Selected Papers of #AoIR2020:
The 21st Annual Conference of the
Association of Internet Researchers
Virtual Event / 27-31 October 2020

RESISTING TRANSNATIONAL REPRESSION: THE DIGITAL SECURITY PRACTICES OF DIASPORA AND EXILED HUMAN RIGHTS DEFENDERS

Marcus Michaelsen
Law, Science, Technology and Society (LSTS) Research Group, Vrije Universiteit Brussels

Extended Abstract

Transnational civil society and advocacy networks play an important role in exposing rights violations and undermining censorship under authoritarian regimes (Keck & Sikkink 1998). In these networks, exiled and diaspora activists act as essential bridge figures brokering information and knowledge across borders, supporting counterparts in their country of origin, raising international awareness, and leveraging external pressure on repressive regimes. With the help of digital communication technologies they maintain close links into the home country and participate in global news and advocacy cycles (Bernal 2014; Brinkerhoff 2009). Yet the use of these technologies also creates multiple points of exposure that repressive state actors exploit for information controls and repression beyond borders. Authoritarian states increasingly resort to surveillance, malware attacks, online harassment and disinformation campaigns to compromise civil society networks and mute their voices (Hankey & Ó Cluanaigh 2013; Freedom House 2018). Because digital communication technologies allow for monitoring and responding to transnational activism rapidly and on a large scale, they enable new and influence established tactics of extraterritorial state control. Digital threats are often intertwined with more traditional methods of transnational repression, such as pressure on in-country families and slander in state-controlled media (Glasius 2018; Moss 2016; Michaelsen 2018, 2020).

Research into 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 (Amnesty International 2018; Citizen Lab 2014). Less is known, however, about the ways in which potential targets perceive and respond to increasingly complex risks, and how they are

Suggested Citation (APA): Michaelsen, M. (2020, October). *Resisting Transnational Repression: The Digital Security Practices of Diaspora and Exiled Human Rights Defenders*. Paper presented at AoIR 2020: The 21th Annual Conference of the Association of Internet Researchers. Virtual Event: AoIR. Retrieved from http://spir.aoir.org.

affected by digital threats. This paper (manuscript in progress) builds on more than 50 qualitative interviews with exiled human rights defenders and journalists from Egypt, Syria and Iran to investigate risk perceptions and security practices of activists in transnational networks. It moves beyond the focus mere technical solutions to online threats in order to consider the broader human and behavioral factors shaping practices of privacy protection and digital security.

Diaspora activists operate in "transnational fields" with ties across multiple countries and communities (Levitt & Schiller 2004). In these networks, a successful attack against the weakest link could lead to severe consequences for all involved. The interviews show that activists often do not have the time, resources, or capacity to make security decisions based on nuanced risk assessment and factual knowledge. Their security models reflect the complex techno-political environment in which they must navigate, and are shaped by the "imagined affordances" of digital technologies, emerging from expectations, fears, and everyday use (Nagy & Neff 2015, Lyon 2017). Reports on successful hacking and surveillance operations or new security flaws in popular applications, for instance, can overwhelm activists and lead to feelings of resignation and 'security paralysis'.

The paper argues that the complexity of today's digital communication tools and the constant evolution of threats only work to aggravate the feelings of uncertainty that activists experience with regards to the aims and capabilities of repressive state actors – and thus risk exacerbating the silencing effects of surveillance and transnational repression. In turn, activists feel more empowered and resilient when they have close ties to local and global networks for incident response, support, and information sharing on digital security. Bringing critical media studies in dialogue with research on transnational diaspora activism and authoritarian politics, the paper answers calls for more research into the social construction of risk and security of human rights defenders, in particular its mediation by digital technologies (Bennett et al. 2015; Kazansky 2015). By focusing on high-risk users and frontline defenders, the paper further contributes to the literature investigating the contentious politics and power inequalities that form around digital technology, especially from a bottom-up perspective (e.g. Beraldo & Milan 2019; Guerses, Kundnani & Van Hoboken 2016).

References

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.

Bennett, K., Ingleton, D., Nah, A. M., & Savage, J. (2015). Critical perspectives on the security and protection of human rights defenders. *The International Journal of Human Rights*, *19*(7), 883-895.

Beraldo, D., & Milan, S. (2019). From data politics to the contentious politics of data. *Big Data & Society*, *6*(2).

Bernal, V. (2014). *Nation as network: Diaspora, cyberspace, and citizenship*. University of Chicago Press.

Brinkerhoff, J. M. (2009). *Digital diasporas: Identity and transnational engagement*. Cambridge University Press.

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

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.

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

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., & Clunaigh, D. Ó. (2013). Rethinking Risks and Security of Human Rights Defenders in the Digital Age. *Journal of Human Rights Practice 5*(3), 535-547.

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

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

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

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

Michaelsen, M. (2020). Silencing Across Borders: Transnational Repression and Digital Threats Against Exiled Activists from Egypt, Syria, and Iran. Hivos. https://www.hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf

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

Nagy, P., & Neff, G. (2015). Imagined affordance: Reconstructing a keyword for communication theory. *Social Media+ Society*, *1*(2).