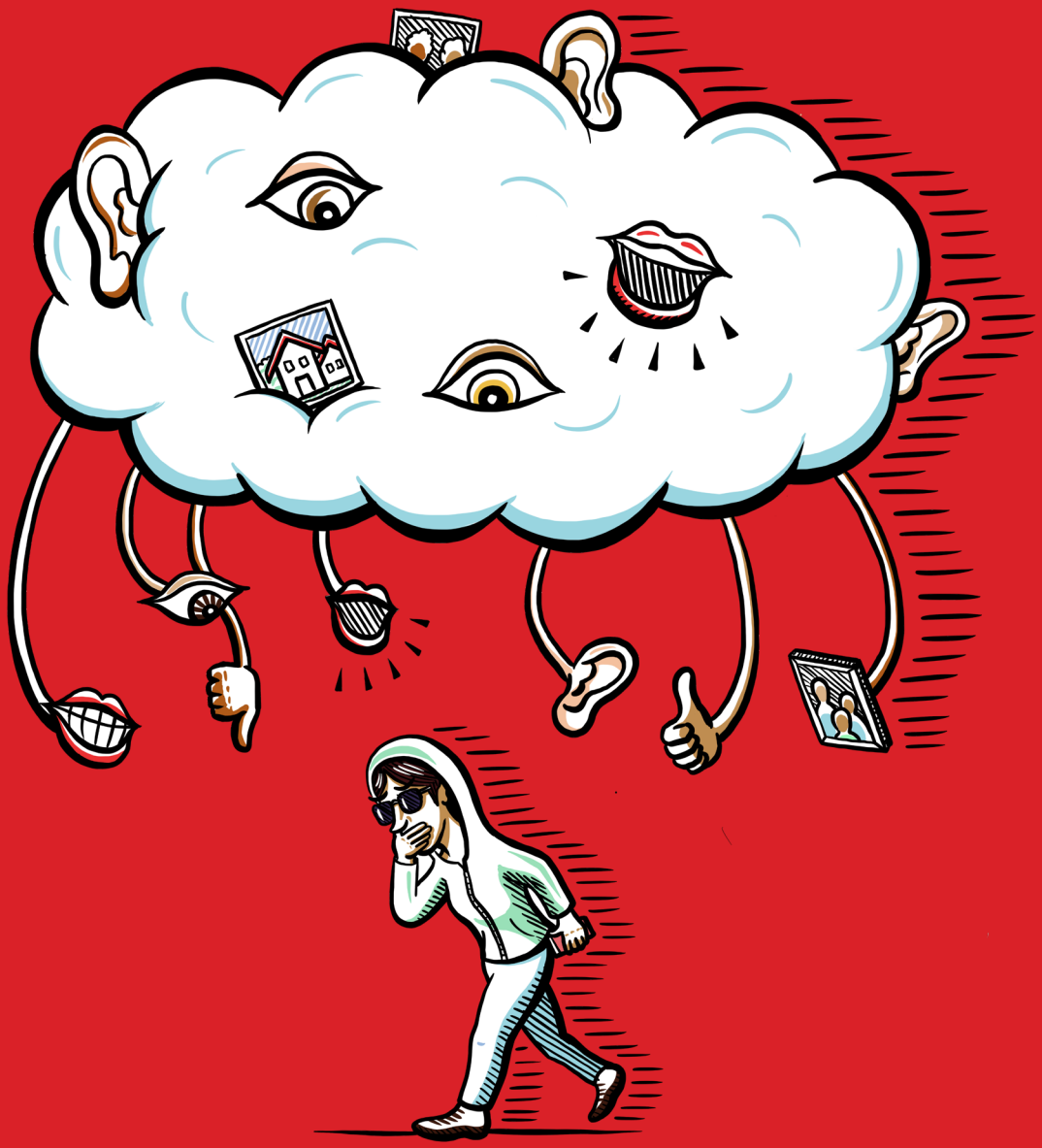


SILENCING ACROSS BORDERS

TRANSNATIONAL REPRESSION AND DIGITAL THREATS AGAINST EXILED ACTIVISTS FROM EGYPT, SYRIA, AND IRAN

Marcus Michaelsen

Hivos
people unlimited

HIVOS

Humanist Organization for Social Change
Grote Marktstraat 47a
2511 BH The Hague
The Netherlands
www.hivos.org

Cover illustration: **Jason Li**
www.hongkonggong.com

Layout: **Ura Design**
ura.design

Hivos
people unlimited

CONTENTS

PAGE

ACKNOWLEDGEMENTS

This research would not have been possible without the generous funding and support of the Open Technology Fund. The Information Controls Fellowship offered the ideal platform and network to complete this project. I am also grateful to the host organization, Hivos, in particular the MENA team who took on the project despite their busy schedule. The research was further facilitated by an affiliation to the Political Science Department of the University of Amsterdam, provided by the program group Transnational Configurations, Conflict and Governance. Valuable feedback on the research process and earlier versions of the report came from Tin Geber, Wieke Meilink, Daniel Ó Cluanaigh, Nadia Novibi, Oussama Jarousse, Gillo Cutrupi, Noura Aljizawi, Robert Adams, and Benjamin Stachursky. Nate Schenkkan gave essential advice on the recommendation section. Thank you to John R. Stith for his meticulous copy-editing of the report. Most of all, I wish to thank my numerous interlocutors for sharing their time and insights with me. Speaking with each one of them has been an instructive and enriching experience. Without them this report simply would not exist. All errors and misrepresentations are obviously mine.

ABOUT THE AUTHOR

Marcus Michaelsen was an Information Controls Fellow with the Open Technology Fund in 2018-19. He holds a PhD in Media and Communication Studies and has previously worked as a researcher for the "Authoritarianism in a Global Age" project in the Political Science Department of the University of Amsterdam. As of 2020, he continues to research digital technologies, human rights, and authoritarian politics in the Law, Science, Technology and Society research group (LSTS) at the Vrije Universiteit in Brussels.

Hivos people unlimited

SUMMARY

1

Authoritarian regimes use a variety of repressive tools to control, silence, and punish dissidents living abroad. Although blatant acts of violence against political exiles, such as kidnappings and assassinations, occasionally catch the public's attention, this report focuses on the more subtle and pervasive forms of transnational repression exerted against activists living outside their homeland. Using Egypt, Syria, and Iran as examples, the report examines how governments rely on surveillance, smear campaigns, and other threats to systematically disrupt cross-border information flows and curtail the opportunities of human rights defenders and journalists in exile.

2

The overseas export of this type of repression has a clear authoritarian intent. Through "toolkits" of transnational repression, regimes looking to shield themselves from criticism and accountability are able to foster restraint and self-censorship among activists living abroad. Targeted activists experience constant tension and stress, and see their ties to the home country undermined. In turn, the dynamics, impact, and outreach of diaspora activism are inevitably altered. These practices of transnational repression represent deliberate and systematic interferences in the fundamental human rights of the targets, primarily by violating their right to privacy and freedom of expression.

3

Digital technologies are essential components of all forms of this transnational repression. They reduce the costs of exerting political control while enabling regimes to monitor and respond to diaspora activism with greater scope and speed. Activists' reliance on digital platforms and social media creates multiple points of exposure that regime agents can attack via malware, online harassment, and disinformation campaigns. These digital threats are often intertwined with more traditional methods of repression, such as pressure on families inside the country and slander in state media.

4

Although the use of digital security precautions is increasingly prevalent, diaspora activists often feel overwhelmed by the complexity of digital platforms and the rapidly evolving environment of sociotechnical risks. With ties across multiple countries and communities, these activists belong to networks in which a successful attack against the weakest link could lead to severe consequences for all involved. Uncertainty about the technical capabilities of regimes further exacerbates the chilling effects of surveillance.

5

To build the security and resilience of transnational civil society networks, it is therefore necessary to continue to raise the general level of understanding of digital technologies and the risks associated with their use. Protecting data and privacy is a collective effort that requires a more even distribution of risks and resources. Activists on the frontlines are empowered when closely tied to networks for incident response, long-term support, and information sharing.

INTRODUCTION

In October 2018, Saudi dissident Jamal Khashoggi was brutally murdered inside the Istanbul consulate of Saudi Arabia. The prominent journalist and vocal critic of the Saudi government had emigrated to the United States in 2017 to evade increasing restrictions in his home country.[1] Khashoggi's assassination served as a shocking reminder of the great lengths authoritarian governments will go to silence dissent abroad. Yet Saudi Arabia is not alone in such actions. Other like-minded regimes consistently target political emigrants and stifle criticism outside their territory.[2] Though their practices of repression across borders are not always as drastic as in the Khashoggi case, such regimes nevertheless engage in widespread and systematic attempts to interfere with civic activism and freedom of expression in diaspora and exiled communities. This report investigates the forms of transnational repression used against political activists, human rights defenders, and journalists from Egypt, Syria, and Iran.

Recent movements for social justice and political freedom in the Middle East and North Africa have been quelled by an authoritarian backlash and sweeping repression. Severe constraints for opposition, civil society, and media have pushed numerous activists and journalists into exile. From abroad, however, many of these emigrants continue to advocate for human rights and political change by creating new initiatives or integrating into existing civil society organizations. In doing so, they act as important relays in transnational advocacy networks, expose human rights violations, and circumvent the information controls of their home regime. Unfortunately, this work often makes them targets of repression for governments willing to reach beyond their borders and into the environments of host societies.

Transnational repression is not a new phenomenon: in 1940, Leon Trotsky was assassinated by a Soviet agent in Mexico; in 1991, Shapour Bakhtiar, the last prime minister of Iran under the Shah, was killed near Paris by assassins of the Iranian regime.[3] Today, however, both the scale and the scope of extraterritorial control and repression have been enhanced by digital technologies. Social media and digital communication allow civil society activists to maintain close relations across borders and access global news and advocacy cycles. Yet the use of these technologies creates multiple points of exposure that state actors can exploit for surveillance, malware attacks, online harassment, and disinformation campaigns. And these digital threats are often combined with more traditional methods of repression, such as pressure on in-country relatives and slander in state media.[4]

[1] Kirkpatrick, D., & Cumming-Bruce, N. (2019, June 19). Saudis Called Khashoggi 'Sacrificial Animal' as They Waited to Kill Him. *The New York Times*. https://www.nytimes.com/2019/06/19/world/middleeast/jamal-khashoggi-Mohammed-bin-Salman.html.

[2] Hirt, N., & Saleh Mohammad, A. (2018). By way of patriotism, coercion, or instrumentalization: How the Eritrean regime makes use of the diaspora to stabilize its rule. *Globalizations, 15*(2), 232-247; Hug, A.(ed.). (2016). No Shelter: The harassment of activists abroad by intelligence services from the former Soviet Union. Foreign Policy Centre, London; Schenkkan, N. (2018, January 29). The Remarkable Scale of Turkey's "Global Purge." *Foreign Affairs*. https://www.foreignaffairs.com/articles/turkey/2018-01-29/remarkable-scale-turkeys-global-purge. *See also* the Central Asian Political Exiles (CAPE) database of the University of Exeter Central Asian Studies Network. https://excas.net/projects/political-exiles.

[3] Iran Human Rights Documentation Center (2011). No Safe Haven: Iran's Global Assassination Campaign. New Haven. https://iranhrdc.org/no-safe-haven-irans-global-assassination-campaign; Shain, Y. (2005). *The Frontier of Loyalty: Political Exiles in the Age of the Nation-State*. University of Michigan Press.

[4] Michaelsen, M. (2018). Exit and voice in a digital age: Iran's exiled activists and the authoritarian state. *Globalizations, 15*(2), 248-264; Moss, D. M. (2018). The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora. *Globalizations, 15*(2), 265-282.

Based on more than 50 qualitative interviews with activists from Egypt, Syria, and Iran, this report aims to provide a deeper understanding of the type of threats faced by human rights defenders and journalists in these situations. In doing so, the report seeks to answer the following questions:

1. What are the tools and practices used by regimes to control and contain dissent across borders?
2. What are the effects of these threats on diaspora and exiled activists?
3. How do targeted activists respond? What are their security practices and needs?

The report highlights the systematic attempts of authoritarian regimes to harass, threaten, and silence critics and dissidents abroad. It also outlines the principal motives and tools of regimes engaging in repression across borders. In line with current literature on authoritarianism, the report argues that the methods and tactics of transnational repression have both an illiberal and an authoritarian dimension: they not only interfere with individual rights, they also serve to consolidate uncontested political power. For example, spying on dissidents abroad by hacking into their accounts and communications is illiberal because it violates one's privacy and dignity. But the practice also has an authoritarian intent, as doing so aides and accompanies other threats to disable the voices of political exiles, suppress and distort critical information, and, ultimately, "shield power-holders from accountability."[5] Transnational repression that utilizes digital technologies is therefore both a human rights problem and a political problem.[6]

This report provides insight into the vulnerabilities of transnational activists and the security practices they rely on in an increasingly complex environment of sociotechnical risks. Diaspora and exiled activists navigate complex "transnational fields" with ties to various contexts and communities in home and host societies.[7] Their security is dependent upon these relations as regime agents identify and exploit weak spots in social networks to reach for key activists abroad. Safeguarding the security of diaspora activists is therefore a collective effort that should seek to strengthen resilience, support, and information-sharing in civil society networks.

EMBEDDING IN CURRENT RESEARCH

This report intervenes at the intersection of three pre-existing areas of research:
(1) the extraterritorial reach of state repression, (2) the use of digital threats against civil society, and (3) the security of human rights defenders.

First, research on the extraterritorial reach of state repression has shown that contemporary authoritarian regimes are not confined to a specific territory with rigid and closely guarded borders. Instead, as global flows of information and migration intensify, these regimes are able to extend the reach of their domestic political controls and assert authority over citizens living abroad via a range of policies designed to threaten and silence dissidents.[8] As this report shows, digital technologies have enabled governments to expand their established tactics of extraterritorial state repression by monitoring and rapidly responding to diaspora activities on a large scale.

[5] Glasius, M. (2018). What authoritarianism is... and is not: A practice perspective. *International Affairs, 94*(3), 515-533, p. 530.

[6] Glasius, M., & Michaelsen, M. (2018). Illiberal and authoritarian practices in the digital sphere—Prologue. *International Journal of Communication 12*, 3795-3813.

[7] Levitt, P., & Schiller, N. G. (2004). Conceptualizing simultaneity: A transnational social field perspective on society. *International Migration Review, 38*(3), 1002-1039.

[8] Glasius, M. (2018). Extraterritorial authoritarian practices: A framework. *Globalizations, 15*(2), 179-197; Jörum, E. L. (2015). Repression across borders: homeland response to anti-regime mobilization among Syrians in Sweden. *Diaspora Studies, 8*(2), 104-119; Lewis, D. (2015). "Illiberal Spaces:" Uzbekistan's extraterritorial security practices and the spatial politics of contemporary authoritarianism. *Nationalities Papers, 43*(1), 140-159; Moss, D. M. (2016). Transnational repression, diaspora mobilization, and the case of the Arab Spring. *Social Problems, 63*(4), 480-498.

Second, research on digital threats against civil society has made important strides in understanding the technical underpinnings of attacks targeting journalists, human rights defenders, and political activists across countries and diaspora communities.[9] It has also shed light on the role of private companies that help governments build intrusive systems for communication monitoring and surveillance.[10] Less is known, however, about the ways in which potential targets perceive and respond to these complex risks, and how they are affected by digital threats.[11] This report explores these critical areas.

Third, the report builds on practitioner-oriented research into the security of human rights defenders. Of particular value are the holistic understandings of security that take into account the sociopolitical context, as well as the physical integrity and well-being of activists, to accurately identify risks and map out potential responses.[12] To better address the risks associated with a reliance on digital technologies, it is important to widen the scope beyond mere technical responses and consider the broader human and behavioural factors shaping practices of privacy protection and digital security.

RESEARCH METHODS

In preparation of this report, interviews were conducted with 52 respondents from Syria, Egypt, and Iran, living in 12 different host countries. Respondents included human rights defenders, journalists, digital security experts, and other civil society activists living and working in exile or diaspora communities (see table, below). While acknowledging the conceptual ambiguities between "diaspora" and "exile," the report uses both terms interchangeably to give consideration to the diverse identities and experiences of respondents. Most interview partners would certainly qualify as "exiles" as they recently left their homeland for political reasons and are engaged in "political activities directed against the policies of a home regime, against the home regime itself, or against the political system as a whole, so as to create circumstances favourable to their return." [13] Whereas exile refers to a more individual experience that is often perceived as temporary, "diaspora" focuses on communities maintaining a collective cultural or national identity across borders based on ties with the homeland. The term therefore also encapsulates migrants of the second and third generation who are engaged in activism directed at their original homelands. [14]

[9] Amnesty International (2018, December 19). When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users. https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough; The Citizen Lab (2014). Communities @ Risk: Targeted Digital Threats against Civil Society. https://targetedthreats.net.

[10] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. The Citizen Lab. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries; Marquis-Boire, M. et al. (2013). Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. The Citizen Lab. https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools; Privacy International (2016). The Global Surveillance Industry. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

[11] For an exception highlighting this research gap see: Marczak, W., & Paxson, V. (2017). Social engineering attacks on government opponents: Target perspectives. *Proceedings on Privacy Enhancing Technologies* (2), 172-185.

[12] Hankey, S., & Ó Cluanaigh, D. (2013). Rethinking risks and security of human rights defenders in the digital age. *Journal of Human Rights Practice 5*(3), 535-547; Kazansky, B. (2016). Digital Security in Context: Learning How Human Rights Defenders Adopt Digital Security Practices. Project report. https://secresearch.tacticaltech.org/media/pages/pdfs/original/DigitalSecurityInContext.pdf; Tactical Technology Collective (2016). Holistic Security: A Strategy Manual for Human Rights Defenders. https://holistic-security.tacticaltech.org.

[13] Shain, Y. (2005). *The Frontier of Loyalty: Political Exiles in the Age of the Nation-State*. University of Michigan Press, p. 15.

[14] Koinova, M. (2018). Sending states and diaspora positionality in international relations. *International Political Sociology, 12*(2), 190-210.

Total number of interviewees	**52**	
Female : Male	**11 : 41**	
Country of origin	**Syria:** **Egypt:** **Iran:**	**20** **16** **16**
Country of residence	**Germany:** **Turkey:** **US:** **France:** **NL:** **UK:** **Czech Rep:** **Tunisia:** **Jordan:** **Canada:** **Other:**	**16** **9** **6** **3** **4** **3** **3** **2** **2** **2** **2**
Professional background	**Journalist:** **Civil Society/Human Rights:** **Digital Tech:**	**15** **26** **11**

Respondents were interviewed from September 2018 to June 2019 after a recruitment through "snowball sampling", building on established contacts of the researcher, funding and host organization (Open Technology Fund and Hivos, respectively). Respondents were selected with the goal of obtaining a diverse sample of interviewees in terms of gender, host country, organizational background, type of activity, and recognition. Nevertheless, the ultimate participation of respondents was determined by the ability—or lack thereof—to secure an introduction and build trust. Despite significant time and effort spent creating a network of supporters around the project, not all contacts who were approached for an interview agreed to participate.

Interviews proceeded on the basis of a semi-structured guideline, leaving room for additional questions. Topics included respondent's reasons for emigration, current activities, links to home country, situation in host country, experienced threats, digital security practices, risk perceptions, and digital security needs. All interviews were transcribed, partly translated into English, and analyzed to assess the emergence of common themes. The coding of the material was also guided by the basic questions and goals of the project. In addition, the research and initial findings were discussed with a number of digital security experts and trainers to further contextualize and corroborate results.

Given that the project dealt with respondents from contexts characterized by high repression and extensive surveillance, security was a core concern throughout the research process. The protection of communications and research data was prioritized in order to minimize potential risks of harm.[15] Great care was taken to create a safe space for conversation and limit intrusions into the professional and personal life of respondents. To obtain informed consent, respondents were notified from the outset about the purpose and background of the project. In doing so, a written consent form was not used to avoid creating an additional paper trail linking respondents by name to the project and scaring off potential respondents reluctant to sign an "official" document.

All interviews were conducted in-person or via a Voice over Internet Protocol (VoIP) channel. Respondents were allowed to choose the application for online interviews, providing a first glimpse into their security behavior (e.g., the decision to use of applications considered to be more safe than others, such as Wire vs. Skype). Interviews were recorded only after the express consent of respondents was obtained. Transcriptions and notes resulting from interviews were anonymized and stored in encrypted documents. When using interview material and quotes in the written findings, the researcher removed all identifying information, such as names of locations or organizations, while seeking to preserve contextual depth. All interviews are referenced anonymously with an archival number and the month in which the interview was conducted.

The selection of respondents has three potential drawbacks. First, due to the use of referral sampling, the researcher was only able to approach those respondents who were still active in their respective field. Any former activists, who may have quit as a result of regime pressure, were excluded. Second, with only two exceptions, none of the respondents had the intention to travel or return to their home country in the near future. This inclination meant they were potentially more immune to threats from the home regime. Third, some respondents may have had an interest to exaggerate threats to emphasize the relevance of their activities; others may have downplayed certain risks in accordance with their own "mental models" of security. The information gained through this research approach is therefore somewhat subjective and risks distorting the scale, pervasiveness, and impact of the repressive practices targeting diaspora communities.

Nonetheless, the sample size of respondents was large enough to reach a level of saturation and identify recurring patterns across all three country cases. Furthermore, as a qualitative study, the research did not aim at a statistical solid representation but rather an in-depth description of the phenomenon of transnational repression and its repercussions. Finally, initial findings and draft versions of this report were shared and discussed with a number of respondents to correct misperceptions on the part of the researcher and give them a voice in the representation of their experiences.

[15] In engaging with respondents from high-risk and activist contexts, the research for this report relied, in part, on the following sources: Glasius, M. et al. (2017). *Research, ethics and risk in the authoritarian field*. Palgrave Macmillan; Kazansky, B., Torres, G., Van der Velden, L., Wissenbach, K., & Milan, S. (2019). Data for the Social Good: Toward a Data-Activist Research Agenda. In: Daly, A., Devitt, K., & Mann, M. (eds). Good Data. Institute for Network Cultures, Amsterdam. http://networkcultures.org/wp-content/uploads/2019/01/Good_Data.pdf.

POLITICAL CONTEXT: DISSENT AND EXILE IN EGYPT, SYRIA, AND IRAN

Countries in the Middle East and North Africa—such as Iran, Syria, and Egypt—are undergoing a period of profound political change and conflict. Across the region, protest movements for social justice and political freedom are challenging long-term dictatorships. In response, regimes have resorted to repression and violence, imposing severe constraints on members of the opposition, civil society, and media.[16] This authoritarian backlash dashed aspirations of more political and economic participation, pushing many people—especially those of the younger generations—to emigrate. Additionally, many of the activists and journalists involved in the protest movements were forced into exile where they then continued to advocate for human rights and political change.

In Iran, the protests of the Green Movement against the manipulation of the 2009 presidential elections were followed by a crackdown on the reformist opposition and civil society that stifled political and civic activism. The following years saw the largest exodus of journalists and activists since the Islamic Revolution.[17] Although the election of a moderate president in 2013 provided temporary reprieve, restrictions on political and civil liberties remained severe. Religious minorities, women's rights advocates, and environmentalists were among recent targets of state pressure.[18] Those who left joined a large and diverse Iranian diaspora in Europe and North America whose roots date back to even before the 1979 revolution. Organizations and initiatives emerging after the Green Movement often united second generation migrants with recent exiles, overriding previous barriers and instilling new life in Iranian diaspora activism. [19]

In Syria, the 2011 uprising against the regime of Bashar Al-Assad has morphed into a protracted civil war.

---

[16] Ansari, A. M. (2010). *Crisis of authority: Iran's 2009 presidential election*. Chatham House, London; Ketchley, N. (2017). *Egypt in a time of revolution. Contentious Politics and the Arab Spring*. Cambridge/New York: Cambridge University Press; Yassin-Kassab, R., & Al-Shami, L. (2018). Burning country: *Syrians in revolution and war*. Pluto Press, London.

[17] Human Rights Watch. (2012). *Why They Left: Stories of Iranian Activists in Exile*. https://www.hrw.org/sites/default/files/reports/iran1212webwcover_0_0.pdf; Michaelsen, M. (ed.) (2011) Election Fallout: Iran's Exiled Journalists on their Struggle for Democratic Change, Berlin: Hans Schiler. https://library.fes.de/pdf-files/iez/08560.pdf.

[18] Amnesty International (2019, January 24). Iran's 'year of shame': More than 7,000 arrested in crackdown on dissent in 2018. https://www.amnesty.org/en/latest/news/2019/01/irans-year-of-shame-more-than-7000-arrested-in-chilling-crackdown-on-dissent-during-2018; United Nations (2019, July 18). Report of the Special Rapporteur on Human Rights in Iran. https://undocs.org/en/A/74/188.

[19] Kelly, M. (2011). Transnational diasporic identities: Unity and diversity in Iranian-focused organizations in Sweden. *Comparative Studies of South Asia, Africa and the Middle East, 31*(2), 443-454.

Over the course of the conflict, more than half a million people have been killed and 5.6 million have taken refuge outside the country.[20] Early on, relentless repression forced many of the civic figures behind the uprising to flee. Systematic imprisonment, torture, military campaigns, and the rise of armed extremist groups have further decimated Syria's civil society.[21] However, numerous non-governmental organizations, associations, and media platforms have emerged outside Syria—particularly in Western European countries, and Istanbul and Gaziantep (hubs of Syrian emigration in Turkey). In addition to creating aid programs for refugees and support for civic initiatives in the liberated areas inside Syria, core areas of diaspora activism include documenting human rights violations and advocating for transitional justice.[22]

In Egypt, the democratic experiment that started in 2011 with the toppling of long-term dictator Hosni Mubarak was aborted by a military coup. After taking power in 2013, the current president Abdel Fatah Al-Sisi swiftly re-established authoritarian rule. Showing no tolerance for any form of political dissent, Sisi's government has engaged in wide-spread and systematic human rights violations.[23] New legislation severely curtailed space for media and nongovernmental organizations and, in 2019, a constitutional amendment granted the president broad powers undermining the independence of the judiciary.[24] Suffocating conditions pushed people of diverse orientations and backgrounds out of the country. Supporters of the Muslim Brotherhood, liberal intellectuals, and young secular activists all left in a wave of political emigration unprecedented in recent Egyptian history. Despite an often traumatizing experience of state repression and exile, recent diaspora members have continued their engagement in political activism, human rights advocacy, and media reporting.[25]

In all three countries, the forced exit of dissidents and activists appeared to be a deliberate strategy of state authorities. An Egyptian human rights defender who was interviewed for this report noted that the government was pleased to see activists leave as a consequence of the intimidating atmosphere: "*They know that these people will be vocal abroad but at least they got rid of them inside the country.*"[26] In Syria, explained another respondent, some activists were warned before their immediate arrest so as to have a chance to leave the country. Others who were released until trial after a temporary arrest without clear charges seized the opportunity to flee.[27] Threatened by arbitrary arrest, torture and Kafkaesque judicial procedures, many Iranian activists were also forced into exile.[28] Pushing critical voices out of the territory, however, did not mean that the regimes let go of them entirely. To the contrary, all three governments devised new policies to monitor and control their diaspora and exiled communities.

---

[20] Fischer, M. (2016, August 26). Syria's Paradox: Why the War Only Ever Seems to Get Worse. *The New York Times*. https://www.nytimes.com/2016/08/27/world/middleeast/syria-civil-war-why-get-worse.html.

[21] Barnard, A. (2019, May 11). Inside Syria's Secret Torture Prisons: How Bashar Al-Assad Crushed Dissent. *The New York Times*. https://www.nytimes.com/2019/05/11/world/middleeast/syria-torture-prisons.html; Human Rights Watch (2012). Torture Archipelago: Arbitrary Arrests, Torture, and Enforced Disappearances in Syria's Underground Prisons since 2011. https://www.hrw.org/report/2012/07/03/torture-archipelago/arbitrary-arrests-torture-and-enforced-disappearances-syrias.

[22] Andén-Papadopoulos, K., & Pantti, M. (2013). The media work of Syrian diaspora activists: Brokering between the protest and mainstream media. *International Journal of Communication, 7,* 22; Stokke, E., & Wiebelhaus-Brahm, E. (2019). Syrian diaspora mobilization: Vertical coordination, patronage relations, and the challenges of fragmentation in the pursuit of transitional justice. *Ethnic and Racial Studies 42*, 1-20.

[23] Amnesty International (2019). Egypt: Gross Human Rights Violations Under President Al-Sisi. https://www.amnesty.org/download/Documents/MDE1202532019ENGLISH.pdf.

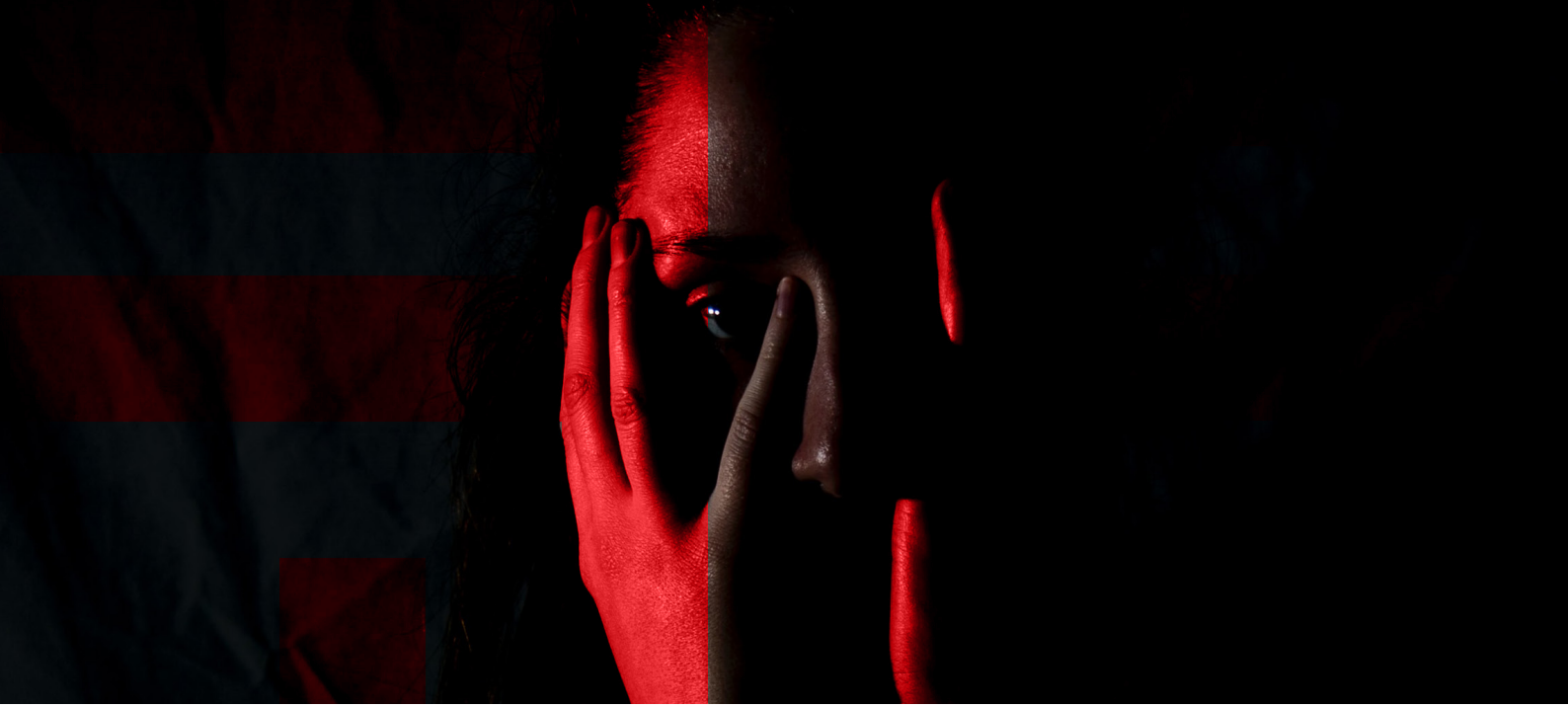
[24] Human Rights Watch (2019, April 2). Egypt: Constitutional Amendments Entrench Repression. https://www.hrw.org/news/2019/04/20/egypt-constitutional-amendments-entrench-repression.

[25] Dunne, M., & Hamzawy, A. (2019). Egypt's Political Exiles: Going Anywhere but Home. Carnegie Endowment for International Peace, Washington. https://carnegieendowment.org/files/Dunne_Hamzawy_EgyptExiles_final.pdf; Matthies-Boon, V. (2017). Shattered worlds: Political trauma amongst young activists in post-revolutionary Egypt. *The Journal of North African Studies, 22*(4), 620-644.

[26] Interview E2, November 2018.

[27] Interview S5, October 2018.

[28] Gholamhosseinpour, M. (2019, February 18). Civil Rights Activists Systematically Forced to Emigrate. *Iran Wire*. https://iranwire.com/en/features/5861.



THREATS BEYOND BORDERS: REGIME MOTIVES AND CAPABILITIES

REGIME MOTIVES

The governments of Iran, Egypt, and Syria all have the political will and capacity to repress dissidents abroad. They extend the influence of their security apparatus across borders using embassies as outposts, activists' in-country relatives as proxies, and digital technologies as tools of surveillance and harassment. The most important assets of diaspora activism—the capacity to mobilize public attention and maintain close ties to the home country[29]—are also key triggers for repressive interventions as regimes feel provoked by the transnational influence and networks of individuals, groups, and organizations opposing them from afar.

After the popular mobilizations of 2009-2011, rulers in the Middle East and North Africa have been wary about the destabilizing role of social media-fuelled protests aided by international civil society and diaspora communities. Western support for projects of democracy promotion and Internet freedom were perceived as threats to regime stability. Learning from recent experiences, regimes in the region have gone through different stages of "upgrading" to strengthen their resilience.[30] In particular, they have built sophisticated systems of Internet censorship while exploiting digital technologies for purposes of surveillance, propaganda, and disinformation. Regime capabilities for Internet control have developed in line with the global securitization of online space and the diffusion of powerful surveillance tools provided by a private sector catering to the needs of intrusive states.[31]

Authoritarian rulers are generally confronted with a "twin problem of uncertainty" in which they are never fully sure about potential threats to regime stability, nor the actual success of their strategies to prevent such threats.[32]

---

[29]Koinova, M. (2012). Autonomy and positionality in diaspora politics. *International Political Sociology, 6*(1), 99-103; Tufekci, Z. (2013). "Not this one" social movements, the attention economy, and microcelebrity networked activism. *American Behavioral Scientist, 57*(7), 848-870.

[30]Bank, A., & Edel, M. (2015). Authoritarian regime learning: Comparative insights from the Arab uprisings. *GIGA Working Papers*. https://www.giga-hamburg.de/de/system/files/publications/wp274_bank-edel.pdf; Heydemann, S., & Leenders, R. (Eds.). (2013). *Middle East Authoritarianisms: Governance, Contestation, and Regime Resilience in Syria and Iran*. Stanford University Press.

[31]Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance: A Review of Multilateralism and International Organizations, 18*(3), 339–361; Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics, 13*(01), 42–54.

[32]Schedler, A. (2013). *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism Oxford University Press*, p. 21

They rely on powerful security agencies and systematic surveillance to detect and contain challenges to their power. They also invest significant effort in information controls to suppress criticism and promote narratives legitimizing their position, both at home and abroad. Authoritarian regimes draw—and carefully guard—"red lines" around topics and activities considered politically sensitive.[33]

Interviews with respondents revealed some of these lines which, if crossed, risked provoking a response from state agents. Topics included regime figures, security agencies, political prisoners, torture, corruption, economic problems, and ethnic and religious minorities. Several interviewees ended their list of taboo topics by essentially saying "*everything is a red line*" and, ultimately, "*you better not talk at all*." Notably, these "red lines" can shift at any moment depending on the specific situation and context. This arbitrary exercise of power is an inherent feature of authoritarian rule, promoting fear and self-censorship among citizens—even across borders. One Egyptian human rights defender summarized the motives behind his government's crackdown on civil society as follows:

"*Part of the obsession of this regime and of Sisi himself is establishing a narrative. They just want one narrative and nothing else. Anyone who promotes a different narrative is a threat to stability.*"[34]

Despite the unpredictability of authoritarian repression, interviews revealed that these regimes aim to cut off two particular resources for diaspora activists: access to public attention, and linkages into their home country. Activists and journalists in the diaspora can act as "information brokers," channelling knowledge and ideas across borders, raising awareness, and leveraging different audiences against the regime. With close ties to peers in the country, they can help to publicize and frame demands, scale up criticism, and provide support to people on the ground.[35] Individuals and groups with influence over international or domestic publics are thus more likely to become a target of transnational repression—not only because they are more visible, but also because they are able to mobilize public opinion against the regime. At the same time, regimes target the links activists maintain to the home country in order to undermine relations between people inside and outside the country.

Not only is transnational repression triggered by the specific activities of diaspora activists and their influence, it is also shaped over time by a regime's international relations, domestic politics, and available resources. The Egyptian government, for instance, is particularly sensitive about human rights advocacy that risks harming its international image, especially vis-à-vis the United States and the European Union due to its reliance on military and economic aid. Less dependent on international support, the Iranian regime targets journalists working in influential news channels, such as the BBC Persian and Radio Farda (Radio Free Europe) due to their role in providing alternative information to audiences inside Iran. In addition, threats against the Iranian diaspora have intensified during election periods and surrounding the conflict over the country's nuclear program.[36] In the case of Syria, some respondents observed that regime attention to outside activism dropped during the critical phase of the civil war, but that threats against the diaspora increased again after the Assad regime regained control over strategic portions of the country.

[33] Glasius, M. et al. (2017). *Research, ethics and risk in the authoritarian field*. Palgrave Macmillan, Chapter 3.

[34] Interview E16, June 2019.

[35] Keck, M. E., & Sikkink, K. (1998). *Activists beyond Borders: Advocacy Networks in International Politics*. Ithaca/New York: Cornell University Press.

[36] The Iranian regime often heightens its controls of information and dissent around critical events, such as elections. Deibert, R., Oliver, J., & Senft, A. (2019). Censors get smart: Evidence from Psiphon in Iran. *Review of Policy Research, 36*(3), 341-356.

REGIME CAPABILITIES AND DIGITAL THREATS

Digital technologies have enhanced the capabilities of regimes seeking to engage in extraterritorial repression by enabling new tactics and and influencing established ones. Prior to the advent of the Internet, authoritarian regimes sought to control the activities of political exiles through propaganda campaigns, espionage, kidnappings, and assassinations.[37] Now, in today's world of intense cross-border communication and information exchange, these regimes have even more opportunities to monitor and respond to the activities of diaspora activists on a rapid and large scale.

The governments of Egypt, Syria, and Iran have all created comprehensive systems of Internet censorship and surveillance with infrastructures propped up by the burgeoning global market for surveillance technology and information controls. Despite sales restrictions and export controls, all three regimes have obtained sophisticated technology to build architectures of mass surveillance capable of tapping into landline and mobile phone communications and intercepting Internet traffic. Egypt, in particular, has enjoyed relatively unrestricted access to the market for surveillance technology. In line with its multisided international relations, the Egyptian government has acquired equipment from German, Italian, French, and US-American manufacturers, and received technical support and training from China.[38] In 2017, the United Arab Emirates transferred to Egypt a state-of-the-art surveillance system made by the French company Amesys.[39] And in 2018, it was revealed that the Egyptian government had used the notorious spyware Pegasus produced by the Israeli NSO group.[40]

Despite both countries being placed under various sanction regimes, Iran and Syria have still found ways to circumnavigate export controls and purchase Western technology for mass monitoring of communications. In the years leading up to the 2011 uprising, Syria established a nationwide surveillance system with equipment of German, Italian, and US-American origin.[41] In Iran, repression against the protests of the Green Movement in 2009 revealed the authorities' use of monitoring technology produced by Nokia Siemens.[42] With tightening sanctions and export controls, Iran has turned to China for surveillance technology and know-how.[43]

In terms of offensive information controls, the governments of Egypt, Syria, and Iran have all engaged in a range of digital attacks against civil society, both inside and outside their territories. The technical underpinnings and background of these campaigns have been documented in detail.[44]

[37] Shain, Y. (1989). *The Frontier of Loyalty Political Exiles in the Age of the Nation-State*. London: Wesleyan University Press.

[38] International Federation for Human Rights (2018, July 2). Egypt: A repression made in France. https://www.fidh.org/en/issues/litigation/egypt-a-repression-made-in-france; Privacy International (2019). State of Privacy in Egypt. https://privacyinternational.org/state-privacy/1001/state-privacy-egypt; Weber, V. (2019). The Worldwide Web of Chinese and Russian Information Controls. Centre for Technology and Global Affairs, University of Oxford. p. 13. https://ctga.web.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf.

[39] Mada Masr (2017, July 5). UAE transfers internet surveillance system bought from French company to Egypt: Télérama. https://madamasr.com/en/2017/07/05/news/u/uae-transfers-internet-surveillance-system-bought-from-french-company-to-egypt-telerama/

[40] Access Now (2019, May 20). Shutdowns, surveillance, and censorship: UPR reviews highlight threats to digital rights. https://www.accessnow.org/shutdowns-surveillance-and-censorship-upr-reviews-highlight-threats-to-digital-rights.

[41] Privacy International (2016). Open Season: Building Syria's Surveillance State. https://privacyinternational.org/sites/default/files/2017-12/OpenSeason_0.pdf.

[42] Center for Human Rights in Iran (2010, October 6). Shirin Ebadi: Nokia Siemens action a major accomplishment for Iranians and for the people of the world. https://www.iranhumanrights.org/2010/10/shirin-ebadi-nokia-siemens-action-a-major-accomplishment-for-iranians-and-for-people-of-the-world/.

[43] Stecklow, S. (2012, March 22). Chinese firm helps Iran spy on citizens. Reuters. http://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322.

[44] Fire Eye (2015). Behind the Syrian Conflict's Digital Frontlines. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf; Scott-Railton, J., & Kleemola, K. (2015). London Calling: Two-factor authentication phishing from Iran. The Citizen Lab, Toronto. https://citizenlab.ca/2015/08/iran_two_factor_phishing; Scott-Railton, J., Marczak, B., Raoof, R., & Maynier, E. (2017). Nile Phish: Large Scale Phishing Campaign Targeting Egyptian Civil Society. The Citizen Lab, Toronto. https://citizenlab.ca/2017/02/nilephish-report/.

Although direct attribution is difficult, it is clear that the security agencies of these countries have established ongoing close relations with groups of threat actors conducting attacks against civil society.

In Egypt, entities involved in digital surveillance and cyberattacks operate under the auspices of intelligence agencies reporting to the president, the military, and the Ministry of the Interior.[45] In Iran, cyberoperations are primarily conducted under the oversight of the Islamic Revolutionary Guard Corps (IRGC), a powerful military and security organization.[46] The governments of both Iran and Syria have utilized cybermilitias (patriotic or state-recruited hackers) for operations conducted against regime opponents. In Syria, the Assad regime relied on different groups of pro-government hackers to help fight the uprising. Most notably, the Syrian Electronic Army (SEA) gained notoriety with aggressive, and at times spectacular, attacks against foreign and opposition targets during the early phase of the conflict. The group also infiltrated the strategic exchanges of rebel fighters.[47] As the conflict evolved, its operations slowed, but in late 2017 the SEA once again resurfaced as the regime's force for online policing and public relations.[48]

The offensive capabilities of these three regimes have developed in response to the Internet's increasing strategic significance for national security, economic well-being, and communication. Cyberattacks have become an important instrument in the geopolitical tensions that mark the region—often reflecting ongoing conflicts between rival countries. Saudi Arabia and Iran, for instance, have launched different forms of attacks against each other, including disinformation campaigns and operations against critical infrastructure.[49] Resourceful state and non-state actors dubbed Advanced Persistent Threat groups use continuous and sophisticated hacking techniques to gain access to information systems and steal or destroy valuable data. They are often identical or overlapping with threat actors targeting civil society. In addition, threat actors from one country occasionally cooperate with groups in other countries to exchange information on targets or outsource operations. For example, threat campaigns in support of the Syrian regime received assistance from both Russia and Iran.[50]

Although Egypt, Syria, and Iran have all invested significant resources in Internet controls and surveillance, the digital security experts interviewed for this report agree that the relative capacities of these countries do not match the level of powerful countries like China and Russia. Nonetheless, all three regimes have significant capacity to threaten civil society, and they continue to invest in expanding these capacities. However, their attacks against civil society are often technically simple, using off-the-shelf or pirated malware and techniques, and relying on the security failures of targets. These threat actors compensate for a lack of technical sophistication with thorough social engineering, which enables them to spread efforts for delivering basic malware in carefully crafted messages.[51]

At the same time, investigations into the technical background of digital attacks against civil society also reveal evidence of constant learning and threat evolution. For instance the "Nile Phish campaign," attributed to the Egyptian government, initially relied on an open-source phishing tool to do its damage.[52]

[45] Privacy International (2019). State of Privacy in Egypt. https://privacyinternational.org/state-privacy/1001/state-privacy-egypt.

[46] Anderson, C., & Sadjadpour, K. (2018). Iran's cyber threat: espionage, sabotage and revenge. *Carnegie Endowment for International Peace*. http://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf.

[47] Franceschi-Bicchierai, L. (2015, April 3). The Syrian Electronic Army's Most Dangerous Hack. *Vice Motherboard*. https://www.vice.com/en_us/article/nze5nk/the-syrian-electronic-armys-most-dangerous-hack.

[48] Abas, A., & Al-Masri, A. (2018, May 17). The new face of the Syrian Electronic Army. *OpenCanada*. https://www.opencanada.org/features/new-face-syrian-electronic-army.

[49] Kausch, K. (2017). Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East. German Marshall Fund of the United States, Policy Brief No. 35, Berlin. http://www.gmfus.org/publications/cheap-havoc-how-cyber-geopolitics-will-destabilize-middle-east.

[50] Harding, L., & Arthur, C. (2013, April 30). Syrian Electronic Army: Assad's cyber warriors. *The Guardian*. https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background; Scott-Railton, J., Abdulrazzak, B., Hulcoop, A., Brooks, M., & Kleemola, K. (2016, August 2). Group5. Syria and the Iranian Connection. https://citizenlab.ca/2016/08/group5-syria/.

[51] Scott-Railton, J. (2016). Security for the high-risk user: Separate and unequal. *IEEE Security & Privacy, 14*(2), 79-87.

[52] Scott-Railton, J.; Marczak, B., Raoof, R., & Maynier, E. (2017). Nile Phish: Large Scale Phishing Campaign Targeting Egyptian Civil Society. The Citizen Lab, Toronto. https://citizenlab.ca/2017/02/nilephish-report/.

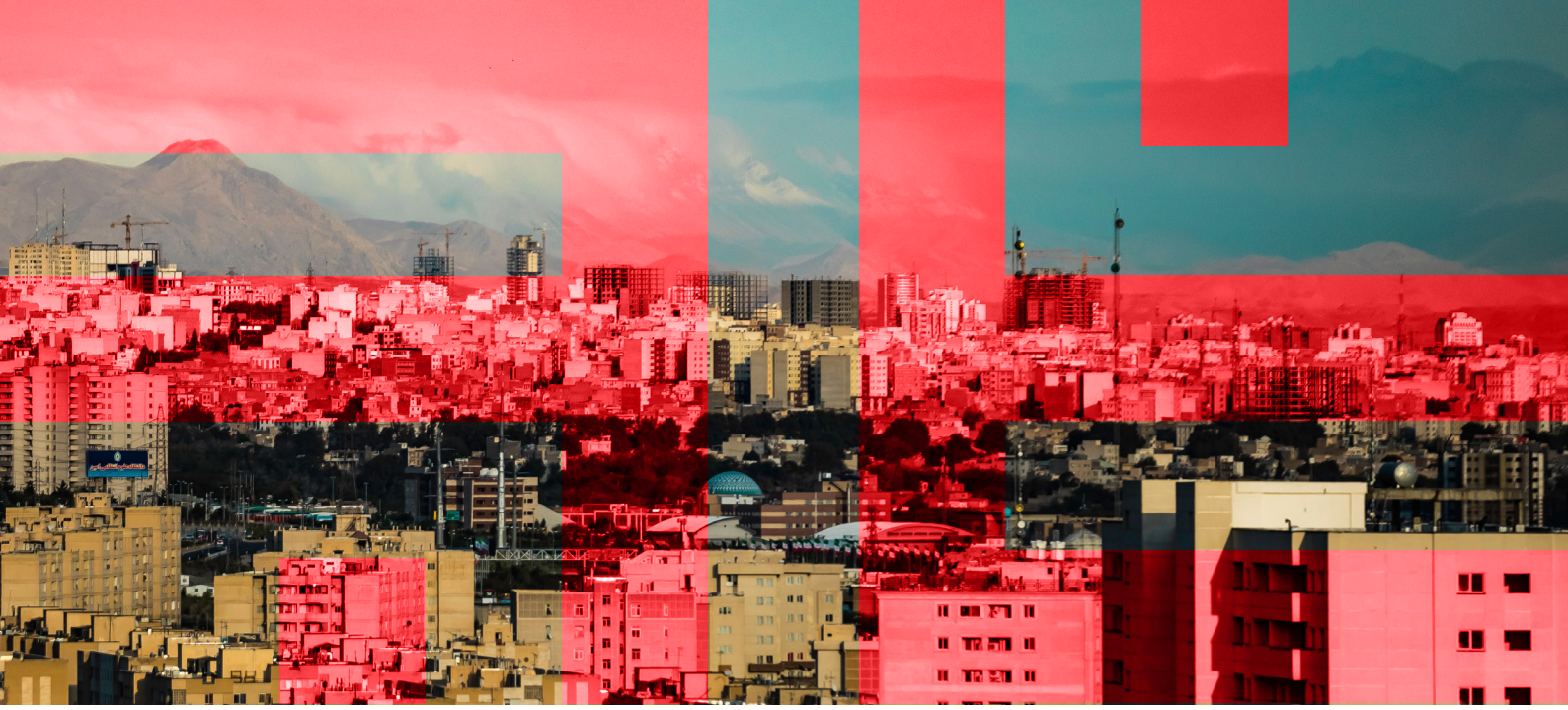
Yet in a more recent attack, perpetrators used a malicious third-party application to gain access to the accounts of their targets.[53] Such a shift illustrates the attackers' ability to adapt as most of their targets among civil society activists have started using two-factor authentication (an additional security hurdle for email accounts that this iteration of the campaign was able to circumvent).[54] Further investigations uncovered that the threat actors behind the operation had even developed new mobile applications to deliver malware and infiltrate the phones of their victims, targeting a number of well-known activists and journalists, including Egyptians living in Canada, Britain, and the United States.[55]

Accordingly, assessing the actual technical capabilities of regimes and devising appropriate security measures is a difficult task for potential targets of digital threats within activist communities. The exact set-ups of targeted and mass surveillance campaigns are often understood by only a small cadre of forensic experts. Activist risk perceptions are therefore often shaped by reports of successful attacks and sophisticated, complex tools of surveillance. As a result, potential targets can easily feel overwhelmed by the projection of unstoppable powerful state actors capable of breaking down all levels of protection. Given this, it is essential to build networks of constant support in digital security and provide civil society with accurate and accessible information detailing the true evolution of state-operated threats.

[53] Amnesty International (2019, March 6). Phishing attacks using third-party applications against Egyptian civil society organizations. https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations.

[54] Guarnieri, C. (2019, March 8). Phishing attacks using third-party applications against Egyptian civil society organizations. https://nex.sx/blog/2019/03/08/phishing-attacks-against-egyptian-civil-society.html.

[55] Bergman, R., & Walsh, D. (2019, October 3). Egypt is using Apps to track and target its citizens, report says. *The New York Times*. https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html.



A TOOLKIT OF TRANSNATIONAL REPRESSION

Authoritarian regimes use a "toolkit" of repressive practices to control and contain activists abroad. Digital technologies are key to all mechanisms of transnational repression as they allow regimes to monitor and respond to diaspora activism with greater scope and speed. Digital and non-digital threats against diaspora activists thus tend to be intertwined.

This section of the report details the range of repressive tools utilized by Egypt, Syria, and Iran. These include: monitoring and surveillance; account and device hacking; slander, harassment, and disinformation campaigns; online publication hacking; threats from embassies and regime agents; threats against in-country relatives; and threats against property rights. Each "tool" is detailed below.

MONITORING AND SURVEILLANCE

State actors aim to gain influence and control through the systematic collection of personal details and information. Most surveillance targeting diaspora and exiled communities takes place online. Digital communication technologies are essential tools for diaspora activists who communicate with contacts and relatives in the home country, maintain work relations across countries and communities, and publish information on different platforms. As avid users of social media and other online channels, activists leave potential clues related to their current activity, travel, conference participation, friends, and collaborators. With professional and personal lives converging on social media, threat actors find ample opportunity to gather open source intelligence: publicly available information collected and exploited for the purposes of intelligence and security agencies.[56]

In general, the use of digital communication technologies exposes diaspora activists to monitoring and surveillance. Communication with contacts inside the home country creates opportunities for messages to be intercepted because their content, at least partly, travels through infrastructure under regime control. Additionally, social media profiles provide information on the activities and social relations of targets which can then be used for social engineering, activist network profiling, and malware attack preparation. This information is also useful for other forms of transnational repression, such as harassment of in-country relatives and disinformation campaigns. In addition, intelligence agencies monitor the programs of international and exiled media, tracking the work of journalists and media appearances of activists in the diaspora.

[56]Bazzell, M. (2016). *Open source intelligence techniques: resources for searching and analyzing online information*. CreateSpace Independent Publishing Platform; Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies, 18*(4-5), 530-547.

These agencies also still rely on classic methods of spying through informants linked to embassies who infiltrate activist groups and attend events involving members of the diaspora. Using these different channels, regime authorities are able to follow closely the activities of dissidents abroad and prepare interventions of control and repression.

In addition to these forms of "silent" monitoring and harvesting of intelligence, interviewees reported they occasionally received signals that monitoring was taking place. A Syrian journalist and an Egyptian activist in Germany, for instance, both reported that state agents in their home countries questioned their parents or colleagues after they appeared on the Arabic television program of Deutsche Welle. Other Syrian journalists interpreted the swift filtering of any new online publication as a sign that regime authorities kept a close eye on the media activities of exiles. Smear campaigns in state-controlled media referring to recent activities, as well as comments and trolling on social media profiles, made activists from all three countries understand they were being watched. Such forms of not-so-hidden monitoring clearly aim to have a silencing effect, shaping and restricting the behavior of targeted communities by making it known that state authorities have taken an interest in their actions.

ACCOUNT AND DEVICE HACKING

Hacking into computers, mobile devices, and personal accounts such as email and social media has become a common technique for targeted surveillance in repressive contexts.[57] This proliferation of more aggressive information gathering tactics can be seen as a response to the heightened security awareness among activists who increasingly resort to email encryption and other protections against surveillance. As a result, threat actors seek to compromise devices and accounts to gain access to a trove of private information, communications, and contacts.[58]

Such attacks often involve some form of social engineering, with perpetrators working to trick targets into opening a malicious link or attachment by impersonating a friend or an organization linked to their field of expertise (or offering otherwise interesting information). The malware, once successfully executed, provides access to a target's device or reveals confidential passwords. As noted in the prior section of this report, threat actors tied to the governments of Egypt, Syria, and Iran have engaged in phishing campaigns against civil society on a large scale, both inside and outside their territories. Respondents reported attempts to compromise their devices and accounts as one of the most common threats they face. As a leading editor in an Iranian exile media organization explained:

"*There is no day when I open my email and I don't have a phishing email. Yesterday I received a message from Google telling me that they couldn't deliver one of my messages. For more details I should click.*"[59]

Interviews revealed attackers attempt to deliver malware in multiple ways, using not only email but also messages on Facebook, WhatsApp, and Telegram. Iranian digital security experts explained that threat actors often try to compromise the accounts of low profile and inexperienced users in activist networks—or even family members—in order to gain access to approach more valuable targets. Iranian intelligence agencies have also used the identities of individuals arrested inside the country to swiftly approach the arrested individual's list of contacts before the arrest became public. Other respondents mentioned phishing attempts carried by invitations to seminars, files on human rights violations, and information on recent bombing raids in Syria, among others.

[57] Citizen Lab (2014). Communities @ Risk: Targeted Digital Threats against Civil Society. https://targetedthreats.net.

[58] Guarnieri, C. (2015, August 16). Helping the Helpless: Targeted Threats to Civil Society. Talk at the Chaos Communication Camp. https://media.ccc.de/v/camp2015-6848-helping_the_helpless.

[59] Interview I11, January 2019.

Targeted digital surveillance allows regime agents to reach targets irrespective of their geographic location. The success of an attack depends on the effort and resources invested in its execution and technical underpinnings, as well as the target's security awareness. Interviewed experts agree that attacks on Iranian, Syrian, and Egyptian diaspora communities are not technically sophisticated but instead built on increasingly clever social engineering. This form of attack requires only a core group with technical expertise, allowing for easier scalability in the ranks of attackers packaging and sending out malware.[60]

Phishing campaigns rarely target only one specific individual. Instead, they build on the ties among activists in seeking to unravel entire groups and networks. Compromising the confidential information of one individual allows attackers to uncover new links and contacts which can then be used to swiftly expand their efforts while also potentially de-anonymizing in-country collaborators. The existence of this type of threat thus not only stresses individual activists seeking to protect their private information, but also increases pressure on whole communities.

SLANDER, HARASSMENT, AND DISINFORMATION CAMPAIGNS

Regimes and regime supporters use false and distorted information and verbal threats to pressure, silence, and taint the reputation of diaspora activists. Online harassment and disinformation against exiled dissidents can take various forms.

In Egypt, broadcast media affiliated with the Sisi government have published direct threats against dissidents abroad. Prominent human rights defender Bahey el-Din Hassan and opposition leader Ayman Nour, for instance, were labelled as traitors on television shows calling for them to be kidnapped and killed.[61] In another example, physical harassment of activists abroad was combined with slander in state-aligned media: after Egyptian participants in a workshop on human rights in Italy were followed and photographed by unknown men, pictures of the event resurfaced in TV programs in Egypt alleging that they were plotting against the country.[62] An Egyptian civil society activist emphasized the psychological pressure these programs put on exiled dissidents:

"*Imagine you are living in Europe, in exile, and some fanatic Egyptian recognizes you from this media show. It puts your life in danger, you always have to be careful about your moves.*"[63]

In Iran, dedicated websites and social media channels closely follow and dissect the content of external media programs to contradict their reporting and attack their staff. Some websites even copy the design of outside media, such as BBC Persian and Radio Farda, only to mock and falsify the content of the original. These duplicates have also published rumours about staff members and private details obtained from tapping the communication between outside journalists and in-country contacts or relatives. The editor of a popular Iranian news media underlined the principal aim of the publications:

"*This is of absolutely no interest to anyone. (...) The only target of this publication is me: to show me that I have to be careful, that they are watching me.*"[64]

[60] See also: Scott-Railton, J. (2016). Security for the high-risk user: Separate and unequal. *IEEE Security & Privacy, 14*(2), 79-87.

[61] Euromed Rights (2018, April 18). Death Threats against CIHRS Director, Bahey el-Din Hassan. https://euromedrights.org/publication/death-threats-against-cihrs-director-bahey-el-din-hassan/; Middle East Eye (2018, October 10), Exiled Opposition Leader Expresses Fear after Khashoggi Disappearance. https://www.middleeasteye.net/news/exiled-egyptian-opposition-leader-expresses-fear-after-tv-death-threats-1398361292.

[62] Euromed Rights (2017, May 23). Extreme Concern about the Harassment of Egyptian Human Rights Defenders in Italy. https://euromedrights.org/publication/extreme-concern-harassment-egyptian-human-rights-defenders-italy.

[63] Interview E9, January 2019.

[64] Interview I15, March 2019.

The same journalist also recounted when a fake weblog published under his name compiled his actual articles and writings for months only to eventually publish a false statement in which he allegedly regretted having interviewed members of an armed separatist group, which would have contradicted the policies of the media organization. Shortly after, in one of his live programs, a caller from Iran even brought up the blog to criticize the editor.

Iranian state media devote persistent attention to well-known journalists and human rights defenders abroad, portraying them as liars, questioning their loyalty, and accusing them of working for foreign powers. False reports about sexual relations and rape among outside journalists are also common. These smear campaigns aim to undermine the credibility of dissidents and critics from abroad, targeting their relationship with domestic audiences. The campaigns are also used as a form of psychological pressure: the sister of prominent women rights activist Masih Alinejad, for instance, was coerced by Iranian authorities to publicly disown Alinejad on state television.[65] Although Iranian interviewees questioned whether these methods had the desired effect of silencing diaspora activists, they agreed that slander and lies were a form of harassment sapping their focus and energy. As an Iranian journalist explained:

"*They create a playing field and you are forced to play along their rules. They attack and you have to defend yourself. You spend time for nothing. Only responding to their lies. You spent time that you could have used for writing articles*." [66]

In addition to attacks in official and state-affiliated media, diaspora activists experience intimidation and harassment on social media. Interviewees experienced threats in their social media feeds of physical violence, assassination, and arrest upon return to the country. Threats were also issued against their family members. An Iranian journalist reported that an online comment under one of her articles threatened her uncle in Tehran, even mentioning his home address. While some of these attacks appear to be coordinated by the government, others simply come from regime supporters.

Online harassment and threats against female journalists and activists warrant specific mention here. The rise of online gender-based violence and attacks against women on social networks has been observed in many different contexts.[67] Every female respondent reported receiving sexualized, degrading, and misogynistic comments and threats through online channels. One Iranian journalist stressed:

"*If you search my name, you will find the ugliest insults*."

And although online trolling and cyberbullying is used by regime agents and supporters to target and silence female activists, interviewees also emphasized that they felt they were struggling against conservative male-dominated societies in general, in which men turn against outspoken women and push them out of the conversation.

ONLINE PUBLICATION HACKING

In an effort to shut down online criticism, regimes target the publications of outside media and dissidents. Brute attacks such as defacements and DDoS-campaigns that make websites unavailable were mentioned by respondents, but these types of attacks appear to be less common—or at least less successful—than a few years ago. Now that many civil society organizations have shifted to social media to publish their information and stories, threat actors have begun to rely on false reports and spamming comments from bots to block profiles. For example, two members of an Egyptian human rights campaign mentioned that their Facebook event page for European protests against the Sisi government was blocked due to massive false reports from government supporters classifying the event as sexual harassment.

[65] Alinejad, M. (2018, July 31). My sister disowned me on state TV. *The New York Times*. https://www.nytimes.com/2018/07/31/opinion/iran-hijab-feminist.html.

[66] Interview I12, February 2019.

[67] Amnesty International (2018). Toxic Twitter – A toxic place for women. https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1

According to a digital security expert, these types of attempts to disrupt online expression are more prevalent in times of political tension, protests, or elections.

THREATS FROM EMBASSIES AND REGIME AGENTS

Serving as outposts for security agencies, embassies and consulates provide different methods to monitor, control, and threaten diaspora activists. Consular services—such as passport renewal or the issuing of birth certificates—give regime authorities an opportunity to gather information and gain leverage over citizens abroad. A Syrian respondent reported that he underwent questioning by an employee of the embassy who eventually refused to renew his passport under an arbitrary pretext. Another activist recalled her hesitance to provide the Syrian embassy with her current address to receive documents by mail. A third Syrian interviewee decided to forgo the request for a renewed passport altogether, and instead filed an application for asylum in the host country.

Because embassies also serve as voting stations for overseas citizens, national elections provide another opportunity for regimes to monitor political opposition in the diaspora. Egyptian respondents expressed fear that their voting behaviour in prior parliamentary and presidential elections had been documented in the embassy and transferred to security agencies in Egypt. One recalled that a fellow activist was arrested upon arrival at the Cairo airport and questioned about having invalidated his ballot in protest when voting in one of Egypt's European embassies during the last parliamentary elections.

Embassy staff also use their position in the host country to spy and disturb political activity in diaspora communities. They participate in public events dealing with the political situation in the home country to bring up government viewpoints or disrupt debates. For one Egyptian respondent, surveillance by regime agents abroad became the reason he chose to not return to the country after he was filmed and threatened by unknown men speaking in an Egyptian dialect at a conference in Italy. Another Egyptian human rights defender explained that consultations at the United Nations in Geneva were used by organizations affiliated with the government to approach and pressure exiled activists. Other Egyptian interviewees mentioned surveillance attempts in restaurants popular among emigrants, as well as possible infiltrations of activist circles by intelligence agents or informants reporting to the embassy. A Syrian respondent pointed out that regime supporters, possibly organized by the embassy, had tried to disturb demonstrations organized by activists in Berlin in order to publicly taint the image of Syrian migrants.

THREATS AGAINST IN-COUNTRY RELATIVES

While attempting to silence, sanction, or retaliate against dissidents living abroad, regime authorities often target relatives still living in the country.[68] These threats can start with *"friendly talks over tea*" and escalate into interrogations, imprisonment, and even torture or assassination. In Syria's context of high repression, just a short visit from regime agents will send a strong signal that authorities are taking note of what the activist is doing outside the country and that they are willing to use relatives as "hostages." A Syrian journalist in an exiled media organization reported that his brother and a colleague were arrested "*to get me back into the country.*"[69] Two years later, the families were informed that both had died in prison. Such extreme measures are not exclusive to Syria. An Iranian journalist and human rights defender suspected that, because of his activities, his brother in Tehran had been pressured and harassed for years by intelligence agents—eventually driving him to suicide.[70]

For regime authorities, threats against families provide a method to escalate extraterritorial repression. This type of "proxy punishment" is primarily used to constrain and retaliate against public activity, such as actions taken by journalists in influential news organizations or human rights advocates who have appeared in international media.

[68] Moss, D., Michaelsen, M., & Kennedy, G. Going after the family: Diaspora activism, transnational repression, and proxy punishment. Manuscript to be submitted.

[69] Interview S4, October 2018.

[70] Interview I8, December 2018.

Authorities seem to be particularly sensitive about the influence that more outspoken and public figures gain over audiences in host and home society. The Iranian authorities, for instance, systematically harass and threaten the families of staff at the BBC's Persian service and other external Iranian news media. Family members have been regularly summoned and interrogated by different organizations of state security. The sister of a BBC journalist was even held in prison for 17 days to force the journalist into an interrogation via Skype.[71] Authorities have also cancelled passports and exit permits of parents scheduled to visit their children working as journalists abroad. One respondent even mentioned attempts to recruit more distant family members to spy on journalists or to provide personal information that could be used for further pressure:

"*This is very terrible because you will always have a doubt in the back of your mind when this friend or that relative is visiting or getting in touch with you, if they might be recruited by the intelligence agencies.*"[72]

In 2017, the BBC filed an official complaint to the UN Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion as well as to the UN Special Rapporteur on human rights in Iran. This was the first time the BBC engaged with the UN over the protection of its journalists. In the process, UN Secretary-General Antonio Guterres expressed his concern over the persecution of BBC staff by the Iranian authorities, and the European parliament condemned the harassment of journalists and their families.[73]

Respondents from Egypt, Syria, and Iran all feared for their relatives back home. These threats place diaspora activists in an critical position where they must decide between protecting their loved ones or pursuing their profession. As one Syrian respondent put it:

"*This is the first nightmare for any activist.*"[74]

By moving against in-country relatives, regimes jeopardize the autonomy and freedom activists enjoy abroad. In the words of another Syrian activist:

"*It is an intimidation that puts huge pressure on activists outside. It is not their lives anymore, it is not their freedom anymore. I am free to express my opinion but not if it causes harm to other people. If it causes harm to me, I am responsible for myself. But I cannot be responsible for the harm on other people.*"[75]

Targeting families is one of the most effective tools to contain and silence dissidents abroad. While repressive rulers have never hesitated to punish the kinship of their opponents, today's threats against in-country relatives of political emigrants build on intense cross-border ties sustained by digital communications. In this manner, regime agents are able to closely monitor activists and journalists beyond their borders—and come up with swift responses. Such actions are made all the more effective because exiled activists quickly learn about threats to their families and then must evaluate the risk that the continuation of their activities entails for both them and their loved ones.

[71] Saremi, N. (2017, October 28). Iran's Persistent Attacks on BBC Persian Journalists. *Iran Wire*. https://iranwire.com/en/features/4934.

[72] Interview I15, March 2019.

[73] BBC Media Centre (2019, March 12). UN Special Rapporteur "deplores" the persecution of BBC Persian staff and their families. https://www.bbc.co.uk/mediacentre/latestnews/2019/persian-un; Greenslade, R. (2019, March 17). Iran's threats to BBC Persian staff must be confronted. *The Guardian*. https://www.theguardian.com/media/commentisfree/2019/mar/17/irans-threats-to-bbc-persian-staff-must-be-confronted.

[74] Interview S10, January 2019.

[75] Interview S5, October 2018.

THREATS AGAINST PROPERTY RIGHTS

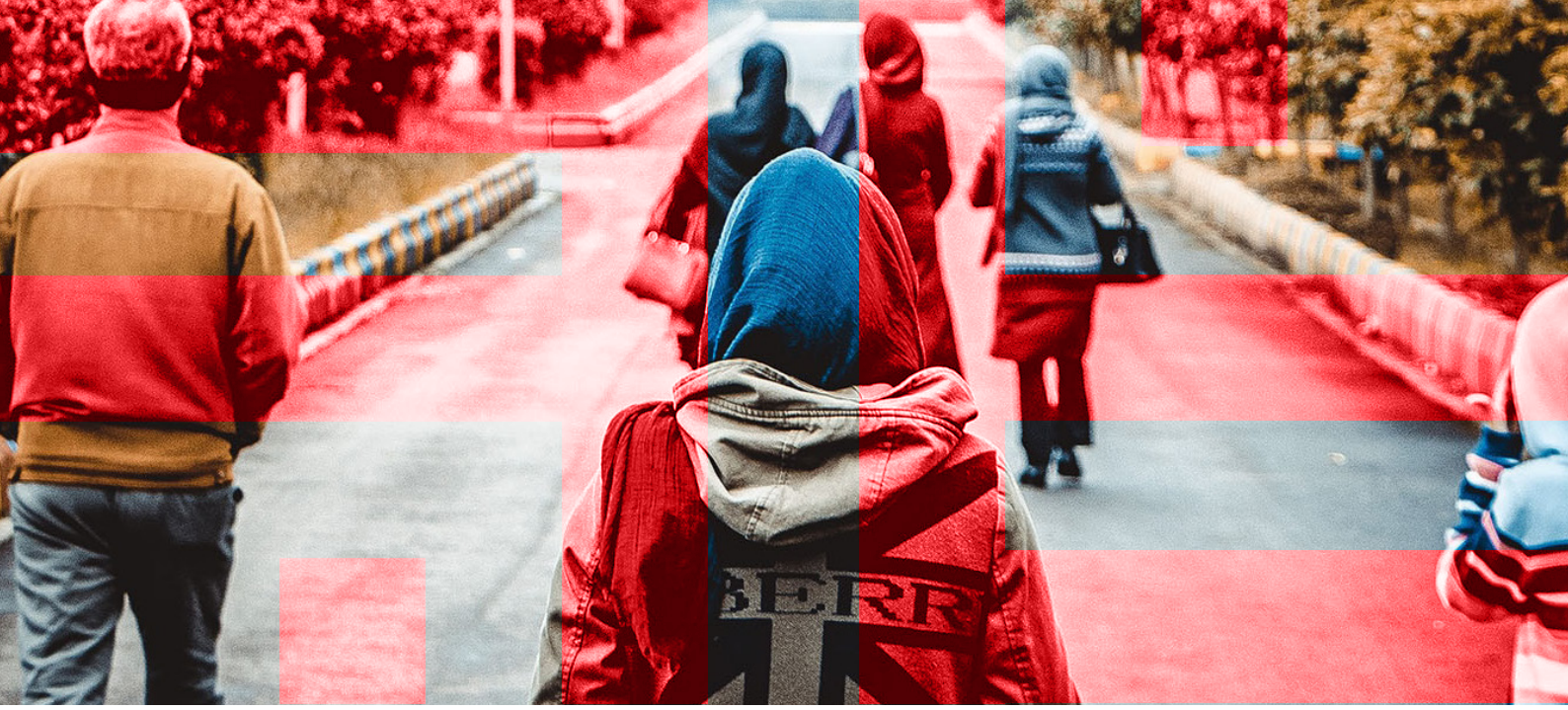
State authorities confiscate property and freeze assets of emigrants and diaspora activists to punish them for criticizing or opposing the regime. For example, Iranian authorities, in an August 2017 court order, accused 152 staff members and contributors of the BBC Persian service of acting against national security and froze their assets inside the country. This prevented current and former BBC employees from Iran to buy or sell property, claim family inheritance, and conduct other administrative affairs.[76]

Similarly, the Syrian government has seized land, houses, and capital of citizens associated with the opposition movement who fled the country during the course of the civil war. In doing so, the regime destroys official property documentation and the assets fall into the hands of the government for redistribution to the advantage of its supporters. This process thus excludes parts of the population from any process of reconstruction, effectively preventing their return and banning them from the territory as a form of punishment for their lack of loyalty.[77] Property confiscations in Syria have also specifically targeted political activists, journalists, and intellectuals (partly using broadly formulated counter-terrorism legislation). Law No. 10, passed in 2018, entitles the government to expropriate residential areas for the purpose of reconstruction. This law, however, has been applied predominantly to neighborhoods known for their opposition to the regime.

In sum, an overview of the most prevalent tools of transnational repression reveals that regimes no longer need to rely on direct physical harm, abductions, or assassinations when attempting to silence critics abroad. Such drastic interventions are not only logistically hard to implement, but can also incur a deterioration of relations with the country hosting targeted dissidents, reputation loss, and other costs. Regimes today operate on a different level of repression when intimidating and harassing diaspora activists, maintaining persistent pressure and permeating targets' everyday routines. Digital technologies have extended the reach and intensity of regime threats across borders. The principal aim of these practices is to silence and punish outspoken dissidents in exile as well as to undermine their cross-border ties by spreading insecurity and mistrust in transnational networks.

[76] Rahimpour, R. (2017, August 15). Iran judiciary freezes assets of BBC Persian staff. *BBC News*. https://www.bbc.com/news/world-middle-east-40936023.

[77] Alrwishdi, D., & Hamilton, R. (2018, April 12). Paying Attention to Land Rights in Syria Negotiations. *Just Security*. https://www.justsecurity.org/54781/paying-attention-land-rights-syria-negotiations; Human Rights Watch (2019, June 28). Rigging the System: Government Policies to Co-Opt Aid and Reconstruction Funding in Syria. https://www.hrw.org/report/2019/06/28/rigging-system/government-policies-co-opt-aid-and-reconstruction-funding-syria; Omari, M. (2019, April 15). Syria's Land Looting Campaign for Reconstruction. *Enab Baladi*. https://english.enabbaladi.net/archives/2019/04/syrias-lands-looting-campaign-for-reconstruction.



THE SILENCING EFFECTS OF TRANSNATIONAL REPRESSION

Even though they reside outside the immediate reach of repressive state authorities, diaspora activists remain exposed to a number of threats from their home regimes. But to what extent do practices of extraterritorial repression actually constrain diaspora activism? The interviews conducted for this report revealed that state authorities are able to pressure activists into self-restraint, undermine their ties to the home country, and put them under tension and stress negatively affecting their mental health. By targeting dissidents and critics across borders, authoritarian regimes thus succeed to impose additional costs on the activities of transnational civil society.

The effects of repression depend as much on how targets perceive the risk of state interventions as on the actual repressive practices experienced by activists.[78] Repressive regimes often try to obscure or exaggerate their capacities, for instance by setting examples through selected cases of drastic or carefully publicized measures against dissidents, so as to scare and silence others. The case of Jamal Khashoggi had such effect even beyond the context of Saudi Arabia: several Egyptian respondents brought up the possibility of Sisi's government engaging in similar targeted assassinations of opponents abroad, especially given the limited international consequences the Saudi government had to face for the implication of its highest officials in the murder of a journalist.

The effects of surveillance, in particular, build on activist uncertainty regarding the capabilities of monitoring authorities. This uncertainty creates an unequal power relation between the watcher and the watched, "giving the watcher greater power to influence or direct the subject of surveillance."[79] When regime agents successfully gather open source intelligence or compromise the email accounts of activists, the threat of continued surveillance expands and morphs into a means of control in and of itself. The knowledge or suspicion of ongoing surveillance can thus have a "chilling effect," constraining the capacity of targets to exercise their fundamental human rights. In particular, "interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression."[80]

[78] Honari, A. (2018). From 'the effect of repression' toward 'the response to repression.' *Current Sociology, 66*(6), 950-973.

[79] Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review, 126*(7), 1934–1965, p. 1953.

[80] United Nations Human Rights Council (2019). Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, p. 7. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf.

This understanding was echoed in the interviews. Although respondents were uncertain about how systematic and coordinated the monitoring from regime authorities actually was, they often assumed it to be comprehensive and permanent. An Iranian human rights defender observed:

"*I don't know how much they actually know about my work (...) but I always assume that they know the details of what I am doing.*"[81]

An Egyptian activist pointed out that all human rights activism inside the country was monitored "*by default*"—therefore he suspected regime authorities were keen to follow activities abroad too.[82]

The lack of precise information regarding the actual tools and resources at the disposal of security agencies exacerbates the silencing effect of surveillance and contributes to the success of repressive tactics across borders. The assumption of continuous online and offline surveillance pushes activists towards various forms of self-restraint. Egyptian human rights defenders who had organized a protest during the visit of President Sisi to Germany explained that some members of their group participated only in disguise, wearing sunglasses, hats or even a wig, in case they were being observed and photographed by security agents. An Egyptian activist who understood through interrogations of peers inside the country that she was on the radar of security agencies after appearing on television said that this knowledge stopped her from following up on invitations for further interviews and media contributions because she was considering to travel back to the country. "*Not only they are surveilling us but we are also surveilling ourselves,*" she observed. She also described conflicts within her group about how to deal with the tension between self-censorship and legitimate security needs.[83]

A women's rights defender from Egypt explained that "*in any seminar or media appearance I will carefully think about how to phrase my sentences*" because "*some topics need to be avoided.*" She also said that despite her long experience as an activist, the regime had successfully "*implant[ed] fear inside me.*"[84] A journalist from Syria, in turn, expressed mixed feelings about the fact that he had never chosen to work under a pseudonym. He said:

"*The whole reason for starting the revolution was to break the fear. So if I live in fear all the time and change my name, then we have done nothing, we lost the country for nothing.*"

At the same time, he admitted that the thought of his parents back in Syria would make him uncomfortable so that he often preferred to keep a "low profile."[85]

UNDERMINING IN-COUNTRY TIES

In addition to curbing freedom of expression, regime surveillance also targets activists' ties to their home country. The security of colleagues and friends in-country is a key concern for many activists. An Egyptian human rights defender emphasized how important and challenging it was to remain connected to contacts back home:

"*This will make both sides more powerful. One target for the government is to isolate people inside from those who are outside. This will make both of them less powerful and less capable.*"[86]

[81] Interview I8, December 2018.

[82] Interview E2, November 2018.

[83] Interview E4, November 2018.

[84] Interview E12, March 2019.

[85] Interview S18, February 2019.

[86] Interview E2, November 2018

Feeling partially responsible for the well-being of in-country contacts, many diaspora activists try to maintain their connections but carefully circumnavigate critical topics or reduce their ties. A Syrian journalist said that he was well-connected to friends and family through different online channels but could not talk freely and tried to "*avoid any political discussions because it can be dangerous for them.*"[87] An Iranian journalist explained that he had limited his relations with friends and colleagues in the country for fear that his communications were monitored and could create problems for anyone he spoke with. He pointed out the consequences of this behaviour:

"*I am giving up on a lot of relations and connections which I need as a journalist to stay in touch with the country. I am not only loosing friends but also access to information sources. Some contacts could provide me with more detailed information or a more precise analysis. I cannot access these sources and the quality of my work suffers.*"[88]

Surveillance of contacts can thus prevent effective collaboration between activists inside and outside a country. An Egyptian human rights defender who was preparing exchanges between civil society representatives in Cairo and visiting members of parliament from an EU-country discovered his communications must have been monitored because all his in-country contacts received threats from security agencies to not proceed with the meetings. The risks entailed for people inside the country force many to reduce or end their collaboration with activists in the diaspora. As a result, exiled journalists explained they were unable to quote sources by name, while others deliberately refrained from working with in-country contributors.

Threats against family members are the most effective means to force activists into self-restraint and undermine their ties to the home country. A Syrian activist emphasized that anybody with family in Syria was effectively prevented from using all opportunities of exile activism:

"*I cannot be a kind of public activist, I cannot speak out in my real name. I cannot do something that puts international pressure on the regime. Even though I am heavily involved, I have no full freedom of movement. I have to define limits.*"[89]

MENTAL PRESSURE AND STRESS

The targeting of in-country relatives also highlights how practices of transnational repression put exiled dissidents under enormous mental pressure and raise the emotional costs of activism from afar. An Iranian journalist working for a big media organization heavily targeted by harassment against the families of its staff noted that stress and depression had increased among colleagues, changing the atmosphere in the office.

"*This is exactly what they want: create tension and conflict in our workplace. They want to disturb outside media, influence our work, the decision to publish some news or not, or the way we present news.*" [90]

[87] Interview S1, September 2018.

[88] Interview I12, February 2019.

[89] Interview S10, January 2019.

[90] Interview I6, December 2018.

In addition to tensions within diaspora groups and organizations, repression against relatives puts the relations between activists and their families under strain. An Egyptian human rights defender said that after his father had been taken to the police station for two nights, "*my father and my brother called me and for the first time they were against my activism. They were angry against me, telling me I am a coward, I am safe and putting them in danger.*"[91]

The Iranian journalist mentioned above chose to take some of the pressure off his family by portraying a strained relationship, at least on the surface:

"*In telephone calls I talked very loudly and sometimes not very politely to my father. I told him that my work was none of his business and he could not interfere. To let them know that they couldn't get to me through my father. To some extent it helped. My father told them that his son was not listening, that he had told me to stop my work but I wouldn't listen.*"[92]

Another Iranian journalist pointed out that dedication, experience, and solidarity among staff in the media organization helped them resist the pressure resulting from the harassment of their families.

"*The people we are talking about know the methods of the Islamic Republic, they work and report on its human rights record. They all know that if they step back, the pressure will not stop. The authorities will know that they have found the soft spot and will move forward step by step.*"

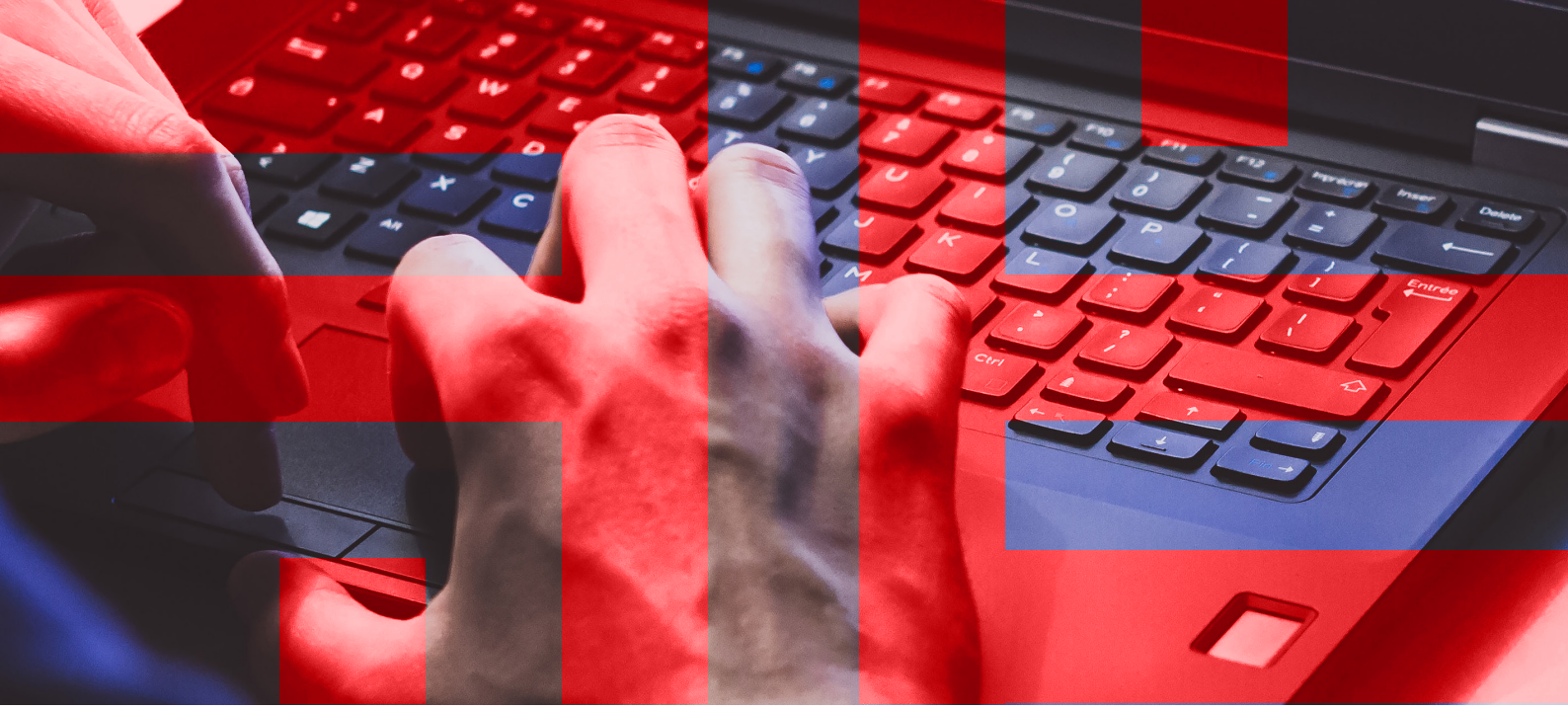
While he insisted that the reporting of the team had not changed as a consequence of threats against their relatives, he also emphasized the psychological impact of the pressure. Knowing that parents were targeted by the Iranian intelligence, he said, would "*leave everybody trembling.*"[93]

The insights provided above show that the repressive tactics employed by authoritarian states affect exiled dissidents, but do not necessarily deter them from their actions. Nonetheless, by reaching across borders with different tools of transnational repression, regimes are able to influence the everyday routines of activists and constrain some of the dynamics, impacts, and outreach of diaspora activism.

[91] Interview E6, November 2018.

[92] Interview I6, December 2018.

[93] Interview I15, March 2019.



DIGITAL SECURITY PRACTICES AMONG EXILED ACTIVISTS

Diaspora activists benefit tremendously from digital technologies. Online tools help them exchange information, connect, coordinate, organize, and mobilize across countries and borders. Yet the extensive use of digital technologies also entails risks. Networked online communication creates multiple points of exposure that threat actors can exploit to compromise confidential information and private data. According to digital security researcher John Scott-Railton, "the capacity to connect has vastly outpaced the ability to secure." [94]

Activists rely on tools and platforms not designed to operate securely within high-risk contexts in which resourceful state actors seek to gather confidential information, penetrate groups and networks, and identify online dissenters to punish them. Now more than ever, activists need to work harder to protect their privacy and secure their data in this environment of rapidly evolving technologies and threats. Although information on digital security has increased in recent years, actual knowledge on risk mitigation and changes in user behaviour still vary considerably across communities and contexts.

UNDERMINING IN-COUNTRY TIES

Both immediate experience with threats, as well as "stories of security incidents spreading through peer groups, organisations and networks," play an important role in raising risk awareness and the adoption of security practices amongst activists.[95] An Iranian digital security expert confirmed that the attacks against civil society in the diaspora during recent years contributed to improving strategies of risk mitigation. Yet not all activists have taken steps to improve their safety. Several Syrian trainers for digital security deplored the fact that individuals who did not feel directly threatened by regime authorities (such as those living outside the country or in areas liberated from regime control) often considered themselves to be out of reach and therefore did not adopt adequate digital security practices. The trainers emphasized that some of these individuals had limited awareness on how their data and accounts could be used to put others at risk—not simply themselves.

[94] Scott-Railton, J. (2016). Security for the High-Risk User: Separate and Unequal, p. 2. https://www.johnscottrailton.com/security-for-the-high-risk-user.

[95] Kazansky, B. (2016). Digital Security in Context: Learning How Human Rights Defenders Adopt Digital Security Practices. Project report, p. 25. https://secresearch.tacticaltech.org/media/pages/pdfs/original/DigitalSecurityInContext.pdf.

Translating knowledge about potential risks in the digital environment into actual practices of data and privacy protection is not a straightforward process. Activists often do not have the time, resources, or capacity to make security practice decisions based on nuanced risk assessment. And when they do try to do so, they may find certain tools and practices too cumbersome to use. Critically, individuals' approaches to communication technologies are shaped by their expectations, attitudes, and perceptions as much as by the technical configuration and usability of tools and applications. Users develop "mental models" to process information systems and guide their evaluation of risks and risk mitigation.[96] As sociologist David Lyon notes, ideas about surveillance "are constructed through everyday involvement with surveillance as well as from news reports and popular media." These "surveillance imaginaries" inform the way individuals respond to, and engage with, processes of monitoring and data collection.[97]

The complexity of digital technologies and the constant evolution of threat environments only work to aggravate the feelings of uncertainty that activists experience with regards to regime security agency capabilities. An Egyptian human rights defender coordinating with colleagues inside Egypt and across several other countries stressed the difficulty of everyday security choices:

"*All the time when we talk in our online meetings we don't know if we can speak freely or not. We have no alternatives, we are between two options: to be practical or to be secure. Every discussion is a test for us, to mention a name, to say something or not, dates, passwords, etc.*"[98]

Moreover, recurring reports on successful hacking and surveillance operations or new security flaws in popular applications can overwhelm activists and lead to feelings of resignation and hopelessness. A Syrian security trainer described the mechanisms leading to "security paralysis" [99] as follows:

"*This 'I don't care'-attitude, this ignorance is sometimes also the result of a high level of stress. If you think about all the possibilities of getting hacked, then it can result in this attitude: OK, I will get hacked anyway. It is a kind of response mechanism to the level of stress (...) Some people can attend three or five trainings, but after all this training they will say OK I will get hacked anyway, if I put antivirus or not, VPN or not.*"[100]

Very few respondents who did not have explicit expertise in digital security felt confident about their ability to protect themselves against potential threats. Most interviewees expressed the need for regular information and advice on practices of digital security. Some reported trying to educate themselves on evolving threats by following the Twitter accounts of experts in the field or studying other online sources. Others did so by consulting with friends and colleagues and asking for advice and recommendations on Internet security. A Syrian editor stressed this reliance on access to support:

"*We are not technical, we are journalists—and it is important to know that there is someone who can help and protect you when you are facing a problem.*" [101]

Some respondents, aware of the potential risks, felt they did not have the knowledge they needed to protect themselves. A few independent freelancers, for instance, highlighted the difficulties they experienced in trying to obtain information and organizational support in matters of digital security.

---

[96] McGregor, S., & Watkins, E. (2016). "Security by Obscurity": Journalists' Mental Models of Information Security. *International Symposium of Online Journalism*. http://isoj.org/research/security-by-obscurity-journalists-mental-models-of-information-security.

[97] Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication, 11*(19), p. 830.

[98] Interview E6, November 2018.

[99] Electronic Frontier Foundation. Security Education Companion: Why your audience should care – and act. https://sec.eff.org/articles/why-your-audience-should-care.

[100] Interview S10, January 2019.

[101] Interview S4, October 2018.

An Egyptian women rights defender observed that trainings were not always appropriate for all age groups:

"*I had one training in digital security and I definitely need to do more. There were a lot of young people in the training who were more advanced and I didn't dare to ask questions all the time because I did not want to take everybody's time and be the stupid person in the class. I definitely need a lower level beginner class and I need to learn this because now I always have to rely on someone else and find someone to ask questions I have about digital security.*"[102]

PRACTICING DIGITAL SECURITY

Respondents identified a few key tools and practices they considered important for their protection. Email encryption and encrypted messaging services such as Signal were frequently mentioned, as was the use of two-step verification to protect email accounts against intrusions and password theft. Syrian interviewees, in particular, emphasized the importance of using VPNs to protect Internet connections. Several respondents also explained that they refrained from using Facebook messenger for communications, emphasizing the risks of Facebook profiles for monitoring and social engineering. Nevertheless, especially in Egypt, Facebook and its messenger app remain in prominent use as activists explained it was difficult to convince people to use other platforms. Indeed, an activist who left Facebook for security purposes started to feel "disconnected" from events and networks.[103]

Several of the security models outlined by respondents reflect the complex techno-political environment in which they must navigate. A Syrian photojournalist, for instance, said she created a specific email account for every new professional activity to distribute her information over different accounts and profiles. And a Syrian journalist based in Turkey explained how his security precautions depended on the contacts he was dealing with:

"*When I call a journalist in the regime area, they use fake names and I also use a fake name. We connect by email, they use VPN, I don't. The danger is for them, not for me. I don't say anything about them, nobody knows their names. When a publication asks me about the name of my source, like who is this journalist, I don't answer. I rather cancel my article. The same thing for contacts in ISIS area before. For areas under control of the SDF (Syrian Democratic Forces), I use a fake name to be safe, because I am in Turkey, and they use their real name, no problem for them.*"[104]

The journalist reported using four different email addresses (two of them protected by two-step verification) and two separate computers (one personal and one for his job), while also refraining from using his phone for anything related to work.

The interviews reveal that activists often must fend for themselves on the digital front lines. Under threat from repressive regimes, they have to make decisions on risk mitigation in their daily routines on an individual level. For transnational activism, the complex, often opaque, technologies of digital communication are certainly indispensable. But an overreliance on purely technical solutions for privacy and data protection risks exacerbating activist dependency on technical experts and an unequal distribution of knowledge and resources. Moreover, on a technical level, knowledge within civil society is usually quickly outpaced by that of the state and private sector.[105]

[102] Interview E12, March 2019.

[103] Interview E4, November 2018.

[104] Interview S13, January 2019.

[105] Gürses, S., Kundnani, A., & Van Hoboken, J. (2016). Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society, 38*(4), 576-590; Kazansky, B. (2015). Privacy, responsibility, and human rights activism. *The Fibreculture Journal 26* (Entanglements–Activism and Technology).

SECURITY NEEDS AND HURDLES

These insights are confirmed by the security needs and hurdles identified by interviewees for the realization of digital security among activist groups and communities. The need for more technical expertise and better equipment was repeatedly mentioned. Tellingly, only a few of the larger organizations involved in the research process had data protection policies and dedicated staff for digital security. The smaller groups and media organizations often lacked the necessary funds to invest in the training, staff, and equipment needed to improve their digital protection.

For example, a Syrian digital security trainer emphasized the problem of using pirated and outdated software. Syrian activists in Turkey and the liberated areas often could not afford to buy original products, even when working for NGOs. Moreover, access to pirated software was more common in Syria as copyrights were not enforced. And sanctions against the country meant Syrian citizens often could not open bank accounts or use credit cards to purchase software updates and anti-virus protection even if they tried.

"*How do you want to build the capacity of these people?*" the trainer asked. "*Without offering them the original version of a program that is more expensive than anything in your training budget?!*"[106]

Another security expert and trainer working with exiled members of the Syrian media pointed out that organizations often worked for years with risky tools without any incidents. Consequently, it was difficult to convince them that they needed to change their routines. This problem was exacerbated by the fact that in-country contacts often lacked sufficient knowledge on digital security and failed to use recommended security tools and applications. For instance, when an exiled journalist needed to quickly get in touch with a source, encrypting emails or shifting to more secure messaging service was considered cumbersome.[107]

Several of the interviewed trainers and experts for digital security emphasized the difficulty of changing the behaviour of individuals in order to improve their protection against digital threats. An Egyptian trainer pointed out the trade-offs of digital security for users without technical expertise:

"*When you add more security you add an extra layer to deal with every day. In the beginning people start to fight the change.*"[108]

And an Iranian trainer complained that he had to "chase" participants after trainings because if not they would soon disable important security features, such as two-step verification. He noted that under pressure and in moments of emergency, activists tend to forget the security methods learned in trainings.[109]

Another Iranian security expert stressed the need to better inform activists about how to collect samples of suspicious emails and files so they could be analyzed to learn about the capabilities of threat actors and possibly identify other targets. He said:

"*I am really going from door to door begging for samples. There is too little information sharing on threats.*"[110]

[106] Interview S10, January 2019.
[107] Interview S3, October 2018.
[108] Interview E10, January 2019.
[109] Interview I13, February 2019.
[110] Interview I1, November 2018.

In the same vein, another security expert working with Iranian diaspora organizations pointed out that individuals who have fallen prey to a digital attack often feel stigmatized and ashamed to admit it. Yet the reality is successful attacks happen quite often in the field. Activists need to accept this fact and share their experiences so that others can learn from them. The expert emphasized the importance of trust and vulnerability disclosure for the resilience of activist communities. At the same time, the respondent highlighted, increased awareness about digital threats among activists also meant that they needed more assistance to avoid people overconsulting with security advisers regarding harmless "false positives."[111]

Groups and organizations with in-country staff emphasised that they needed better strategies for securing information and preventing access to accounts in case of arrests. Physical access to devices, for example after a seizure or arrest, allows security agents to gather detailed information about cross-border networks. To combat this recurring problem, interviewed digital security experts working in rapid response networks stressed the importance of privileged access to contacts in big social media companies so in cases of arrest social media profiles could be closed down or data secured.

STRENGTHENING NETWORK RESILIENCE

As highlighted by the interviews, activist security is closely intertwined with all members of a network and thus cannot appropriately be tackled on an individual level. An Iranian journalist described his perception of risks in transnational collaborations as follows:

"*The biggest risk in terms of digital security is that I respect all necessary measures but somebody else doesn't. As if you were driving a car and you respect all the rules, but somebody else doesn't and you get into an accident with that person.*"[112]

Another Iranian journalist dealing with sources and contacts inside the country felt the responsibility to transfer her knowledge:

"*The updates I receive, I try to pass them on to my connections. Like Telegram is good for this and that conversation, but Signal is better for that. (...) Depending on the different people, time and circumstances, I am trying to advise them to be more safe. It is not only about me, they are more at risk.*"[113]

For diaspora activists whose communities and peer groups are often distributed across several countries (including close ties to the repressive context of the home country), the protection of data and privacy is a collective effort. Activists cannot be considered as individuals with a certain risk profile that needs addressing. Instead, they must be viewed—and view themselves—as part of a larger network in which a successful attack against the weakest link can have severe consequences for all. Trainings and technical tools for digital security alone cannot provide sufficient protection against resourceful state actors targeting civil society across borders. Rather, the collective understanding of the threats faced by diaspora networks must be improved. Activists feel more empowered and resilient when they strengthen their ties to local and global networks for incident response, support, and information sharing.

[111] Interview G1, December 2018.

[112] Interview I12, February 2019.

[113] Interview I8, December 2018.

CONCLUSION

In October 2019, Iranian security agents lured exiled journalist Ruhollah Zam (an administrator of a popular Telegram news channel) from Paris to Iraq. There he was arrested and transferred back to Tehran. Iran's Revolutionary Guards announced the capture on state television as well as through Zam's own Telegram channel, boasting about their long reach across borders.[114] As in the example of Jamal Khashoggi and Saudi Arabia, the case demonstrated an authoritarian regime's willingness and capability to silence dissidents beyond its territory. Yet although such blunt operations draw public attention and help regimes send chilling messages into broader diaspora communities, the reality is they occur infrequently. Today, as this report has shown, transnational repression often unfolds in more subtle ways: through various forms of surveillance and harassment that aim to put activists under persistent pressure and constrain the opportunities they gained in exile.

Authoritarian regimes perceive diaspora activists as a threat when such activists are able to raise public attention, garner support for civil society and opposition in the country, or disseminate alternative news and opinion (both at home and abroad). With close ties to the home country as well as contacts to international organizations, media, and policy circles, diaspora activists occupy a strategic position to leverage critical information against regimes. To a significant extent, therefore, practices of transnational repression are information controls used by regimes to monitor and disrupt information flows in cross-border activist networks. Methods such as targeted surveillance, online harassment, slander, and pressure against in-country relatives are all attempts to intimidate and silence diaspora activists and punish their attempts to gain to public attention.

Digital technologies are key components to transnational repression as they enable regimes to follow and respond to diaspora activism with greater scope and speed. Activists' reliance on digital media creates vulnerabilities and exposes sensitive information that state agents can use to threaten dissidents abroad and their cross-border networks. Moreover, digital threats are often carried out with little chance to identify perpetrators and hold them accountable. The complexity of today's digital platforms and networks often means that potential targets are left in the dark about the actual capabilities of regimes to intercept communications and penetrate accounts. As a consequence, digital media not only create new opportunities for extending the extraterritorial reach of the security apparatus, but also reduce the costs of political control compared to more traditional methods of repression.

By relying on a toolkit of transnational repression, regimes such as Egypt, Syria, and Iran are able to foster restraint and self-censorship among activists, undermine their ties to the home country, and raise their level of tension and stress. Even though state authorities cannot completely succeed in deterring activism in exile, they are still able contain some of its impact and outreach by imposing additional costs and risks on activists living abroad. The practices identified in this report represent deliberate and systematic interferences in the fundamental human rights of targets—namely the rights to freedom of expression and privacy. As such, practices of transnational repression seeking to shield regimes from criticism and accountability have a clear authoritarian intent.

Threats against activists in exile and diaspora communities exemplify the broader trends of rising authoritarian politics and shrinking civic space. Authoritarian governments extend the reach of their repressive policies into the territory of other countries to target dissidents who often emigrated to escape similar restrictions on civic freedoms and rights at home. These states instrumentalize digital technologies to amplify their control over citizens and information flows beyond borders. And they employ increasingly invasive methods to spy on, compromise, and disrupt civil society networks in an effort to outmaneuver the basic protections activists rely on to secure their data and communications. As a consequence, civil society's continued ability to use digital tools to freely exchange, coordinate, and organize is in danger.[115]

[114] Radio Farda (2019, October 14). Iran TV Shows Film of Captured Dissident Apologizing to Regime. https://en.radiofarda.com/a/irgc-says-it-lured-a-fierce-critic-in-exile-back-to-iran-and-arrested-him-/30216087.html.

[115] Access Now (2019, August 29). Digital civic space under attack. https://www.accessnow.org/digital-civic-space-under-attack/; Freedom House (2018). Freedom on the Net 2018: The Rise of Digital Authoritarianism. https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism; Tactical Technology Collective. Shrinking Civil Space: A Digital Perspective. https://ourdataourselves.tacticaltech.org/posts/shrinking-civil-space-a-digital-perspective.

RECOMMENDATIONS

Based on the findings of this report's research, the following recommendations are offered to help stimulate strategies to better protect diaspora activists from transnational repression. In general, more work needs to be done to:

1. Build digital resilience,
2. Contain surveillance technology,
3. Take care of activist wellbeing,
4. Involve host societies.

BUILDING DIGITAL RESILIENCE

Efforts must be made to improve the digital resilience of activists and civil society. The research confirms the limited impact of singular training events. Trainings introduce activists to basic protections and tools, but they often fail to initiate a more substantial change in actual security behavior and practices. And at times, they risk confusing or even scaring participants. It is therefore necessary to explore additional forms of capacity building and education. Follow-up events to prior trainings can help consolidate knowledge and clarify questions which may have emerged during the first phase of practice. More promising still are initiatives of long-term partnership and mentoring to help organizations develop their own systematic approach to information security, provide ongoing context-specific advice, and respond to new or changing threats.[116] This shift in focus also needs to be taken into account by donors in order to obtain more flexible core support, instead of project-based funding expecting specific quantifiable results.

Research also shows that activists are often forced to decide on matters of digital security at an individual level, especially when not embedded in organizations or when pressured to act on short notice. Yet in such situations individuals can feel debilitated by the complex setup of digital technologies and the seemingly endless options of resourceful state and corporate actors to capture their data. It is therefore vital to reduce the uncertainty about the actual capabilities of adversaries so that activists can differentiate between legitimate and unfounded fears. In addition to creating networks of support and advice, accessible and context-specific educational resources should be developed to raise the general level of understanding of digital technologies and the risks associated with their use.

[116] *See, e.g.*, the Digital Integrity Fellowship of the Digital Defenders Program. https://manuals.digitaldefenders.org.

Instead of appearing as a burden keeping activists from doing their "real" work, the informed and knowledgeable use of digital technologies needs to be presented as a way to maintain agency and autonomy under conditions of evolving sociotechnical risks.

Recognizing the role of the individual in practicing digital security, however, does not mean one should neglect the broader power relations and structural inequalities forming around digital technologies. Protecting the right to privacy and freedom of expression in the digital realm demands a collective effort by all parties. This is particularly relevant for diaspora activists who maintain multiple ties and relations across countries and communities. Within these networks, a shared understanding of risks and vulnerabilities needs to be developed, and resources must be distributed more evenly. Establishing strong communities of practice will make it easier to provide more accurate information on threats as well as emergency support and advice on information security. Building coalitions to connect large, international organizations with smaller, local groups will allow support to be properly and rapidly scaled while also offering natural and trusted contact points for activists on the frontlines. In turn, Computer Emergency Response Teams (CERTs) for civil society can be used to form an important backbone of such networks, linking rapid responders, digital security helpdesks, and infrastructure providers so they can all share data on incidents and resources for response.[117] In addition, digital rights initiatives will help civil society take part in shaping the norms and regulations around privacy, data protection, and online expression in order to defend the new and vulnerable areas of civic space created by digital technologies.

CONTAINING SURVEILLANCE TECHNOLOGY

Surveillance technology and related information controls used by repressive regimes must be contained. Research highlights the consequences of the proliferation of powerful surveillance tools across geographic and political borders. As demonstrated, threat actors from Iran, Syria, and Egypt often rely on conventional malware for attacks against civil society. Yet such attacks cause even more harm when employing advanced surveillance technology. Of the three countries, Egypt (and possibly the others) has already acquired commercial spyware on a large scale, including products of leading companies like Italy's Hacking Team and the Israeli NSO group. The research findings make clear how authoritarian powerholders, when given the opportunity, abuse such invasive technologies to target dissidents and undermine fundamental rights within and beyond their territories.

The report thus strongly supports the ongoing efforts being made to scrutinize and constrain the current opaque global market for commercial surveillance technology. The UN Special Rapporteur on freedom of opinion and expression, David Kaye, considers the threat of this industry so grave he has called for an immediate moratorium on the global sale, transfer, and use of surveillance technology until rigorous human rights safeguards have been put in place.[118] Companies must observe the UN Guidelines for businesses and human rights, which require robust mechanisms of due-diligence, to prevent the abuse of their products for human rights violations. Unfortunately, the self-regulation of companies has proven insufficient. Strict rules and independent oversight are therefore needed to bring transparency and accountability into the market for spyware. Strengthening existing control regimes, for instance by making export licenses conditional upon a human rights review, is just one step of many that must be taken. Strategic litigation should also be used to constrain the deceptive practices of companies providing surveillance tools that interfere with the rights of targets.

[117] *See* CiviCERT (https://www.civicert.org) as an example of such an international initiative, and TibCERT (https://tibcert.org) as an example of such a coalition of Tibetan organizations

[118] United Nations Human Rights Council (2019). Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf.

The sale, purchase, and use of surveillance technology by governments should also be subject to robust public debate and stakeholder consultation, and there must be mechanisms for sanctions and redress in case of abuse.[119]

TAKING CARE OF ACTIVIST WELLBEING

The wellbeing of activists must be protected if they are to continue to do their essential work. Activists must tackle a range of issues when relocating to another country including obtaining asylum or a residence permit, covering costs of living, and navigating new language and cultural barriers. They may also face racism, xenophobia, and other forms of discrimination and harassment. Even host country authorities can be a source of pressure and threats. Moreover, exiled activists have often experienced government pressure, persecution, imprisonment, and even torture before deciding to leave their home country. Accordingly, after reaching a more secure environment, they may need to deal with the resulting challenges to their wellbeing such as burnout, depression, and post-traumatic stress disorder. They may also harbor feelings of isolation and guilt vis-à-vis those who stayed behind. The tensions of living in exile, especially when combined to continuous harassment and threats from the home regime, thus risk aggravating feelings of prolonged stress and paranoia – of having "no place to hide."

Unfortunately, the emotional and psychosocial security of activists is a critical, but usually neglected, component in protection strategies for human rights defenders. Human rights practice is itself impregnated by ideas of "self-sacrifice, heroism, and martyrdom."[120] Activists often find it difficult to talk about and deal with any emotional and mental challenges they are facing because of social, cultural, or religious norms and stigmas. Diaspora and exiled activists, in particular, may feel compelled to compare their condition with that of peers inside the country, under immediate threat from state authorities, and simply take issues of psychosocial security off the table. But the wellbeing of activists must be considered an essential element for "the sustainability and effectiveness of activism over the longer term."[121] Accordingly, interventions aiming to support the security and resilience of civil society activists need to provide the appropriate mechanisms to address the wellbeing of activists by taking into account the political, social, and cultural contexts they come from and operate in, as well as their individual experiences.[122] Much more work must be done in this area to properly support activists operating in exile.

INVOLVING HOST SOCIETIES

Host societies must work to become more involved in protecting the rights of activists living within their borders. Societies hosting exiled and diaspora activists have a responsibility to help counter the practices of governments exporting repression overseas. At the level of civil society, it is important to document and raise awareness on transnational repression. Authoritarian regimes have proven to be susceptible to the pressure of public attention and the instruments of human rights advocacy, such as the Universal Periodic Review of the United Nations Human Rights Council. Media focus on targeted dissidents can help shed light on, and frustrate, tactics of silencing across borders.

---

[119] Anstis, S., Deibert, R., & Scott-Railton, J. (2019, July 19). A Proposed Response to the Commercial Surveillance Emergency. Lawfare Blog. https://www.lawfareblog.com/proposed-response-commercial-surveillance-emergency; McKune, S., & Deibert, R. (2017). Who's watching Little Brother? Citizen Lab. https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf.

[120] Human Rights Defender Hub (2017). Wellbeing, Risk, and Human Rights Practice. Policy Brief 1, University of York, p. 2. https://static1.squarespace.com/static/57ab08756a49635fe426003e/t/58ee2a3debbd1a718d29553c/1505738548404/HRD+Hub+Policy+Brief+1+EN.pdf.

[121] The Barcelona Guidelines on Wellbeing and Temporary International Relocation of Human Rights Defenders at Risk. (2019, June), p. 6. https://static1.squarespace.com/static/58a1a2bb9f745664e6b41612/t/5de6a0d7ae38e0103312349b/1575395544981/The+Barcelona+Guidelines+-+EN+%28Final%29.pdf.

[122] Ibid.

International human rights groups, which are often based in Western host societies, need to monitor and record cases of transnational repression in its various forms in a more systematic and active manner. Within the United Nations, transnational repression currently falls between the mandates of different bodies and therefore is not captured in its entirety. This should be corrected. Similarly, related initiatives focus on specific regions or cover only selected forms of transnational repression.[123] Academic research and human rights advocacy therefore need to develop a comprehensive definition of transnational repression and guidelines for studying it in order to facilitate rigorous documentation.

In general, host country governments need to be more aware of the extent and nature of harassment that dissidents residing on their territories experience. The status of asylum-seeker or political refugee fundamentally involves the need for assistance and protection in order to preclude further persecution.[124] Practices of transnational repression, which violate the sovereignty of the host state as well as international human rights and refugee protection standards, should be a topic of diplomatic pressure on the perpetrating regimes. They cannot simply be ignored. Foreign policy makers need to consider these practices as actions undertaken by increasingly assertive authoritarian states to undermine principles of liberal democracy, and respond accordingly.[125]

New legislation may be required for appropriate action to be taken. In Europe and the United States, legal instruments penalizing human rights violations by external actors cover only blatant forms of transnational repression. Yet as this report has demonstrated, much of the repression that occurs today is that of a more subtle variety. On a positive note, the US government recently introduced the "TRAP Act" to restrict the ability of repressive governments to use Interpol to issue requests to detain and extradite political opponents abroad.[126] In order to respond to the broader range of tactics of transnational repression it is important to familiarize and involve domestic agencies of law enforcement and so that they can more systematically use the instruments provided by the rule of law. For instance, Scandinavian countries impose legal penalties on foreign intelligence activities targeting dissidents in exile (so-called "refugee espionage").[127] Similarly, cybercrime laws could be used to litigate against targeted surveillance and hacking attacks on civil society activists.[128]

[123] See, e.g., the Central Asian Political Exiles (CAPE) database of the University of Exeter Central Asian Studies Network, https://excas.net/projects/political-exiles. A new project on transnational repression, launched in fall 2019 at Freedom House, seeks to measure the scope and scale of transnational repression globally, with an emphasis on collecting data on physical attacks against dissidents all over the world (website to be released).

[124] UN High Commissioner for Refugees (UNHCR) (2014, February). *Comments by the United Nations High Commissioner for Refugees (UNHCR) on the Memorandum of 6 December 2013, proposing Criminalization of Refugee Espionage.* https://www.refworld.org/docid/5829ad6c4.html.

[125] Brechenmacher, S., & Carothers, T. (2019). Defending Civic Space: Is the International Community Stuck? Working Paper, Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP_Brechenmacker_Carothers_Civil_Space_FINAL.pdf. Cooley, A. (2015). Authoritarianism Goes Global: Countering Democratic Norms. *Journal of Democracy, 26* (3), 49-63.

[126] Commission on Security and Cooperation in Europe (2019, September 12). Helsinki Commission Leaders introduce Transnational Repression Accountability and Prevention (TRAP) Act. https://www.csce.gov/international-impact/press-and-media/press-releases/helsinki-commission-leaders-introduce.

[127] Swedish Security Service. Refugee Espionage. https://www.sakerhetspolisen.se/en/swedish-security-service/counter-espionage/refugee-espionage.html. The German domestic security agency also warns refugees, especially those from Syria and Iran, of attempts to spy on and pressure dissidents in exile. Bundesamt für Verfassungsschutz. (2018). How can I identify extremists and members of foreign secret services within my environment? https://www.verfassungsschutz.de/embed/publication-2018-02-important-information-for-refugees-in-germany.pdf.

[128] McKune, S., & Deibert, R. (2017). Who's watching Little Brother? Citizen Lab. https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf.

REFERENCES

Abas, A., & Al-Masri, A. (2018, May 17). The new face of the Syrian Electronic Army. *OpenCanada.* https://www.opencanada.org/features/new-face-syrian-electronic-army

Access Now (2019, May 20). Shutdowns, surveillance, and censorship: UPR reviews highlight threats to digital rights. https://www.accessnow.org/shutdowns-surveillance-and-censorship-upr-reviews-highlight-threats-to-digital-rights

Access Now (2019, August 29). Digital civic space under attack. https://www.accessnow.org/digital-civic-space-under-attack/

Alinejad, M. (2018, July 31). My sister disowned me on state TV. *The New York Times*. https://www.nytimes.com/2018/07/31/opinion/iran-hijab-feminist.html

Alrwishdi, D., & Hamilton, R. (2018, April 12). Paying Attention to Land Rights in Syria Negotiations. *Just Security*. https://www.justsecurity.org/54781/paying-attention-land-rights-syria-negotiations

Amnesty International (2018). Toxic Twitter – A toxic place for women. https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1

Amnesty International (2018, December 19). When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users. https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough

Amnesty International (2019). Egypt: Gross Human Rights Violations Under President Al-Sisi. https://www.amnesty.org/download/Documents/MDE1202532019ENGLISH.pdf

Amnesty International (2019, January 24). Iran's 'year of shame': More than 7,000 arrested in crackdown on dissent in 2018. https://www.amnesty.org/en/latest/news/2019/01/irans-year-of-shame-more-than-7000-arrested-in-chilling-crackdown-on-dissent-during-2018

Amnesty International (2019, March 6). Phishing attacks using third-party applications against Egyptian civil society organizations. https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations

Andén-Papadopoulos, K., & Pantti, M. (2013). The media work of Syrian diaspora activists: Brokering between the protest and mainstream media. *International Journal of Communication, 7, 22*

Anderson, C., & Sadjadpour, K. (2018). Iran's cyber threat: espionage, sabotage and revenge. *Carnegie Endowment for International Peace.* http://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

Ansari, A. M. (2010). *Crisis of authority: Iran's 2009 presidential election.* Chatham House, London

Anstis, S., Deibert, R., & Scott-Railton, J. (2019, July 19). A Proposed Response to the Commercial Surveillance Emergency. Lawfare Blog. https://www.lawfareblog.com/proposed-response-commercial-surveillance-emergency

Bank, A., & Edel, M. (2015). Authoritarian regime learning: Comparative insights from the Arab uprisings. *GIGA Working Papers.* https://www.giga-hamburg.de/de/system/files/publications/wp274_bank-edel.pdf

Barcelona Guidelines on Wellbeing and Temporary International Relocation of Human Rights Defenders at Risk. (2019). https://static1.squarespace.com/static/58a1a2bb9f745664e6b41612/t/5de6a0d7ae38e0103312349b/1575395544981/The+Barcelona+Guidelines+-+EN+%28Final%29.pdf

Barnard, A. (2019, May 11). Inside Syria's Secret Torture Prisons: How Bashar Al-Assad Crushed Dissent. *The New York Times.* https://www.nytimes.com/2019/05/11/world/middleeast/syria-torture-prisons.html

Bazzell, M. (2016). *Open source intelligence techniques: resources for searching and analyzing online information*. CreateSpace Independent Publishing Platform.

BBC Media Centre (2019, March 12). UN Special Rapporteur "deplores" the persecution of BBC Persian staff and their families. https://www.bbc.co.uk/mediacentre/latestnews/2019/persian-un.

Bergman, R., & Walsh, D. (2019, October 3). Egypt is using Apps to track and target its citizens, report says. *The New York Times*. https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html.

Brechenmacher, S., & Carothers, T. (2019). Defending Civic Space: Is the International Community Stuck? Working Paper, Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP_Brechenmacker_Carothers_Civil_Space_FINAL.pdf.

Bundesamt für Verfassungsschutz. (2018). How can I identify extremists and members of foreign secret services within my environment? https://www.verfassungsschutz.de/embed/publication-2018-02-important-information-for-refugees-in-germany.pdf.

Center for Human Rights in Iran (2010, October 6). Shirin Ebadi: Nokia Siemens action a major accomplishment for Iranians and for the people of the world. https://www.iranhumanrights.org/2010/10/shirin-ebadi-nokia-siemens-action-a-major-accomplishment-for-iranians-and-for-people-of-the-world/.

Citizen Lab (2014). Communities @ Risk: Targeted Digital Threats against Civil Society. https://targetedthreats.net.

Commission on Security and Cooperation in Europe (2019, September 12). Helsinki Commission Leaders introduce Transnational Repression Accountability and Prevention (TRAP) Act. https://www.csce.gov/international-impact/press-and-media/press-releases/helsinki-commission-leaders-introduce.

Cooley, A. (2015). Authoritarianism Goes Global: Countering Democratic Norms. *Journal of Democracy, 26*(3), 49-63.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance: A Review of Multilateralism and International Organizations, 18*(3), 339–361.

Deibert, R., Oliver, J., & Senft, A. (2019). Censors get smart: Evidence from Psiphon in Iran. *Review of Policy Research, 36*(3), 341-356.

Dunne, M., & Hamzawy, A. (2019). Egypt's Political Exiles: Going Anywhere but Home. Carnegie Endowment for International Peace, Washington. https://carnegieendowment.org/files/Dunne_Hamzawy_EgyptExiles_final.pdf.

Electronic Frontier Foundation. Security Education Companion: Why your audience should care – and act. https://sec.eff.org/articles/why-your-audience-should-care.

Euromed Rights (2017, May 23). Extreme Concern about the Harassment of Egyptian Human Rights Defenders in Italy. https://euromedrights.org/publication/extreme-concern-harassment-egyptian-human-rights-defenders-italy.

Euromed Rights (2018, April 18). Death Threats against CIHRS Director, Bahey el-Din Hassan. https://euromedrights.org/publication/death-threats-against-cihrs-director-bahey-el-din-hassan/.

Fire Eye (2015). Behind the Syrian Conflict's Digital Frontlines. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf.

Fischer, M. (2016, August 26). Syria's Paradox: Why the War Only Ever Seems to Get Worse. *The New York Times.* https://www.nytimes.com/2016/08/27/world/middleeast/syria-civil-war-why-get-worse.html.

Freedom House (2018). Freedom on the Net 2018: The Rise of Digital Authoritarianism. https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.

Franceschi-Bicchierai, L. (2015, April 3). The Syrian Electronic Army's Most Dangerous Hack. *Vice Motherboard*. https://www.vice.com/en_us/article/nze5nk/the-syrian-electronic-armys-most-dangerous-hack.

Gholamhosseinpour, M. (2019, February 18). Civil Rights Activists Systematically Forced to Emigrate. *Iran Wire*. https://iranwire.com/en/features/5861.

Glasius, M. (2018). What authoritarianism is... and is not: A practice perspective. *International Affairs, 94*(3), 515-533.

Glasius, M. (2018). Extraterritorial authoritarian practices: A framework. *Globalizations, 15*(2), 179-197.

Glasius, M., de Lange, M., Bartman, J., Dalmasso, E., Lv, A., Del Sordi, A., Michaelsen, M., & Ruijgrok, K. (2017). *Research, ethics and risk in the authoritarian field*. Palgrave Macmillan.

Glasius, M., & Michaelsen, M. (2018). Illiberal and authoritarian practices in the digital sphere—Prologue. *International Journal of Communication 12*, 3795-3813.

Greenslade, R. (2019, March 17). Iran's threats to BBC Persian staff must be confronted. *The Guardian*. https://www.theguardian.com/media/commentisfree/2019/mar/17/irans-threats-to-bbc-persian-staff-must-be-confronted.

Guarnieri, C. (2015, August 16). Helping the Helpless: Targeted Threats to Civil Society. Talk at the Chaos Communication Camp. https://media.ccc.de/v/camp2015-6848-helping_the_helpless.

Guarnieri, C. (2019, March 8). Phishing attacks using third-party applications against Egyptian civil society organizations. https://nex.sx/blog/2019/03/08/phishing-attacks-against-egyptian-civil-society.html.

Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics, 13*(01), 42–54.

Gürses, S., Kundnani, A., & Van Hoboken, J. (2016). Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society, 38*(4), 576-590.

Hankey, S., & Ó Cluanaigh, D. (2013). Rethinking risks and security of human rights defenders in the digital age. *Journal of Human Rights Practice 5*(3), 535-547.

Harding, L., & Arthur, C. (2013, April 30). Syrian Electronic Army: Assad's cyber warriors. *The Guardian*. https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background.

Heydemann, S., & Leenders, R. (Eds.). (2013). *Middle East Authoritarianisms: Governance, Contestation, and Regime Resilience in Syria and Iran*. Stanford University Press.

Hirt, N., & Saleh Mohammad, A. (2018). By way of patriotism, coercion, or instrumentalization: How the Eritrean regime makes use of the diaspora to stabilize its rule. *Globalizations, 15*(2), 232-247.

Honari, A. (2018). From 'the effect of repression' toward 'the response to repression.' *Current Sociology, 66*(6), 950-973.

Hug, A.(ed.). (2016). No Shelter: The harassment of activists abroad by intelligence services from the former Soviet Union. Foreign Policy Centre, London.

Human Rights Defender Hub (2017). Wellbeing, Risk, and Human Rights Practice. Policy Brief 1, University of York. https://static1.squarespace.com/static/57ab08756a49635fe426003e/t/58ee2a3debbd1a718d29553c/1505738548404/HRD+Hub+Policy+Brief+1+EN.pdf.

Human Rights Watch (2012). Torture Archipelago: Arbitrary Arrests, Torture, and Enforced Disappearances in Syria's Underground Prisons since 2011. https://www.hrw.org/report/2012/07/03/torture-archipelago/arbitrary-arrests-torture-and-enforced-disappearances-syrias.

Human Rights Watch. (2012). *Why They Left: Stories of Iranian Activists in Exile*. https://www.hrw.org/sites/default/files/reports/iran1212webwcover_0_0.pdf.

Human Rights Watch (2019, April 2). Egypt: Constitutional Amendments Entrench Repression. https://www.hrw.org/news/2019/04/20/egypt-constitutional-amendments-entrench-repression.

Human Rights Watch (2019, June 28). Rigging the System: Government Policies to Co-Opt Aid and Reconstruction Funding in Syria. https://www.hrw.org/report/2019/06/28/rigging-system/government-policies-co-opt-aid-and-reconstruction-funding-syria.

International Federation for Human Rights (2018, July 2). Egypt: A repression made in France. https://www.fidh.org/en/issues/litigation/egypt-a-repression-made-in-france.

Iran Human Rights Documentation Center (2011). No Safe Haven: Iran's Global Assassination Campaign. New Haven. https://iranhrdc.org/no-safe-haven-irans-global-assassination-campaign.

Jörum, E. L. (2015). Repression across borders: homeland response to anti-regime mobilization among Syrians in Sweden. *Diaspora Studies, 8*(2), 104-119.

Kausch, K. (2017). Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East. German Marshall Fund of the United States, Policy Brief No. 35, Berlin. http://www.gmfus.org/publications/cheap-havoc-how-cyber-geopolitics-will-destabilize-middle-east.

Kazansky, B. (2015). Privacy, responsibility, and human rights activism. *The Fibreculture Journal 26* (Entanglements–Activism and Technology).

Kazansky, B. (2016). Digital Security in Context: Learning How Human Rights Defenders Adopt Digital Security Practices. Project report. https://secresearch.tacticaltech.org/media/pages/pdfs/original/DigitalSecurityInContext.pdf.

Kazansky, B., Torres, G., Van der Velden, L., Wissenbach, K., & Milan, S. (2019). Data for the Social Good: Toward a Data-Activist Research Agenda. In: Daly, A., Devitt, K., & Mann, M. (eds). Good Data. Institute for Network Cultures, Amsterdam. http://networkcultures.org/wp-content/uploads/2019/01/Good_Data.pdf.

Keck, M. E., & Sikkink, K. (1998). *Activists beyond Borders: Advocacy Networks in International Politics*. Ithaca/New York: Cornell University Press.

Kelly, M. (2011). Transnational diasporic identities: Unity and diversity in Iranian-focused organizations in Sweden. *Comparative Studies of South Asia, Africa and the Middle East, 31*(2), 443-454.

Ketchley, N. (2017). *Egypt in a time of revolution. Contentious Politics and the Arab Spring*. Cambridge/ New York: Cambridge University Press.

Kirkpatrick, D., & Cumming-Bruce, N. (2019, June 19). Saudis Called Khashoggi 'Sacrificial Animal' as They Waited to Kill Him. *The New York Times*. https://www.nytimes.com/2019/06/19/world/middleeast/jamal-khashoggi-Mohammed-bin-Salman.html.

Koinova, M. (2012). Autonomy and positionality in diaspora politics. *International Political Sociology, 6*(1), 99-103.

Koinova, M. (2018). Sending states and diaspora positionality in international relations. International *Political Sociology, 12*(2), 190-210.

Levitt, P., & Schiller, N. G. (2004). Conceptualizing simultaneity: A transnational social field perspective on society. *International Migration Review, 38*(3), 1002-1039.

Lewis, D. (2015). "Illiberal Spaces:" Uzbekistan's extraterritorial security practices and the spatial politics of contemporary authoritarianism. *Nationalities Papers, 43*(1), 140-159.

Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication, 11*(19).

Mada Masr (2017, July 5). UAE transfers internet surveillance system bought from French company to Egypt: Télérama. https://madamasr.com/en/2017/07/05/news/u/uae-transfers-internet-surveillance-system-bought-from-french-company-to-egypt-telerama/.

Marquis-Boire, M. et al. (2013). Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. The Citizen Lab. https://citizenlab.ca/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools.

Marczak, W., & Paxson, V. (2017). Social engineering attacks on government opponents: Target perspectives. *Proceedings on Privacy Enhancing Technologies* (2), 172-185.

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. The Citizen Lab. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries.

Matthies-Boon, V. (2017). Shattered worlds: Political trauma amongst young activists in post-revolutionary Egypt. *The Journal of North African Studies, 22*(4), 620-644.

McGregor, S., & Watkins, E. (2016). "Security by Obscurity": Journalists' Mental Models of Information Security. *International Symposium of Online Journalism*. http://isoj.org/research/security-by-obscurity-journalists-mental-models-of-information-security.

McKune, S., & Deibert, R. (2017). Who's watching Little Brother? Citizen Lab. https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf.

Michaelsen, M. (ed.) (2011) Election Fallout: Iran's Exiled Journalists on their Struggle for Democratic Change, Berlin: Hans Schiler. https://library.fes.de/pdf-files/iez/08560.pdf.

Michaelsen, M. (2018). Exit and voice in a digital age: Iran's exiled activists and the authoritarian state. *Globalizations, 15*(2), 248-264.

Middle East Eye (2018, October 10), Exiled Opposition Leader Expresses Fear after Khashoggi Disappearance. https://www.middleeasteye.net/news/exiled-egyptian-opposition-leader-expresses-fear-after-tv-death-threats-1398361292.

Moss, D. M. (2016). Transnational repression, diaspora mobilization, and the case of the Arab Spring. *Social Problems, 63*(4), 480-498.

Moss, D. M. (2018). The ties that bind: Internet communication technologies, networked authoritarianism, and 'voice' in the Syrian diaspora. *Globalizations, 15*(2), 265-282.

Moss, D. M., Michaelsen, M., & Kennedy, G. Going after the family: Diaspora activism, transnational repression, and proxy punishment. Manuscript to be submitted.

Omari, M. (2019, April 15). Syria's Land Looting Campaign for Reconstruction. *Enab Baladi*. https://english.enabbaladi.net/archives/2019/04/syrias-lands-looting-campaign-for-reconstruction.

Privacy International (2016). The Global Surveillance Industry. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

Privacy International (2016). Open Season: Building Syria's Surveillance State. https://privacyinternational.org/sites/default/files/2017-12/OpenSeason_0.pdf.

Privacy International (2019). State of Privacy in Egypt. https://privacyinternational.org/state-privacy/1001/state-privacy-egypt.

Radio Farda (2019, October 14). Iran TV Shows Film of Captured Dissident Apologizing to Regime. https://en.radiofarda.com/a/irgc-says-it-lured-a-fierce-critic-in-exile-back-to-iran-and-arrested-him-/30216087.html.

Rahimpour, R. (2017, August 15). Iran judiciary freezes assets of BBC Persian staff. *BBC News*. https://www.bbc.com/news/world-middle-east-40936023.

Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review, 126*(7), 1934–1965.

Saremi, N. (2017, October 28). Iran's Persistent Attacks on BBC Persian Journalists. *Iran Wire*. https://iranwire.com/en/features/4934.

Schedler, A. (2013). *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*. Oxford University Press.

Schenkkan, N. (2018, January 29). The Remarkable Scale of Turkey's "Global Purge." *Foreign Affairs*. https://www.foreignaffairs.com/articles/turkey/2018-01-29/remarkable-scale-turkeys-global-purge.

Scott-Railton, J. (2016). Security for the high-risk user: Separate and unequal. *IEEE Security & Privacy, 14*(2), 79-87.

Scott-Railton, J., & Kleemola, K. (2015). London Calling: Two-factor authentication phishing from Iran. The Citizen Lab, Toronto. https://citizenlab.ca/2015/08/iran_two_factor_phishing.

Scott-Railton, J., Abdulrazzak, B., Hulcoop, A., Brooks, M., & Kleemola, K. (2016, August 2). Group5. Syria and the Iranian Connection. https://citizenlab.ca/2016/08/group5-syria/.

Scott-Railton, J., Marczak, B., Raoof, R., & Maynier, E. (2017). Nile Phish: Large Scale Phishing Campaign Targeting Egyptian Civil Society. The Citizen Lab, Toronto. https://citizenlab.ca/2017/02/nilephish-report/.

Shain, Y. (2005). The Frontier of Loyalty: Political Exiles in the Age of the Nation-State. University of Michigan Press.

Stecklow, S. (2012, March 22). Chinese firm helps Iran spy on citizens. Reuters. http://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322.

Stokke, E., & Wiebelhaus-Brahm, E. (2019). Syrian diaspora mobilization: Vertical coordination, patronage relations, and the challenges of fragmentation in the pursuit of transitional justice. *Ethnic and Racial Studies 42*, 1-20.

Swedish Security Service. Refugee Espionage. https://www.sakerhetspolisen.se/en/swedish-security-service/counter-espionage/refugee-espionage.html.

Tactical Technology Collective. Shrinking Civil Space: A Digital Perspective. https://ourdataourselves.tacticaltech.org/posts/shrinking-civil-space-a-digital-perspective.

Tactical Technology Collective (2016). Holistic Security: A Strategy Manual for Human Rights Defenders. https://holistic-security.tacticaltech.org.

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies, 18*(4-5), 530-547.

Tufekci, Z. (2013). "Not this one" social movements, the attention economy, and microcelebrity networked activism. *American Behavioral Scientist, 57*(7), 848-870.

United Nations (2019, July 18). Report of the Special Rapporteur on Human Rights in Iran. https://undocs.org/en/A/74/188.

United Nations Human Rights Council (2019). Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, p. 7. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf.

UN High Commissioner for Refugees (UNHCR) (2014, February). *Comments by the United Nations High Commissioner for Refugees (UNHCR) on the Memorandum of 6 December 2013, proposing Criminalization of Refugee Espionage*. https://www.refworld.org/docid/5829ad6c4.html.

Weber, V. (2019). The Worldwide Web of Chinese and Russian Information Controls. Centre for Technology and Global Affairs, University of Oxford. https://ctga.web.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf.

Yassin-Kassab, R., & Al-Shami, L. (2018). *Burning country: Syrians in revolution and war.* Pluto Press, London.