

MAY 2026

---

# Digital Transnational Repression of Uyghurs

## The Costs of Dissent Beyond Borders

REYHAN TOPAL

---



UTJD

OTF

## TABLE OF CONTENTS

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| <b>ACKNOWLEDGMENTS</b> .....                                            | <b>2</b>  |
| <b>ABOUT THE AUTHOR</b> .....                                           | <b>2</b>  |
| <b>GLOSSARY OF TECHNICAL TERMS</b> .....                                | <b>3</b>  |
| <b>INTRODUCTION</b> .....                                               | <b>6</b>  |
| <b>DIGITAL TRANSNATIONAL REPRESSION</b> .....                           | <b>9</b>  |
| <b>METHODOLOGY</b> .....                                                | <b>15</b> |
| <b>ANALYSIS</b> .....                                                   | <b>18</b> |
| THE ROLE OF HOST STATES .....                                           | 18        |
| STATE-STATE DYNAMICS OF DIGITAL TRANSNATIONAL REPRESSION.....           | 24        |
| TECHNICAL MECHANISM OF DIGITAL TRANSNATIONAL REPRESSION .....           | 28        |
| <i>Email Flooding Attacks and Repeated Silent Calls</i> .....           | 29        |
| <i>Account Takeover Attacks</i> .....                                   | 31        |
| <i>Deepfakes</i> .....                                                  | 32        |
| <i>Email Impersonation Attacks</i> .....                                | 33        |
| <i>Digital Intimidation by Chinese Police</i> .....                     | 34        |
| <i>Account Suspension and Content Removal</i> .....                     | 35        |
| <i>State-Coerced Intra-Community Surveillance</i> .....                 | 36        |
| <i>Hacking</i> .....                                                    | 37        |
| <b>KEY FINDINGS</b> .....                                               | <b>39</b> |
| RELUCTANCE TO REPORT INCIDENTS TO LOCAL AUTHORITIES .....               | 39        |
| STRUCTURAL BARRIERS LIMITING POLICE AND GOVERNMENT RESPONSE .....       | 39        |
| POLICE RESPONSES REINFORCE HARM RATHER THAN PROVIDING PROTECTION .....  | 39        |
| INEFFECTIVE RESPONSE MEANS MORE INCIDENTS .....                         | 40        |
| UYGHURS FACE DIGITAL REPRESSION CONCURRENTLY WITH PSYCHOLOGICAL HARM .. | 40        |
| UYGHURS TAKE ACTION AND SUPPORT HOST COUNTRIES WHEN NECESSARY .....     | 40        |
| THERE IS PROGRESS, THOUGH SLOW .....                                    | 41        |
| <b>CONCLUSION</b> .....                                                 | <b>42</b> |
| <b>RECOMMENDATIONS FOR FUTURE RESEARCH</b> .....                        | <b>44</b> |

## **ACKNOWLEDGMENTS**

This project was generously supported by the Open Technology Fund (OTF) through its Information Controls Fellowship Program, which is designed to support research on digital repression methods. I would like to thank the OTF family for their kind assistance, encouragement, and helpful conversations throughout the application process and the course of the project.

I thank the Uyghur Transitional Justice Database (UTJD) for voluntarily serving as my host organization, connecting me with the Uyghur communities worldwide, and generously offering their time and support during my research.

I would like to extend my sincere thanks to the participants in my research for speaking up, sharing their experiences, and standing up for the digital rights of Uyghurs despite all the pressure and intimidation they face. I hope this project serves as a channel for their voices to be heard.

## **ABOUT THE AUTHOR**

Reyhan Topal is an Assistant Professor of Political Science at Augusta University, where she teaches courses for the PhD program in Intelligence, Defense, and Cybersecurity Policy. Her research interests include digital surveillance and control, authoritarianism, civil resistance, and political violence. She holds a PhD in Political Science from the Rockefeller College of Public Affairs & Policy at the University at Albany, State University of New York (SUNY). She has over ten years of experience as an instructor, project manager, data consultant, editor, and researcher for academic and nonacademic institutions.

## **GLOSSARY OF TECHNICAL TERMS**

**Account suspension:** Temporary or permanent restriction of a user's access to their online accounts due to actual or alleged policy violations.

**Account takeover (ATO):** A form of identity fraud in which an unauthorized third party gains access to a user's account.

**Anonymous:** Not named, defined, or identified. The term is used to describe online identities whose owner or creator is unknown, such as anonymous social media accounts.

**Artificial Intelligence (AI):** Advanced technology that enables computers to perform complex tasks by simulating learning, creating, and human reasoning.

**Cloud storage:** A type of computing service that allows users to store and manage their data securely over the internet.

**Cyberattack:** Any malicious activities by hackers (independent or state-sponsored) to gain unauthorized access, damage, or destroy computer networks.

**Cyberbullying:** The consistent and deliberate use of cyber tools to inflict harm on others in different ways, including targeting, intimidation, and humiliation.

**Cyberstalking:** The persistent and unwanted use of digital tools to track the online behavior of others, often with the intent to cause fear and harm.

**Deepfake:** Visual or audio content that appears real but has been digitally manipulated or entirely generated using artificial intelligence.

**Denial-of-service (DoS) attack:** An attempt to make a digital resource (such as a server or website) unavailable by overwhelming it with excessive traffic or requests, preventing legitimate users from accessing it.

**Deplatforming:** The banning of individuals or groups from an online platform, typically for violating the platform's policies.

Email flooding attack: Also called email bombing and email bombardment attack. A type of denial-of-service attack during which an attacker or scammer (independent or state-sponsored) floods targeted email address(es) with an extreme volume of emails.

Email impersonation attack: A deceptive tactic in which cybercriminals pretend to be a trusted individual or organization to mislead users and cause harm through email communication.

End-to-end encryption (E2EE): A secure communication system that ensures messages can only be accessed by the sender and the recipient.

Hacking: The act of using illicit tools to gain unauthorized access to a digital device, network, or system.

Malware: Short for *malicious software*. Software designed to exploit or harm a computer, network, or data.

Phishing: A type of social engineering attack that deceives users through emails, text messages, or other online channels to steal their sensitive information and material possessions.

Spyware: Short for *spying software*. A form of malware that is secretly installed on a device to gather user information and share it with third parties.

Technological surveillance: The use of technological tools to monitor and collect data on individuals.

The Onion Router (Tor): A free and open-source privacy network that enables anonymous online communication by directing traffic through multiple servers.

Two-factor authentication (2FA): A security method that requires users to complete two steps of verification to confirm their identity and access their data, making it more difficult for unauthorized parties to gain access to the account.

Virtual Private Network (VPN): A tool that establishes a secure connection between a device and a network by encrypting internet traffic and masking the user's IP address.

## INTRODUCTION

On October 2, 2018, Jamal Khashoggi, a Saudi journalist and outspoken critic of the Saudi government, entered the Saudi consulate in Türkiye and never returned. The assassination of Khashoggi by the Saudi government had a significant technological component behind it. It was reported that the phones of Khashoggi, his fiancée, and one of his close associates, Omar Abdulaziz, were infected with Pegasus spyware created by the Israel-based NSO Group. Using Pegasus, the Saudi government could track Khashoggi's WhatsApp chats and obtain prior information about his appointment at the consulate, which made it possible to organize Khashoggi's assassination. This marked the first case of digital transnational repression that resulted in the death of a person in another country for his political stance against their government.

Following this alarming incident, the concept of digital transnational repression, which refers to digital tools and strategies that governments employ to surveil, control, and silence dissidents among diasporas or exiles, has increasingly garnered scholarly attention. However, despite growing interest in the concept, the number of studies on digital transnational repression is still small. In this project, I aim to fill this gap by proposing a comprehensive agenda to address rising digital transnational repression politically, legally, and technically, and to enable journalists, activists, or anyone to speak up freely. To this end, I draw evidence from my in-depth interviews with Uyghur activists who have been targeted by China's digital transnational repression acts in different countries.

This project has four main goals. First, I thoroughly analyze how digital transnational repression is implemented. Our current knowledge of digital transnational repression revolves mostly around state-led surveillance, spyware, server espionage, and similar targeted attacks against critics of governments in general. However, such repression also manifests as the intimidation of dissidents abroad that results in self-censorship, phishing through fake interview requests, and threatening family members of dissidents abroad for sharing undesirable social media content. Therefore, my goal is to broaden the scope of our current knowledge by uncovering the

hidden aspects of digital transnational repression, in addition to further exploring the widely known strategies.

Second, I examine whether current political and legal frameworks effectively combat digital transnational repression. Although this form of repression has become prevalent in recent years, states still lack a comprehensive political or legal agenda to address it. While existing studies discuss the obligation of host states to protect communities against human rights violations through digital tools, we need better national and international laws and policies to minimize the risk of digital transnational repression and protect the security and privacy of users targeted by their governments. Therefore, I propose recommendations for policymakers to deal effectively with digital transnational repression.

Third, I explore the technical aspect of digital transnational repression. To that end, I analyze each of the following methods employed by China to digitally oppress Uyghur activists abroad: email flooding attacks and repeated silent calls, account takeovers, deepfakes, email impersonation attacks, digital intimidation by Chinese police, digital intimidation by pro-China actors, account suspension, state-coerced intra-community surveillance, and hacking. Drawing insights from my interviews with Uyghur activists who have been targets of digital transnational repression, I map all of these repressive digital methods in detail. Using this map, I aim to develop concrete digital solutions to the existing threats.

Fourth, I develop a set of practical recommendations for researchers, policymakers, and legal practitioners to counter digital transnational repression. Although activists abroad try to find alternative ways to mitigate digital repression, those approaches do not always render them immune to its risks. For example, the use of a VPN or Tor—a very common safeguard—may protect the privacy of users while also generating vulnerabilities. Therefore, it is of utmost importance for researchers to adopt a broader approach and for policymakers and legal practitioners to redesign current policy and legal frameworks to effectively combat this threat.



In conclusion, with this project, I address the urgent need for effective strategies to combat digital transnational repression, which poses a serious threat to human rights worldwide. By combining political, legal, and technical approaches, I generate practical and feasible solutions to counter this dangerous form of repression.

## DIGITAL TRANSNATIONAL REPRESSION

Researchers in the state repression field primarily focus on the strategies governments use to manage domestic dissent and the methods individuals adopt to resist these strategies. With the growing prevalence of new digital tools over the last two decades, researchers have begun investigating how new technologies alter the longstanding contention between state repression and civil resistance. Digital transnational repression is a relatively new concept that has emerged in this growing body of research. What makes it unique and intrusive is that states now oppress antigovernment activists, scholars, and journalists, even when they are abroad, by employing digital means. Therefore, dissidents become intimidated and avoid sharing information about their experiences.

While researchers endeavor to contextualize digital transnational repression within their debates, in Table 1 I present a glimpse of how research on this subject has evolved over the past decade.<sup>1</sup> One of my main observations is that the field has been driven by the research of a small community of scholars, including Marcus Michaelsen and Siena Anstis, who have meticulously examined the social, political, and emotional aspects of digital transnational repression. Although this form of repression was not conceptualized when these authors were conducting their research prior to 2020, the scholars focused on diaspora activism, extraterritorial authoritarian practices, and digital monitoring against activists.

With the growing interest in the subject, we now have a tight but rapidly expanding cluster of scholars and practitioners who produce academic publications and research reports on this topic.

---

<sup>1</sup> My regularly updated digital transnational repression reading list can be accessed through the publicly available Zotero library that I created as part of this project: [https://www.zotero.org/groups/5747407/digital\\_transnational\\_repression/library](https://www.zotero.org/groups/5747407/digital_transnational_repression/library).

**Table 1. The State of the Field on Digital Transnational Repression in the Last Decade**

| Item Type       | Year | Author                                                                                                                                                                                                                                                                                                                        | Title                                                                                                                                     |
|-----------------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Journal Article | 2025 | Michaelsen, Marcus; and Anstis, Siena                                                                                                                                                                                                                                                                                         | Gender-Based Digital Transnational Repression and the Authoritarian Targeting of Women in the Diaspora                                    |
| Journal Article | 2025 | Garbe, Lisa; Maerz, Seraphine F.; Freyburg, Tina                                                                                                                                                                                                                                                                              | Authoritarian Collaboration and Repression in the Digital Age: Balancing Foreign Direct Investment and Control in Internet Infrastructure |
| Book            | 2025 | Oztig, Lacin Idil; Celil Karluk, Abdurresit                                                                                                                                                                                                                                                                                   | China's High-Tech Repression Against Uyghurs: Novel Theoretical Insights                                                                  |
| Journal Article | 2024 | Oztig, Lacin Idil; Karluk, Abdurresit Celil                                                                                                                                                                                                                                                                                   | The Impact of China's High-Tech Repression on Uyghurs: A Case Study of Uyghur Diaspora in Turkiye                                         |
| Report          | 2024 | Aljizawi, Noura; Anstis, Siena; Michaelsen, Marcus; Arroyo, Veronica; Baran, Shaila; Bikbulatova, Maria; Böcü, Gözde; Franco, Camila; Geybulla, Arzu; Iliqud, Muetter; Lawford, Nicola; LaFlèche, Émilie; Lim, Gabrielle; Meletti, Levi; Mirza, Maryam; Panday, Zoe; Posno, Claire; Reichert, Zoë; Taye, Berhan; Yang, Angela | No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression                                               |
| Journal Article | 2024 | Oztig, Lacin Idil; Karluk, Abdurresit Celil                                                                                                                                                                                                                                                                                   | Theorizing the Spatiality of ICT-Mediated Transnational Repression: Evidence from China's Repression of Uyghurs in Turkiye                |
| Journal Article | 2024 | Conduit, Dara                                                                                                                                                                                                                                                                                                                 | Digital Authoritarianism and the Devolution of Authoritarian Rule: Examining Syria's Patriotic Hackers                                    |

|                 |      |                                                                                                                    |                                                                                                       |
|-----------------|------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Journal Article | 2024 | Uluyol, Yalkun                                                                                                     | China's Transnational Repression Against Uyghurs                                                      |
| Book Section    | 2024 | Michaelsen, Marcus                                                                                                 | Nowhere to Hide: Digital Transnational Repression Against Exiled Activists from the Middle East       |
| Journal Article | 2024 | Anstis, Siena; LaFlèche, Émilie                                                                                    | Gender-Based Digital Transnational Repression as a Global Authoritarian Practice                      |
| Journal Article | 2024 | Michaelsen, Marcus; Ruijgrok, Kris                                                                                 | Autocracy's Long Reach: Explaining Host Country Influences on Transnational Repression                |
| Journal Article | 2023 | Lemon, Edward; Jardine, Bradley; Hall, Natalie                                                                     | Globalizing Minority Persecution: China's Transnational Repression of the Uyghurs                     |
| Journal Article | 2023 | Michaelsen, Marcus; Thumfart, Johannes                                                                             | Drawing a Line: Digital Transnational Repression Against Political Exiles and Host State Sovereignty  |
| Blog Post       | 2022 | Al-Jizawi, Noura; Anstis, Siena                                                                                    | The Effects of Digital Transnational Repression and the Responsibility of Host States                 |
| Report          | 2022 | Al-Jizawi, Noura; Anstis, Siena; Barnett, Sophie; Chan, Sharly; Leonard, Niamh; Senft, Adam; Deibert, Ron          | Psychological and Emotional War: Digital Transnational Repression in Canada                           |
| Journal Article | 2022 | Moss, Dana M.; Michaelsen, Marcus; Kennedy, Gillian                                                                | Going After the Family: Transnational Repression and the Proxy Punishment of Middle Eastern Diasporas |
| Journal Article | 2022 | Dukalskis, Alexander; Furstenberg, Saipira; Gorokhovskaia, Yana; Heathershaw, John; Lemon, Edward; Schenkkan, Nate | Transnational Repression: Data Advances, Comparisons, and Challenges                                  |
| Journal Article | 2022 | Anstis, Siena; Barnett, Sophie                                                                                     | Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses   |

|                 |      |                                                                                                 |                                                                                                                         |
|-----------------|------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Journal Article | 2021 | Furstenberg, Saipira; Lemon, Edward; Heathershaw, John                                          | Spatialising State Practices Through Transnational Repression                                                           |
| Report          | 2021 | Schenkkan, Nate; Linzer, Isabel                                                                 | Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression                                  |
| Book Section    | 2021 | Fatafta, Marwa                                                                                  | Transnational Digital Repression in the MENA Region                                                                     |
| Report          | 2021 | Al-Jizawi, Noura; Anstis, Siena; Barnett, Sophie; Chan, Sharly; Senft, Adam; Deibert, Ronald J. | Annotated Bibliography: Digital Transnational Repression                                                                |
| Report          | 2020 | Michaelsen, Marcus                                                                              | The Digital Transnational Repression Toolkit, and Its Silencing Effects                                                 |
| Journal Article | 2018 | Moss, Dana M.                                                                                   | The Ties that Bind: Internet Communication Technologies, Networked Authoritarianism, and 'Voice' in the Syrian Diaspora |
| Journal Article | 2018 | Michaelsen, Marcus                                                                              | Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State                                    |
| Journal Article | 2018 | Glasius, Marlies                                                                                | Extraterritorial Authoritarian Practices: A Framework                                                                   |
| Journal Article | 2017 | Michaelsen, Marcus                                                                              | Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran                      |

Around the years 2020–2022, the term digital transnational repression became more explicit. Consequently, researchers scrutinized some of the digital tools that states employ to oppress activists abroad and how those strategies have a silencing impact on the activists, exiled people, and diaspora communities. While Michaelsen described the digital transnational repression toolkit, others applied the term to regional and global contexts. Those years were also important in terms of the production of academic research on legal and ethical aspects of the topic. Yet, the activists of the Middle East and North Africa remained the primary cases studied.

From 2023 onward, the field diversified with the inclusion of new cases, such as China's digital transnational repression against Uyghurs, and new aspects, including gender. However, the field has several gaps that I aim to fill in my project.

The first gap is that the field lacks a broad and integrative agenda to discuss the concept of digital transnational repression. The number of interdisciplinary studies on this topic is very small, and existing studies concentrate on legal, political, and technical aspects of the debate. However, each scrutinizes specific elements of the concept; therefore, we still do not have an inclusive agenda for debating digital transnational repression. For example, Freedom House's recent report presents a fruitful debate pertaining to transnational repression, including tactics used and host states' responsibility to protect migrants from this specific type of repression. Like most studies on transnational repression, this report does not provide a complete picture of how states employ digital tools to oppress dissidents abroad. The report lists only two common digital tactics: spyware and digital threats; therefore, its technological aspect is limited in scope. I encounter this gap in studies of transnational repression across the social sciences literature, as political and legal perspectives of the debate prevail over the technical aspect. In this report, I complement the existing policy- and legal-oriented research by integrating a technical layer into the transnational repression debate. To this effect, I open the digital toolbox of the Chinese regime and thoroughly analyze all digital tactics, including email flooding attacks and repeated silent calls, account takeovers, deepfakes, email impersonation attacks, digital intimidation by Chinese police, digital intimidation by pro-China actors, account suspension, state-coerced intra-community surveillance, and hacking. This effort is vital because we cannot develop concrete solutions to digital transnational repression without fully understanding how governments implement it.

The second notable gap within the current field of research is the limited discussion among scholars regarding the collaboration between states in the realm of digital transnational repression. This aspect remains unexplored, with insufficient attention dedicated to understanding the dynamics and implications of state-state collaborations in perpetuating digital repression

across borders. Therefore, I address this gap by analyzing the complex interplay between states within the context of digital transnational repression.

The third gap in the field is the lack of research that may connect the academic aspect of the debate to policymaking or lawmaking. Although researchers underscore that digital transnational repression silences opposition actors and violates freedom of speech and expression, they have not yet proposed an agenda-making policy or legal suggestions about how to counter it. In this report, I offer detailed suggestions for policymakers, lawmakers, and researchers. This helps bridge the gap between the research community and political and legal circles.

## METHODOLOGY

This report draws insights from in-depth interviews with 10 Uyghur activists who have been targeted by various forms of digital transnational repression in Germany, Norway, the Netherlands, the United States, and Türkiye. The method of in-depth interviewing is commonly described as a thorough “conversation with purpose.”<sup>2</sup> To that end, my purpose as the interviewer was to design and lead a safe conversation environment in which participants could share in detail their experiences with digital transnational repression. I prepared the questionnaire in a semi-structured format so that I could have the flexibility to use follow-up questions to delve into unique aspects of each participant’s story.

I selected participants in three ways: relying on my personal connections within the Uyghur diaspora; seeking the help of the Uyghur Transitional Justice Database (UTJD), which has access to a network of Uyghur activists worldwide; and using snowball sampling based on the recommendations of participants. The existence of these established relationships—with people I already knew or who were introduced to me by the UTJD or former participants—helped activists share their thoughts and feelings openly in an environment of trust. I conducted the interviews in Turkish and English and, at times, participants referred to specific terms, places, or expressions in the Uyghur language.

In terms of demographics, I paid additional care to choose participants from different age groups, from the early 20s to late 50s, to ensure that I could compare the experiences of Uyghurs who had dealt with traditional forms of repression before social media became widespread with those for whom social media has always been available. My sample included an equal gender distribution, with five female and five male participants from different backgrounds.

---

<sup>2</sup> Rossman, G. B., & Rallis, S. F. (2011). *Learning in the field: An introduction to qualitative research*. Sage Publications; Legard, R., Keegan, J., & Ward, K. (2003). In-depth interviews. In J. Ritchie & J. Lewis (Eds.), *Qualitative research practice: A guide for social science students and researchers* (pp. 138–169). Sage Publications.



As a researcher, I recognize that interviewing individuals in high-risk situations brings about significant responsibilities regarding their safety and privacy. In the case of Uyghurs, there is a risk that any public criticism of China's policies on their part could have severe consequences for their family members and relatives in East Turkistan. Therefore, I removed any details that could reveal their identity from the quotations I collected from the interviews. Although several participants gave me their consent to list their names among the participants, I maintained this confidentiality policy throughout the report for all participants. If any specific details about the occupation, age, or gender of the participants is included in the quotations, it is only because the participants gave their consent to share them.

At the very beginning of each interview, I provided participants with detailed information about myself, my research, the Open Technology Fund, and the use and protection of their data. Then, I asked them to verbally confirm that they understood the provided information and that they consented to participate in my research. I conducted the interviews over three end-to-end encrypted communication platforms. Upon participants' consent, I recorded and stored the interviews on an external device with no internet connection.

Speaking up for their communities by risking themselves and their loved ones, dealing with the insecurities caused by digital transnational repression, and having lost contact with their families in East Turkistan might have created a significant mental and emotional burden for Uyghurs. Drawing from my prior experience in ethnographic research with individuals who struggled with trauma,<sup>3</sup> I adopted a trauma-informed approach in my interviews. Trauma-informed approaches prioritize a research process in which the impact of traumatizing life situations on participants is carefully considered. Accordingly, researchers are expected to promote principles like safety, collaboration, and empowerment.<sup>4</sup> During my interviews, I made every effort

---

<sup>3</sup> In 2015 and 2016, I conducted ethnographic research with the Turkmen community who had fled the Syrian civil war and settled in Türkiye, as well as at an art center attended by women who had experienced domestic violence. During this period, I gained experience in conducting qualitative research with individuals who had undergone trauma.

<sup>4</sup> Sobel, S. (2021). Trauma-informed qualitative research: Some methodological and practical considerations. *International Journal of Mental Health Nursing*, 30, 1456–1469; Harris, M., &

to choose my words carefully to avoid triggering negative feelings, refrained from asking detailed questions about issues that participants found emotionally challenging, and conveyed understanding throughout the conversations.

Finally, after each interview, I asked participants whether they would like to review the quotations from our conversation before the publication of this report. I shared the relevant excerpts with them if they agreed.

---

Fallot, R. D. (2001). Envisioning a trauma-informed service system: A vital paradigm shift. *New Directions for Mental Health Services*, 2001(89), 3–22.

## ANALYSIS

### The Role of Host States

When it comes to the repression of diaspora communities, it is crucial to examine the interactions among various factors related to the direct and indirect roles of host states. To better understand how host countries shape the digital transnational repression of Uyghurs, I asked participants several questions about their contact with authorities when they experienced a digital incident.

When targeted by the acts of digital transnational repression, participants either remained silent and avoided asking for help or reached out to the authorities to report their experience. When I asked participants why they remained silent, they provided two reasons. First, they had a negative experience with authorities in the past in terms of receiving help; therefore, they decided not to ask for help again. Second, they believed that even if they asked for help, they would not receive any response due to the difficulties in addressing transnational repression and holding China accountable for such acts of repression.

When I asked a participant from Germany—who has been stalked, insulted, and threatened by a user to “be found dead in their basement”—if they had ever reported their deeply concerning experience with digital transnational repression to the German police, they said:

*No, never. I was almost certain they would not do anything because the accounts were anonymous. Previously, I met with someone from the European Parliament. Suddenly, a Chinese man walked into the room and said, “Oops, sorry!” It was strange because the room where we were meeting was deep inside the hotel. We had to pass several doors, turn corners, and go through corridors to get there. You cannot just end up there by mistake. After that, we contacted the police. That was the first time I felt someone might be following me. The police did nothing, to my knowledge.*

This explanation is significant in its emphasis on how the lack of a proper response by police to handle an act of digital transnational repression

discourages targeted Uyghurs from asking for help in the future. Additionally, this case reveals that anonymity, a feature of digital transnational repression, makes it difficult and time-consuming to identify the perpetrators. Even when the real identities of the perpetrators are discovered, holding them accountable is a daunting task if they are located abroad. In the face of all these obstacles, Uyghurs feel compelled to remain silent.

My conversation with a participant from Türkiye further confirmed the issue surrounding anonymity and location. People in the participant's social circle had been frequently contacted by the Chinese police via WhatsApp, Telegram, and WeChat, and forced to provide extensive information about themselves. Talking to one of those people who had audio recordings of the calls, the participant offered to go to the police together, but their friend declined because they believed it would lead to no result. The participant also thought that, even if they told the police that someone in China was threatening them, the police would probably have no idea what they were supposed to do about it.

In Türkiye, another participant, whom the Chinese police persistently called from foreign phone numbers registered in various countries, such as Kyrgyzstan, decided to go to the police when they began receiving calls from Turkish operators as well, only to be disappointed by the reaction of the police:

*In 2023, as I kept receiving calls from Turkish numbers, I went to the provincial police department in the city where I lived. When I described the situation, the officer did not even file a report. They listened to my story and then asked, "Which country are you a citizen of?" I said, "China." They replied, "You are living in Türkiye, but we have no proof that you have not committed a crime in China. Did you commit a crime there? Is that why they are still after you?" I was totally disappointed. I did not want to go to the police station again for anything. I do not think Turkish authorities are cooperating with China, but I believe they simply do not care.*

This highly concerning experience between the participant and the police officer indicates that Uyghurs, who have already been targeted by digital transnational repression, become targets once again when authorities

question their innocence instead of focusing on the details of the digital incidents. Although it might be misleading to frame a police officer's biased reaction as an official policy, such a reaction clearly shows that the police were not well-trained in terms of the responsibilities of host states in protecting communities and addressing the cases of digital transnational repression. This leads to three key issues. First, China might expand its digital transnational operations in the country due to the lack of a proper response by Turkish authorities. Second, members of the Uyghur community might lose trust and avoid asking for help from authorities, even when it is urgently needed. Third, and in a related manner, the fact that Uyghurs hesitate to communicate their problems to Turkish authorities makes it difficult for officials to recognize existing digital transnational repression issues and, consequently, delays the development of necessary policy and legal measures.

The same issue also arose in the case of Norway. A participant received phishing emails and dealt with numerous unauthorized login attempts on their Telegram, Signal, Facebook, and Instagram accounts while conducting a project to document China's human rights violations. Despite using two-factor authentication, their Telegram account, through which they exchanged critical information with other activists, was logged into by an unknown person(s). Right after the participant shared their experience with the international community, their personal computer completely broke down. Yet again, when I asked them if they had ever contacted the Norwegian police about any of these issues, they said:

*Not really. I never see my case as a single case. When I was working for a nongovernmental organization advocating for Uyghurs, we had occasional meetings with intelligence agencies. We would report what happened to other people and us in the community, such as calls from the Chinese embassies or intimidation by the Chinese police. We would report these to intelligence agencies, but they honestly did not care. The last time we had a meeting last year [2023], we were talking to them about how serious this issue is, and we were asking them to investigate it. Then, the answer was simple: "We do not have resources." I know reporting to the police would not help. In Europe, I feel like they are not taking the issue seriously and giving enough attention. At least, they could try some ways to deal with it, like talking to the Chinese embassy about the*

*claims, bringing the issue to diplomatic channels, etc. But they did not care. Their response was not satisfactory.*

In the second case, when targeted Uyghurs reached out to the police for help, most of them could not get their problems addressed properly. A participant from the Netherlands, who went to the police three times, described a terrifying incident that had encouraged them to contact the police for the first time:

*We, as the Uyghur community, had a meeting with the American ambassador to the Netherlands during the first Trump administration. After that meeting, while I was on my way home, I got a call from a private number. I said “hello,” but there was only silence. In the background, someone was screaming in Chinese—angrily or maybe in distress. The first thing that came to my mind was, “Is this my father [in East Turkistan]?” After a few seconds, I realized it was not his voice. Then I heard heavy breathing on the phone. I hung up immediately and went to the police station to report it. That was the first big moment when I felt, “This is serious,” and I decided to go to the police.*

After the participant reported the incident to the police and provided all the details, the officers wrote down everything, but the participant could not get any response from them in the following days.<sup>5</sup> When their Instagram account used for raising awareness of the Uyghur issue was hacked, the participant contacted the police for the second time. The third police contact would occur when an Instagram user, who was speaking in Dutch and using Chinese subtitles in their videos, claimed that the participant was associated with the East Turkistan Islamic Movement.<sup>6</sup> The alarming part was that the user also included pictures of the participant taken during a recent protest against China, showing that they had been physically surveilled. They did not receive any response from the police following this incident either. When I asked about

---

<sup>5</sup> The participant provided a copy of the five-page police report, which has been withheld from this report to ensure their safety, since it includes personal details.

<sup>6</sup> The East Turkistan Islamic Movement (ETIM) is a separatist group which the United Nations added to its list of terrorist groups for their likely association with Usama bin Laden and the al-Qaida network in 2002.

the possible reasons behind such silence, the participant addressed the structural problems within the current political and legal frameworks:

*There is a structural problem. We have been constantly told by politicians to report our incidents to the police, but the police do not do anything because, in most cases, they cannot. Dutch law regarding digital transnational repression was very weak. Until last year [2024], I think we did not even have an espionage law.*

Based on their observation, it seems that there is a lack of coordination in terms of addressing transnational repression effectively due to the gaps in the legal system. Victims are encouraged to report incidents to the police, but in many cases, the authorities have limited room to act due to the lack of standards for digital offenses and jurisdictional limits. As a result, digital transnational repression frequently falls between mandates and leaves victims without timely solutions. Building further on this argument, the participant illustrated how the Uyghur diaspora's efforts to counter digital transnational repression were undermined by structural problems:

*In the Netherlands, all Uyghur groups collected incidents of transnational repression, and 50 of those incidents were collectively reported to the police in 2021 or 2022. After several months, we saw a news headline saying that the Dutch police had stopped their investigation because they deemed transnational repression impossible to detect, track, or fully understand. They needed help from the Chinese police, but of course, they could not get it. This created a lot of mistrust within the Uyghur community because the decision was never communicated to us directly. We had to learn about it from the news. So, there was a serious communication problem as well. It destroyed the credibility of the Dutch police and government in ever addressing this issue.*

There are three key takeaways for this example. First, the Uyghur diaspora is willing to cooperate with its host states to effectively mitigate the risks of digital transnational repression. To this end, they meticulously documented the details of the incidents and shared them with the authorities to develop solutions. Second, the complexities regarding the attribution problem inherent to digital transnational repression make it a challenging issue for the police to

address. Third, in the case of the Netherlands, there is a lack of communication between the Dutch police and Uyghurs, evident in the example that Uyghurs learned about the end of the investigation from the media. This might create mistrust toward law enforcement authorities and discourage the Uyghur community from reporting future incidents of transnational repression.

In the absence of a concrete step from the Dutch authorities, the Uyghur diaspora is working to find alternative ways to deal with digital transnational repression. The participant in the Netherlands mentioned that they spoke with the members of the Turkish and Moroccan communities in the country and found out that they had similar experiences. Together, they created an alliance against foreign interference through which they managed to push for the establishment of a hotline. In 2025, for the first time, the Dutch government made this hotline operational to allow people to report incidents of transnational repression through a secure website. This gives us hope that persistent efforts by targeted communities can lead to political change.

The same situation regarding progress and persistent limitations is evident in the case of Germany. A participant shared an incident they experienced with their family and the German police's reaction:

*Chinese intelligence agents contacted my spouse through WhatsApp, saying they wanted to be friends with them. They said, "We know your relatives [in East Turkistan]. If you'd like, we can help you get in touch with them." My spouse hadn't been in contact with anyone for years because all of them had deleted them [my spouse] from WeChat. Agents managed to connect my spouse with some of their elderly relatives, and they all cried while speaking. After a couple of years, when I took a critical role in Uyghur activism, they [the agents] contacted my spouse on WeChat and wanted them to convince me to work for Chinese intelligence, and they would give me money and a house. They told my spouse, "We'll give you a device; just install it on your spouse's computer."*

When the participant's spouse kept receiving phone calls, the couple decided to report the situation to the police. However, the police were uncertain about how to respond. Since the calls originated from outside Germany, they stated that there was little they could do. According to the participant, the situation



has improved since then. The Uyghur community, which has been frequently targeted by digital transnational repression, engaged with the representatives of the German Bundestag<sup>7</sup> and proposed the establishment of a hotline dedicated to reporting incidents of transnational repression. Although the hotline remains in its early stages and lacks full professional capacity, the participant noted that the communication between targeted communities and the German authorities has improved since its creation. The government is now taking incremental steps toward institutionalizing its response to digital transnational repression.

Another participant from Germany further elaborated on this progress:

*We're now in contact with multiple government actors, and there is much greater awareness of the issue. More resources have been allocated to address digital transnational repression, and it has become a significant topic in Germany. Last September [2024], the World Uyghur Congress, together with partner organizations in Germany, launched a coalition against transnational repression. As part of this initiative, several briefings were organized with government officials and members of parliament. Parliamentary representatives have become increasingly engaged with the issue. In December [2024], members of the Uyghur community attended a breakfast meeting in the German Bundestag about transnational repression. Officials from the Ministry of the Interior also participated and informed attendees about forthcoming measures. We now have a hotline dedicated to transnational repression, including digital cases. Both the Ministry of Foreign Affairs and the Ministry of the Interior, along with the police, are working to ensure that awareness and response mechanisms are extended across all levels of government, down to local authorities. Police officers are also receiving training on how to handle incidents of transnational repression.*

### **State-State Dynamics of Digital Transnational Repression**

Putting together all these narratives surrounding the political, legal, and structural problems in addressing digital transnational repression, one may end up questioning whether a host country's relationship with China affects

---

<sup>7</sup> The federal parliament of Germany.

its strategies for addressing such repression. China is an economic partner for the abovementioned host countries. For example, according to preliminary figures from the German statistics office, China became Germany's leading trading partner in the first eight months of 2025, surpassing the United States, which was Germany's top trading partner the year before.<sup>8</sup> Similarly, as for the Netherlands, China is a major actor in bilateral trade, as the largest Asian supplier of goods to the country and the primary destination for Dutch exports headed to South, East, and Southeast Asia.<sup>9</sup> In such situations, it is critical to question whether the dynamics of economic interdependence cause host countries to hesitate to develop strict attitudes toward China's oppression of Uyghurs.

I asked Uyghur activists if they observed any hesitation or, even more, cooperation between their host country and China in terms of their digital repression. In order not to influence the participants, I did not mention that economic or political relations with China might play a role in their governments' policies.

In the case of Germany, all participants agreed that the German government is willing to help Uyghurs in the face of digital transnational repression, although there is still room for improvement. For them, the initiation of a hotline is a sign of the German authorities' dedication to addressing China's digital repression of Uyghurs in Germany. Therefore, they do not observe or sense any hesitation, connivance, or cooperation with China. The participants emphasized that officials have expressed a willingness to help and have promised additional measures, such as training sessions for affected communities. However, they also stressed that greater institutional commitment and dedicated funding are needed for the German government to

---

<sup>8</sup> German imports and exports with China totaled \$190.7 billion (€163.4 billion) between January and August, and \$189 billion (€162.8 billion) with the United States during the same period. Source: Reuters. (2025, October 22). China overtakes the U.S. as Germany's largest trading partner. *Al Jazeera English*. <https://www.aljazeera.com/economy/2025/10/22/china-overtakes-the-us-as-germanys-largest-trading-partner>.

<sup>9</sup> Centraal Bureau voor de Statistiek. (2024). *Trade in goods 2024*. CBS. <https://www.cbs.nl/-/media/pdf/2024/44/dutchtrade2024.pdf>.

develop a more systematic and effective approach to countering transnational repression. For example, one of the participants said:

*The German authorities are willing to help, but they are still not very professional. The German government needs to allocate more funding to eliminate digital transnational repression. They are trying to make the process more systematic. Until now, we have tried to handle everything on our own, but the authorities promised that they would help. They said they would work on it. Therefore, I do not think that they cooperate with China.*

Other participants emphasized the support of the government in additional cases. For example, a participant mentioned that the police have always been supportive during the pro-Uyghur demonstrations, while another talked about the technical support they received from the German police after a cyberattack.

In the case of Norway, participants expressed their skepticism regarding the insufficiency of the authorities in handling the incidents of digital transnational repression. One participant emphasized that economic interests might have played a role in this situation:

*I do not want to say that the Norwegian authorities simply do not care about digital transnational repression, but they do not do anything about it, even though we have been reporting these incidents for a long time. They do not want to understand the issue, or maybe they do not know how to deal with it. There is a gap: when you talk to politicians, they say something that law enforcement agencies are completely unaware of. These actors do not have an information flow. There is a communication problem. The government has economic relations with and interests in China, since oil, fish, and everything depend on the Chinese market. So, this is partially why I believe digital transnational repression is not being addressed effectively.*

Based on this statement, it can be concluded that the participant views structural problems, along with Norway's economic cooperation with China, as the potential reasons behind the country's failure to prevent or address digital transnational repression.

Similar parameters persist in the case of the Netherlands. A participant described the situation in detail:

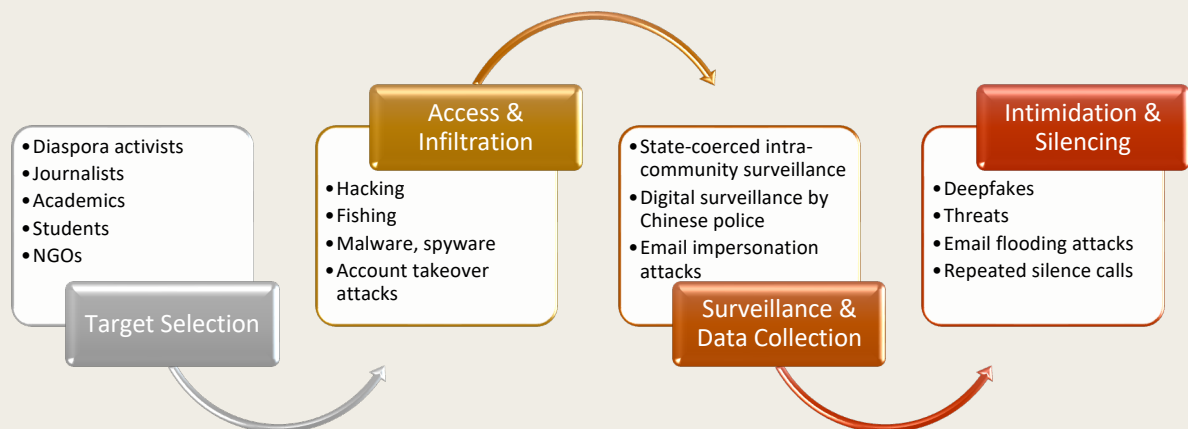
*When the Chinese regime blames us, and we blame the Chinese regime, Dutch people tend to believe that the truth is somewhere in between, like, “Okay, China is authoritarian and may be intimidating Uyghurs, but it should not be as bad as they describe.” Also, they cannot comprehend the idea that a state is constantly watching you. This constant paranoia and fear... They cannot even comprehend it. From that lack of understanding comes forth the other things. The Netherlands’ relationship with China is also important. It is part of the equilibrium. But if they could fully understand the situation, economic relations with China would not be this important in the equilibrium. The new espionage law is changing things in a good way. Previously, there were efforts to address digital transnational repression, but it was generally discussed within the context of radicalism and terrorism. For a long time, when you complained about transnational repression, you were usually directed to a civil servant specialized in radicalization and terrorism. This is changing with the new law.*

This statement provides valuable insights into the cultural nuances that might affect how the Dutch authorities handle digital transnational repression. As the participant emphasized, the severity of the repression might not be fully grasped by those living in a democratic and inclusive society. In such a scenario, the experiences of Uyghur communities with transnational repression might sound unrealistic, even dystopic, to the politicians of host countries, preventing them from fully understanding the mechanism behind it. However, it is promising to learn that new legal regulations might help the government have a clear understanding of the problem and effectively address it—which, according to the participant, might make a difference despite the economic relations between the two countries.

## Technical Mechanism of Digital Transnational Repression

China's digital transnational repression is neither ad hoc nor short term. Rather, it operates as a deliberate and systematic mechanism designed to silence the Uyghur diaspora over the long run. Drawing on my in-depth interviews and research, I present in Figure 1 a clear and accessible model to illustrate how this mechanism functions.

**Figure 1. The Mechanism of China's Digital Transnational Repression**



According to this model, Chinese authorities first identify their targets. Anyone who seeks to draw international attention to state repression and human rights violations in East Turkistan, including diaspora activists, journalists, academics, NGO workers, and students, can be a target. The regime's most powerful source of leverage lies in the family members of activists whom it holds hostage in East Turkistan. As a result, many activists face an acute dilemma: while attempting to be the voice for their families and communities, they simultaneously fear that their activism may expose their loved ones to further harm, such as being sent to internment camps.

In its second strategy, China conducts a range of cyberattacks against targeted activists. Through these attacks, it seeks both to collect data and to

compromise or destroy the data held by activists. This dual objective allows Chinese authorities to monitor any activities within the diaspora while simultaneously undermining activists' ability to document abuses and amplify their voices by erasing evidence.

The third strategy centers on surveillance. Chinese police monitor Uyghurs through digital platforms such as WeChat, or coerce individuals into monitoring one another. This form of surveillance is often used to obtain insider information from within the Uyghur diaspora. At the same time, surveillance produces broader social effects: it encourages self-censorship, causes distrust within the community, and weakens communal ties. Uyghurs who are aware they are under constant surveillance or that other Uyghurs around them are being forced to monitor them also fear repercussions for their family members in East Turkistan.

The fourth strategy involves intimidation and silencing through a variety of tactics, including direct threats and the use of deepfakes. These practices are not entirely new. Even before the widespread adoption of internet technologies, Chinese authorities relied on persistent surveillance and harassment to paralyze Uyghur activism. What has changed is the scale, speed, and reach of these tactics in the digital era. For this reason, it is essential to examine how long-standing intimidation practices have been adapted and intensified in the post-internet environment.

The following section examines in detail the digital attacks associated with each of these strategies.

### ***Email Flooding Attacks and Repeated Silent Calls***

Based on the interviews I conducted, one of my main observations is that China relies on simple yet highly disruptive sabotage techniques, such as email flooding and repeated silent calls, to disrupt Uyghurs' communication with each other and other actors, overwhelm them by paralyzing their digital channels, and isolate them abroad. These tactics are low-cost and difficult to trace, but they can have extremely negative impacts on the daily lives and work of Uyghur activists. They aim not only to interrupt communications, but also to create psychological pressure, disrupt community organizing, and obstruct

access to journalists, policymakers, or legal actors who might otherwise engage with the Uyghur activist.

As a concerning point, it should be highlighted that these attacks often occur during politically sensitive moments. Therefore, they are coordinated strategically with the intention of suppressing the visibility of the Uyghur diaspora.

In an interview, a participant who has been playing a key role in Uyghur activism since their youth described in detail how repeated emails and silent telephone calls<sup>10</sup> paralyzed their lives following the July 5, 2009, Urumchi Massacre. At the time, they were serving in a critical position at the World Uyghur Congress. According to the participant, both the Congress's and their personal email accounts were hacked. They began receiving hundreds of emails per minute every day, making it impossible to distinguish real messages from fake ones. As a result, they had to delete everything in bulk, and some important emails, such as requests for interviews, were unintentionally missed.

A few days later, the telephones in their office started ringing nonstop. When they picked up, there was no sound. The same thing happened to their mobile phone: continuous calls with silence on the other end. They eventually had to unplug the office phone. Their home phone was also targeted in the same way. Because of this, people who wanted to obtain information from them about the genocide could not reach them, and their children were unable to sleep due to the constant disturbance. The participant noted that they prepared a report and submitted it to the German police, and they contacted Deutsche Telekom,<sup>11</sup> but neither could help.

The participant added that the same pattern repeated in 2010, during the first commemoration of the Urumchi events. From one week before to one week after the commemoration, they again received hundreds of emails and their

---

<sup>10</sup> Traditional landlines are considered analog, non-digital communication tools. Nonetheless, intimidation through telephone calls is included in the report to illustrate how communication technologies were used as instruments of repression prior to digitalization.

<sup>11</sup> Deutsche Telekom is a former state telephone service provider.



phones (mobile, home, and office) rang continuously. They were organizing demonstrations in various places related to the Urumchi events, and they believed the harassment was connected to that activity. The calls came from hidden numbers as well as numbers that appeared to originate from China, Taiwan, Hong Kong, and Germany, though most appeared as unknown callers. They prepared another report that year and submitted it to the German police, who were again unable to do anything to help.

This incident illustrates how digital transnational repression sometimes relies on seemingly unsophisticated methods to achieve significant disruptive effects. Yet again, despite not involving advanced spyware or complex intrusion techniques, the power of these types of attacks lies in overwhelming activists' communication channels at precisely the moments when their visibility and leadership are critical.

### ***Account Takeover Attacks***

Social media is an important venue for activists to speak up, coordinate, and garner international support for their demands. As a result, account takeover attacks represent one of the most direct forms of digital transnational repression to silence activists. It not only allows oppressive regimes to take control of and limit the online presence of activists, but also means losing their years of work and impersonation.

During an interview, a participant explained that they had approximately 15,000 followers on X (formerly Twitter) in the early 2020s. One day, they noticed that they could no longer access their account and all of their posts had been deleted. About 20 hours after contacting X, they regained access. However, all of their posts, including significant material about Uyghurs, from the past ten years had been erased permanently. The participant was eventually able to regain their followers, but their 10–11 years of content could not be restored. The participant explained:

*I was hacked. I used Instagram as my main advocacy channel, and it was taken over. Every single person I followed, and everyone who followed me, received a message saying, "Hello, can I get your phone number?" I eventually regained access and reported the incident to the police, but nothing happened. When I got*



*the account back, the interface had been switched to Turkish, which I found quite strange.*

This case illustrates how account takeovers can erase long-term digital advocacy, and it reveals the limited ability of social media platforms and host state authorities to prevent or respond to such attacks.

### ***Deepfakes***

As technology advances and new tools emerge, digital transnational repression adopts new strategies. Accordingly, deepfakes pose an alarming risk for activists by allowing oppressive regimes to create fake audio and video content that can harm the activists' reputations. Unlike usual forms of disinformation, deepfakes utilize artificial intelligence (AI) to create highly convincing content that can be difficult for many viewers to recognize as fraudulent.

A participant explained that, while holding a key leadership position for the organization of a significant meeting for Uyghur activists, they were directly targeted with deepfakes. According to the participant, this was the first time AI was used against them. The attackers used audio recordings of one of their colleagues to generate a fake YouTube video in which that colleague appeared to defame the participant and another colleague.

The disinformation campaign was effective: many people began gossiping about them as a result of the video. In the midst of the stress of the meeting, the colleague whose voice had been misused approached the participant and showed them the video, emphasizing that it was not them. The participant said they could immediately tell that it was AI-generated but acknowledged that not everyone could make that distinction.

Initially, the participant found the situation ridiculous, assuming that people would not take the video seriously. However, members of the Uyghur community got frustrated and accused the colleague in the deepfake video of insulting the participant. Only then did they realize that people were indeed falling for the fake content. The colleague eventually streamed a live video to explain the situation. However, the participant said that the incident not only

harmed them personally, but also damaged their organization's prestige by portraying its members as unprofessional and hostile. They issued a press release and documented the entire incident.

This account shows how deepfakes can inflict reputational, psychological, and organizational harm even when the targeted individual identifies the content as fabricated and provides a clarification. Within diaspora communities already under immense pressure, deepfakes can magnify distrust, fuel interpersonal conflict, and undermine collective organizing.

### ***Email Impersonation Attacks***

Activists frequently contact governmental and nongovernmental actors to raise awareness about their problems and seek international support to mitigate state repression. In this process, email exchanges can play a key role in information and document sharing. However, this opportunity might also bring about certain privacy and security risks.

Email impersonation attacks exploit the trust that activists place in governmental and nongovernmental actors because they manipulate activists into sharing sensitive information with oppressive governments by mimicking authoritative identities, signatures, and communication formats. For example, one of the participants recounted that when Michelle Bachelet, then the United Nations High Commissioner for Human Rights, visited China for the “friendly dialogue,” they, along with other activists, had submitted numerous important documents regarding Uyghurs’ detention, disappearances, and the locations of internment facilities. Although there had been some email exchanges, the participant believed that they never managed to reach Bachelet’s office directly. The participant and a colleague instead approached the foreign ministry of their country through its United Nations delegation to ensure the documents were delivered. According to the participant, their colleague personally handed these documents to ministry officials, who then passed them on to the Office of the High Commissioner for Human Rights (OHCHR).

A few days later, the participant received an email from someone pretending to be OHCHR staff. The message was sent by an individual impersonating the High Commissioner who thanked them for submitting the documents and

instructed them to communicate only with her directly from that point forward, allegedly for “privacy reasons,” rather than contacting other OHCHR departments or government offices. Although the logo and signature looked legitimate, the email was not sent from an official United Nations address. Strangely, the message was not sent to the participant or their colleague but to the Uyghur committee in their country. The participant suspected that someone within the United Nations might have shared their correspondence with Chinese authorities, which could explain why such an email was sent.

This incident described by an Uyghur activist illustrates that impersonation attacks can manipulate information flows at critical diplomatic moments. In the context of Uyghur advocacy, these tactics can undermine crucial channels for reporting human rights violations and can harm trust among activists, host governments, and international organizations.

### ***Digital Intimidation by Chinese Police***

In China, a common strategy of digital transnational repression is to force Uyghurs living abroad to stay in touch with police and report regularly via communication platforms such as WeChat and Telegram. This way, authorities can constantly monitor Uyghurs, control their behavior, and exert psychological pressure. Most of the time, Uyghurs maintain this communication to protect their families in East Turkistan from police pressure or the risk of being sent to the internment camps.

A participant explained that the attitude of the police officers contacting them through WeChat began to change in 2017, as state repression intensified in East Turkistan. The officers started sending extremely harsh messages, ordering the participant to fill out and return various forms, often using an aggressive tone. These forms typically asked questions about where the participant studied, their monthly living expenses, and similar personal information. The participant said they filled out such forms several times and sent them back via WeChat.

One day, the officer told the participant that Islamic names had been banned by the Chinese regime, so they needed to change their last name, which contained an Islamic term. When the participant reminded the officer that

their original last name appeared on their academic diplomas, making it difficult to change, the officer became very hostile and responded aggressively, questioning who the participant thought they were and saying things like, “Do you think the people who make these laws do not know what they are doing?” The participant described trying to remain calm during these interactions and noted that whenever they received a message from the police on WeChat, they trembled with fear.

The participant also recounted that the officer later ordered them to take and send several photographs: one holding their Chinese passport and national ID in both hands, another at the entrance of the university, and another with the police officer responsible for their district. The officer also demanded photos with friends or professors. The participant complied, sending the photo with their passport and ID, and later one with a professor. However, they were scolded in a WeChat call in the middle of the night for not sending the photo at the entrance of the university. Their roommates were asleep, and it was difficult to leave the dorm at that hour without security approval. The participant sought help from a friend, and the two of them went together to the entrance to take and send the required photograph.

The key takeaway from this incident is that the scale and intensity of digital transnational repression can reach extreme levels that can intimidate Uyghurs and instill profound fear.

### ***Account Suspension and Content Removal***

My conversations with Uyghur activists demonstrate that digital platforms originating in China do not tolerate content being posted in the Uyghur language, let alone using the platform to contact family members without surveillance. By removing their content and suspending their accounts, the regime prevents Uyghurs from sharing information with those in East Turkistan.

During an interview, one of the participants explained that their Chinese social media accounts on platforms such as Douyin and Kuaishou were taken down. Although they were not an active user, they relied on these platforms to follow others’ updates and occasionally obtain information about their relatives. All

of their accounts were systematically removed, leaving them with no remaining presence on China-based online media platforms.

Another participant described their experience with Douyin. They said that opening an account was extremely difficult, as it required facial recognition, their WeChat ID, and a photo of their Chinese ID card. They could create an account only after completing all of these steps. They believed that people outside China have to go through similar challenges. When they tried to post something, it took a very long time, even hours. Most of the time, their content in the Uyghur language was removed with warnings such as “sensitive content” or “unrecognized language.” They also had posted a few things about the Uyghur-language books they were reading, but those posts were also taken down. Even the videos in which they simply spoke Uyghur and sent greetings to their family were removed.

Based on these experiences, it can be concluded that platform-level controls can be weaponized by governments to suppress minority identity, language, and communication across borders. By removing accounts and censoring even cultural content, China-based platforms limit the Uyghur diaspora’s ability to maintain their relationship with their families. The pattern reflects a broader strategy of digitally isolating Uyghurs from those in East Turkistan so they cannot obtain information from inside the region and share it with the world.

### ***State-Coerced Intra-Community Surveillance***

During the interviews, many participants reported that they were either coerced by Chinese police to gather information on other community members or informed by acquaintances that the police had pressured them to collect intelligence on the participants themselves. This tactic can have extremely negative consequences for Uyghurs’ relationships by transforming their community ties into potential channels for surveillance.

A participant reported that people in their social circle were approached and questioned about them. One of their friends contacted the participant to share that the police had requested extensive information about them, which left that person feeling guilty. According to the participant, authorities had reached out to their friend via WhatsApp, and in some cases also used Telegram or

WeChat. The participant stated that they believed the most recent outreach occurred through WhatsApp. Their friend had forwarded the message, and the participant was able to listen to the voice recording sent by the police. The participant noted that pressures and fears of this kind led many Uyghur friends to block them on social media, and that some friends were even afraid to take photos with them.

This example reveals the social and emotional costs of state-coerced surveillance. By pressuring community members to surveil each other, Chinese authorities weaponize social relationships and turn ordinary communication channels into sites of intimidation and fear.

### ***Hacking***

Hacking is a common vector of digital transnational repression that allows oppressive states to infiltrate activists' devices, collect information about their activities, and delete materials that are significant for activists, such as proof of state oppression.

A participant recounted several suspicious incidents that occurred when they used China-based applications. They described an app called WangYiYun, which can be used to listen to music, send messages, and share content. A relative contacted the participant through that app. Because the participant had lost all communication with their family, they had no idea what was happening at home.

According to the participant, this relative had visited their father in prison and had taken the participant's sibling there. The relative sent the participant a photo of their father and sibling from inside the prison, one that appeared to have been taken secretly. They also sent an image of a Chinese propaganda poster, along with other similar materials. The participant said they did not fully understand why these items were sent, but perhaps the relative thought such information might be useful abroad or could help amplify the family's situation.

However, the participant then noticed something unusual. Although they never deleted anything, all the files they had downloaded from WangYiYun suddenly

disappeared from their phone. The participant stated that the app did not have any feature that would automatically remove content from a user's phone. The relative who had contacted them also vanished, and the prison photo was gone as well.

At the time, the participant spoke with someone knowledgeable about hacking. When the participant told them what happened, they warned that someone may have infiltrated the phone and advised them to delete WeChat and even reset the device. The participant concluded by saying that they still do not know how it happened, only that these specific items disappeared from the phone.

The strange and sudden disappearance of files, especially sensitive material, underscores how hacking can be used not only for data collection, but also for deleting evidence and instilling fear. Even without technical confirmation, such incidents signal the pervasive insecurity that Uyghurs face when using digital platforms originating in China.

## **KEY FINDINGS**

### **Reluctance to Report Incidents to Local Authorities**

Many of the activists I interviewed chose not to report the incidents of digital transnational repression for two main reasons. First, they previously had a negative interaction with local authorities who dismissed their experiences or questioned their innocence. Second, they had a perception that reporting the incident would be futile due to the complexities surrounding digital transnational repression, such as attribution problems and the transnational nature of the threats.

Across all countries studied, these two issues discouraged participants from future reporting. Therefore, an effective and understanding approach to victims of digital transnational repression is greatly needed.

### **Structural Barriers Limiting Police and Government Response**

In addition to anonymity and the technical complexity of digital transnational repression, a lack of effective coordination between police, legal actors, and government actors prevented meaningful action when victims sought support. Many countries do not have a well-designed espionage law to address other countries' attempts to infiltrate their digital systems. Furthermore, police responses often reflect poor training or a misunderstanding of host states' obligations to protect diaspora communities.

These structural problems create a recurring pattern: victims are encouraged to report incidents, but authorities have limited tools to act.

### **Police Responses Reinforce Harm Rather Than Providing Protection**

In several cases, when participants asked for help, they were interrogated about whether or not they had committed crimes in China instead of having their complaints properly registered. Such an attitude exacerbated their feelings of victimization and discouraged them from contacting authorities for future incidents due to loss of trust.



The loss of trust in host state institutions may contribute to silence and self-censorship among Uyghur activists. Moreover, it may reduce the likelihood of future incidents, which may prevent governments and researchers from fully understanding the scale of digital transnational repression.

### **Ineffective Response Means More Incidents**

Participants continue to receive persistent phone calls from numbers registered abroad; experience unauthorized access attempts on their social media accounts, which they use to advocate for Uyghurs' rights; and are subjected to constant physical and technological surveillance when authorities do not effectively respond to digital transnational repression. This is significant in demonstrating that China's digital operations expand without consequence in countries that have not taken concrete steps to solve this problem.

### **Uyghurs Face Digital Repression Concurrently with Psychological Harm**

Participants reported that they experienced fear and anxiety due to receiving death threats, hearing heavy breathing or screaming during anonymous phone calls, and being the targets of physical surveillance during protests and meetings. The emotional cost of such experiences is exacerbated due to the lack of awareness and limited capacity to investigate digital transnational repression.

### **Uyghurs Take Action and Support Host Countries When Necessary**

Uyghurs cooperate with other affected groups against digital transnational repression and support their host countries by documenting their cases and sharing them with authorities, working actively with politicians and nongovernmental organizations to raise awareness, and lobbying for technical solutions, legal reforms, and training programs. These collective efforts have compelled governments to take incremental steps to combat digital repression.

### **There is Progress, Though Slow**

Evidence drawn from interviews and additional research shows recent progress in some countries, particularly Germany and the Netherlands. For example, the initiation of hotlines for reporting transnational repression, increasing political engagement from politicians, new legal regulations and espionage laws, ongoing training for police on transnational repression and digital threats, and improving coordination between community organizations and government offices are promising developments.

While these steps remain early and uneven, they demonstrate that persistent advocacy can lead to tangible policy change.

## CONCLUSION

This report has presented a comprehensive analysis of the mechanisms behind China's digital transnational repression and its impact on the Uyghur diaspora. Drawing on in-depth interviews with Uyghurs in Germany, Norway, the Netherlands, the United States, and Türkiye, the report has demonstrated that this form of repression significantly constrains the Uyghur diaspora from speaking out for themselves and for Uyghurs in East Turkistan facing state repression that has long taken a dystopian turn.

During the interviews, participants consistently underlined the legal and institutional gaps that limit the protection of victims of digital harassment and intimidation, including but not limited to anonymous threats, surveillance, and unauthorized attempts to access their online accounts. However, many chose not to report these incidents due to previous negative encounters with authorities, and consequently, the common perception that governments lack the necessary capacity to address digital threats of foreign origin. While some countries have made progress toward establishing effective response mechanisms to minimize the risk of transnational repression, this progress remains slow and limited to a small number of countries, such as Germany and the Netherlands.

The report has also highlighted the profound psychological toll that digital intimidation imposes on targeted individuals. Fear, anxiety, and self-censorship have emerged as common consequences of persistent harassment that has escalated to death threats in some cases. These feelings were exacerbated when host states failed to protect the victims, or even worse, questioned their innocence. As a result, victims lost trust in the institutions that are supposed to protect them and avoided reporting the digital incidents that they experienced, making it challenging for researchers to assess the extent of the problem.

Despite these challenges, the findings demonstrate the strong agency and resilience of Uyghur activists who collaborated with civil society organizations and diaspora communities in host states, documented digital incidents, shared

their experiences with policymakers, and advocated for political and legal reforms to counter digital transnational repression. These efforts have begun to produce meaningful progress in some countries, including the creation of hotlines and additional training for police officers. While the progress remains modest, it suggests that persistent advocacy and reporting can make change possible.

## **RECOMMENDATIONS FOR FUTURE RESEARCH**

### **Toward a More Inclusive and Interdisciplinary Research Agenda**

The interviews I conducted demonstrate that digital transnational repression encompasses various components: local, international, political, legal, social, and emotional. Consequently, future research should incorporate perspectives from political science, sociology, anthropology, information science, cybersecurity, and diaspora studies to capture the complex and multilayered nature of digital transnational repression more accurately.

### **Development and Use of Large-Scale Datasets to Identify Cross-Case Trends**

Although the literature on digital transnational repression is expanding, the majority of studies focus on a single case (a community, country, or region). Therefore, it is challenging to observe the general trends in digital transnational repression across cases. I recommend that scholars prioritize building and expanding systematic large-N datasets that capture repression patterns and state-diaspora interactions to strengthen comparative analysis and move the field beyond single-case descriptions.

### **Expanded Analyses of Understudied or Marginalized Communities**

While there is an increasing volume of research on the digital transnational repression of certain communities, such as Iranians and Uyghurs, many targeted communities still remain understudied. I suggest that future research expand the focus to communities that have received limited scholarly attention, as doing so will reveal diverse manifestations of digital repression and prevent narrow understandings of the phenomenon.

### **Policy-Oriented Research to Inform Actionable Interventions**

Each of my interviews revealed a significant problem: the absence of a proper policy design to effectively address digital transnational repression. Therefore, I recommend that scholars aim to generate findings with direct utility for policymakers, civil society organizations, and international institutions. They

can consider highlighting practical pathways for improving protection mechanisms and accountability frameworks.

### **Careful Assessment of Risks When Sharing Evidence of Repression**

Proof of how Uyghurs have been targeted by digital transnational repression has not been included in this report to avoid any risks, even minor ones, that participants or their families would face. I strongly recommend that, in future work, scholars carefully evaluate the risks, prioritize the security and privacy of targeted community members, and ensure that documentation practices do not inadvertently expose them to further harm.

### **Closer Examination of the Responsibilities of Mainstream Social Media Platforms**

This report critically evaluated the role of China-originating digital platforms in digital transnational repression. Future scholarship may investigate the responsibilities of other major platforms in detecting, enabling, or failing to address digital transnational repression.