approach to addressing gender-based digital transnational repression to ensure that all relevant agencies and institutions are coordinated in their responses and provide consistent and coherent information and reporting channels.
- Provide easily accessible and safe reporting mechanisms, designed to respect and protect user privacy, for women human rights defenders living in exile or in the diaspora to raise concerns about digital transnational repression or other forms of transnational repression with relevant government agencies.
- Proactively consult with civil society and relevant public sector institutions and agencies to ensure the adequate sharing of information with affected exiled and diaspora communities regarding government responses to gender-based digital transnational repression.
- Provide financial and other necessary support for community initiatives aimed at addressing gender-based digital transnational repression, such as:
    - ensuring easily accessible group and individual counselling services to exiled and diaspora women human rights defenders;
    - developing community support groups for exiled and diaspora women human rights defenders and opportunities for peer-to-peer learning; and
    - providing regular and tailored digital training, through local organizations, for exiled and diaspora women human rights defenders who are experiencing gender-based transnational repression.

- Ensure that relevant institutions and agencies, such as law enforcement and intelligence bodies, receive specific training on gender-based digital transnational repression and on immigration and legal-status related issues to ensure that appropriate support is provided to those who are targeted.
- Facilitate access to justice for targets of gender-based digital transnational repression by, among other measures, amending state immunity laws to allow civil litigation by victims to proceed against state perpetrators of transnational repression.

6.2 Social Media Platforms

As our research on gender-based digital transnational repression has revealed, social media companies are key players in the practice of transnational repression as platforms like X, Instagram, and Facebook are sites where gender-based digital transnational repression takes place. Our review of social media policies and guidelines among a small set of platforms shows that there is little to no specific awareness of digital transnational repression (or gender-based digital transnational repression). Social media platforms need to take the following measures to begin to address gender-based digital transnational repression.

- Recognize the problem of digital transnational repression and enact and enforce community policies and guidelines to specifically address it, including its gender-dimensions.
- Work closely with civil society organizations that support women human rights defenders in the diaspora or in exile to mitigate gender-based digital transnational repression by developing and sharing tailored digital security advice and tools, in consultation with such organizations.
- Develop accessible, trauma-informed public reporting channels specifically for gender-based digital transnational repression that mitigate re-traumatization and provide human-based support, ensuring that these incidents are quickly and appropriately identified and addressed.
- Research and publish on the commercial surveillance technology industry,[146] transparently report on digital threats originating from state actors, and make such underlying data and related information available to independent researchers who are studying the surveillance-for-hire industry.
- Invest sufficient resources into understanding and mitigating how foreign states weaponize gender as part of online harassment and disinformation campaigns

[146] Mike Dvilyanski, Margarita Franklin, and David Agranovich (2022), "Threat Report on the Surveillance-for-Hire Industry," *Meta* (December 15) <https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf>.

targeted at women human rights defenders in the diaspora and in exile. In particular, this means hiring employees who speak languages fluently from countries in the Middle East, Latin America, Asia, and Africa and who have an advanced social, cultural, and political understanding of different countries from these regions.

6.3 Civil Society Organizations

Civil society organizations that work with women human rights defenders in exile or in the diaspora are also key actors in the response to transnational repression. Civil society organizations should work to provide the following resources.

- Produce briefs to government agencies working on gender-based digital transnational repression with information regarding the types of interventions that are helpful to community members and the support required.
- Facilitate and nurture support networks for women in exile or in the diaspora that address the compounded vulnerabilities of exiled and diaspora women human rights defenders – several respondents noted that feelings of social isolation were alleviated by understanding that others were experiencing the same threats and impacts.
- Deliver, fund, or facilitate counselling services to women human rights defenders in exile or in the diaspora as concerns regarding psychological and physical health in the face of gender-based digital transnational repression were reported by several respondents.
- Include components focused on gender-based and intersectional risks in general digital security training and education material as respondents noted that while some had taken digital security courses, gender was not a key focus in these trainings.
- Provide information, legal support, and counsel to women activists in exile or in the diaspora who decide to report targeting to law enforcement or other host state institutions.

Conclusion

Through the voices and experiences of 85 interview respondents, this report has shown that digital transnational repression against women human rights defenders in the diaspora and in exile is aggravated by a gendered dimension as attacks exploit and weaponize the fact that targets are women.

Authoritarian governments draw on patriarchal norms and gender hierarchies to extend and amplify their threats against critics and opponents outside their borders. By relying on invasive surveillance, online harassment, sexualized threats, abuse, and defamation, authoritarian regimes fuel hostility against outspoken and politically engaged women in exile and in the diaspora. As a result, women human rights defenders in exile and in the diaspora face attacks not only from regime actors, but also a broader range of aggressors, including government loyalists and even other diaspora or opposition members, who share the same chauvinist ideas and behaviour. Misogyny thus becomes a powerful tool to silence and punish women who criticize and demand accountability from the government in their country of origin. Gendered attacks aim to push women out of public space and inhibit their social and political participation. Further, our interviews reveal that these attacks build not only on the gender and sexuality of targets, but also other characteristics of their intersecting identities – such as their race, ethnicity, religion, disability, or socio-economic class – exacerbating their vulnerability to state-backed repression as well as to racism, xenophobia, misogyny and other forms of discrimination in their broader host society.

As a consequence of gender-based threats and attacks, research participants described a series of negative impacts including stress, anxiety, and other harms to their mental wellbeing. They also experienced limitations on their ability to engage in professional and activism work, self-censorship, withdrawal from activism, and social isolation. Despite these overwhelming challenges, the resilience and agency of the women we interviewed in the face of a constant onslaught of digital threats and violence cannot be overstated. Many of them continued their activism work and developed innovative tactics to resist the multifaceted forms of gender-based digital transnational repression. They mobilized significant resources (emotional, social, financial, and professional) to mitigate and cope with the attacks and to protect themselves, their colleagues, and their families.

The demands of such harm-preventing labour were further exacerbated by the lack of protection and support from host states or social media platforms. The host state has a crucial role to play in preventing these attacks. Yet, as we observed in our interviews, host states have failed to take on this role. Usually viewed as safe havens for political exiles, host states continue to lack adequate mechanisms to protect exiled women human rights defenders from digital transnational repression. Furthermore, at times they appear to be influenced by the attacks that authoritarian regimes carry out on exiled activists within the borders of the host state and end up contributing to or facilitating the repression.

From these findings, we bring forward two central conclusions. First, gender-based digital transnational repression strikes at the core human rights of women human rights defenders in exile or in the diaspora by creating an environment of hostility and insecurity. In doing so, it impedes their ability to live, speak, and associate freely and securely as women human rights defenders or journalists without having to fear repercussions from the states and other power holders they criticize. Second, protecting against gender-based digital transnational repression requires the concerted efforts of various stakeholders to counter the hostility, abuse, and attacks against these women which thrive in the current digital environment, allowing authoritarian regimes to silence demands for accountability, justice, and equality, both at home and abroad.

Tackling gender-based digital transnational repression will require not only specific, tailored action as we have recommended above, but also systemic change. It arises in a broader socio-technical environment in which technology-facilitated gender-based violence is prevalent and where states and non-state actors can easily leverage and exploit existing patriarchy, sexism, and misogyny to silence critics who challenge their hold on power. In the absence of functional regulation and protection for women human rights defenders in exile or in the diaspora, the contemporary online environment – which is defined by the business practices of social media platforms and actors like the mercenary spyware industry that facilitates surveillance and targeting of human rights defenders – is a welcoming environment for this practice. Further, host states, while subject to an obligation to protect human rights, have designed exclusionary immigration systems that can leave individuals like the research participants in this study uncertain about their residence status and vulnerable to deportation or extradition. This environment is amplified by rising anti-migrant rhetoric and sentiment in many host countries.

While acknowledging that gender-based digital transnational repression is a multi-faceted and complex problem, our review of host states responses (to gender-based and more general transnational repression) highlights a failure by states to act and fulfill their obligation to protect against such human rights violations. We also note that, in our review of social media platforms, there has been no specific action to protect against gender-based digital transnational repression by these companies. Already, women experiencing technology-facilitated gender-based violence on such platforms are left on their own "to navigate a complex – and often inaccessible – network of 'solutions.'"[147] Our findings indicate that host states and social media platforms have an urgent obligation to protect exiled and diaspora women human rights defenders from gender-based digital transnational repression (and transnational repression more generally) and to be conscious of and specifically address the gender-dimensions of this practice.

[147] Chandell Gosse (2022), "'Don't Take on the Responsibility of Somebody Else's Fu**ed Up Behavior': Responding to Online Abuse in the Context of Barriers to Support," *Canadian Journal of Law and Technology* 19(1) at 252.