



RESEARCH ARTICLE

Drawing a line: Digital transnational repression against political exiles and host state sovereignty

Marcus Michaelsen*  and Johannes Thumfart 

The Law, Science, Technology and Society (LSTS) Research Group, Vrije Universiteit Brussel, Brussels, Belgium

*Corresponding author. Email: email@marcusmichaelsen.eu

(Received 17 December 2021; revised 8 July 2022; accepted 17 August 2022)

Abstract

Authoritarian regimes increasingly resort to surveillance and malware attacks to extend their coercive reach into the territory of other states and silence dissidents abroad. Recent scholarship has examined the methods of digital transnational repression and their detrimental effects on the fundamental rights and security of targeted individuals. However, the broader normative and security dimensions of these practices remain underexplored, especially with regard to the states hosting the affected exiles. Addressing this gap, our article investigates digital transnational repression as a potential violation of host state sovereignty. Mobilising emerging research on digital sovereignty and cybersecurity, we argue that digital repression can violate host state sovereignty in that it constitutes extraterritorial enforcement jurisdiction; interferes with open debate and national self-determination; impedes the host state's adherence to fundamental norms of international humanitarian law; and undermines host state authority, domestic sovereignty, and integrative capacities. We outline possible pathways to counter digital transnational repression, focusing notably on distributed cyber deterrence, punitive measures like sanctions, and norms and regulations restricting the global proliferation of offensive cyber capabilities. Building on a post-territorial notion of sovereignty that centres on the effects of state actions in and beyond cyberspace, our article contributes to reflections on a human-centric approach to cybersecurity.

Keywords: Digital Transnational Repression; Extraterritorial Coercion; Sovereignty; Cyberspace; Authoritarianism; Diaspora

Introduction

Authoritarian governments increasingly reach across borders to threaten dissidents and opponents residing in other countries.¹ The 2018 assassination of exiled journalist Jamal Khashoggi in Saudi Arabia's consulate in Istanbul reveals the great lengths repressive rulers will go to silence opponents abroad. Regimes engaging in transnational repression rely on a range of tactics, from Interpol listings, renditions, and assaults to pressure on home country relatives and online harassment.² Given their border-blurring qualities, digital technologies are essential components in the toolkit of extraterritorial coercion. Practices of *digital transnational repression* ('DTR') include surveillance and hacking attacks, online harassment, and disinformation campaigns against

¹Saipira Furstenberg, Edward Lemon, and John Heathershaw, 'Spatialising state practices through transnational repression', *European Journal of International Security* (2021), pp. 1–21; Marlies Glasius, 'Extraterritorial authoritarian practices: A framework', *Globalizations*, 15:2 (2018), pp. 179–97; Dana M. Moss, 'Transnational repression, diaspora mobilization, and the case of the Arab Spring', *Social Problems*, 63:4 (2016), pp. 480–98.

²Nate Schenkkan and Isabel Linzer, *Out of Sight, Not Out of Reach: Understanding Transnational Repression* (Freedom House, February 2021), available at: {<https://freedomhouse.org/report/transnational-repression>}.

The online version of this article has been updated since original publication. A notice detailing the change has been published at <https://doi.org/10.1017/eis.2023.23>

migrants with ties to authoritarian countries.³ They provide repressive regimes with ways to monitor and respond to the activities of exiles with greater scope and speed.⁴ Moreover, these digital threats are often intertwined with traditional methods of extraterritorial coercion, preparing or triggering an escalation of threats. In the Khashoggi case, the Saudi regime decided to go ahead with the operation against the journalist after it had penetrated the smart phone of one of his close associates living in Canada and apprehended details of the projects the two dissidents were planning.⁵

Despite the increasing occurrence of DTR and the potentially severe consequences for the personal lives and political activities of those targeted, its normative implications and security dimensions remain underexplored, particularly with regard to the states hosting the affected exiles. Digital threats against civil society are typically considered as human rights violations, infringing on the rights to privacy and freedom of expression, among others.⁶ However, the human rights approach primarily shines a spotlight on the relation between the authoritarian state as rights violator and its 'subjects' abroad, thereby obscuring the role and interests of the host state. Only recently research has turned to investigating host governments' obligations under international humanitarian law and their responses to transnational repression.⁷

While we believe that it is necessary and urgent to continue pursuing the issue under a human rights framework, in this article we explore an alternative approach and consider practices of DTR as sovereignty violations against the state hosting the targeted migrants, both in a juridical and a political sense. We argue that acts of DTR can violate state sovereignty in that they constitute extraterritorial enforcement jurisdiction; distort public debate and interfere with national self-determination; and impede the host state's adherence to fundamental norms of international humanitarian law. In addition to these three normative arguments grounded in international law, we stress that DTR is also contrary to states' self-interest: by weakening government institutions, rule of law, and social cohesion in the receiving countries of political exiles, practices of DTR undermine the host state's internal authority, domestic sovereignty, and capacity to successfully integrate immigrants.⁸

³Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Adam Senft, and Ron Deibert, *Annotated Bibliography: Digital Transnational Repression* (Citizen Lab, University of Toronto: November 2020), available at: {<https://citizenlab.ca/2020/11/annotated-bibliography-transnational-digital-repression/>}.

⁴Marcus Michaelsen, 'Exit and voice in a digital age: Iran's exiled activists and the authoritarian state', *Globalizations*, 15:2 (2018), pp. 248–64; Marcus Michaelsen, *Silencing Across Borders: Digital Threats and Transnational Repression against Exiled Activists from Egypt, Syria and Iran* (Research Report for Hivos, The Hague), available at: {<https://hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf>}.

⁵Office of the High Commissioner for Human Rights, 'Khashoggi Killing: UN Human Rights Expert Says Saudi Arabia Is Responsible for "Premeditated Execution"' (19 June 2019), available at: {<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24713>}.

⁶United Nations Human Rights Council, 'Surveillance and Human Rights', Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2019), available at: {<https://digitallibrary.un.org/record/3814512>}.

⁷Siena Anstis and Sophie Barnett, 'Digital transnational repression and host states' obligation to protect against human rights abuses', *Journal of Human Rights Practice* (2022); Yana Gorokhovskaia and Isabel Linzer, *Defending Democracy in Exile: Policy Responses to Transnational Repression* (Freedom House, June 2022), available at: {<https://freedomhouse.org/report/transnational-repression>}; Marko Milanovic, 'The murder of Jamal Khashoggi: Immunities, inviolability and the human right to life', *Human Rights Law Review*, 20:1 (2020), pp. 1–49; Dana M. Moss and Don Picard, 'Countering transnational repression using international law', in Dana M. Moss and Saipira Furstenberg (eds), *Transnational Repression in the Global Age*, manuscript in progress.

⁸Krasner distinguishes between four meanings of sovereignty: domestic, interdependence, Westphalian, and international legal sovereignty. The two most relevant types for this study are domestic sovereignty, which refers to the organisation and level of control of public authority within a state, and Westphalian sovereignty, 'referring to the exclusion of external actors from domestic authority configurations'. Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 1999), p. 9.

Framing transnational repression as a violation of sovereignty has two advantages: First, it spells out more clearly the ways in which practices of extraterritorial authoritarian rule interfere with the interests and authority of other states, underlining that transnational repression does not threaten ‘only foreigners’, but also raises security issues for the host state. Even Western democracies are at times reluctant to apply the language of human rights to cases of extraterritorial repression, given their own use of force in counterterrorism operations abroad.⁹ Foregrounding the aspect of sovereignty violation highlights the normative *and* strategic relevance to counter DTR. This focus might push host country governments more effectively to meet their obligations for protecting the targeted individuals as well as society more broadly against such practices. Second, emphasising sovereignty violations caused by DTR meets the main perpetrators on their own discursive grounds. Regimes engaging in transnational repression and human rights violations, such as China and Russia, typically stress the normative importance of state sovereignty and condemn external interference, including in the context of digital technologies.¹⁰ Among other instances where these regimes have violated state sovereignty in a more drastic sense, their extraterritorial practices in the context of DTR are clearly at odds with this rhetoric.¹¹ As the ‘only generally acceptable and practical normative basis of world politics’,¹² the notion of sovereignty could help establish an inclusive discourse for condemning and curtailing DTR across political divides.

Our arguments should be read with the following clarifications in mind. First, our emphasis on the integrity of state sovereignty is not a return to a brand of realism that conceives of national security as an end in itself. On the one hand, stressing that the principles associated with sovereignty are frequently violated, a purely realist view would likely register DTR as a rather low-intensity transgression and subordinate potential answers to the interest of stability and other strategic priorities.¹³ On the other hand, any response to DTR primarily focusing on national security and ignoring the needs of civil society would run the risk of furthering the securitisation of the digital sphere that is already unfolding in relation to other, similar phenomena, such as the spreading of misinformation across borders.¹⁴ Instead, we follow a broadly liberal approach that considers sovereignty as essential to guarantee the rule of law, particularly individual rights and human security within a given territory.¹⁵ In the context of digital technologies, this perspective corresponds to a ‘human-centric approach to cybersecurity’.¹⁶

⁹Marko Milanovic, ‘The Salisbury attack: Don’t forget human rights’, *EJIL: Talk!* (15 March 2018), available at: {<https://www.ejiltalk.org/the-salisbury-attack-dont-forget-human-rights/>}.

¹⁰Sarah McKune and Shazeeda Ahmed, ‘The contestation and shaping of cyber norms through China’s Internet sovereignty agenda’, *International Journal of Communication*, 12 (2018), pp. 3835–55; Johannes Thumfart, ‘The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the Covid-crisis 2020/21 as catalytic event’, in Dara Hallinan, Ronald Leenes, and Paul de Hert (eds), *Enforcing Rights in a Changing World*, Computers Privacy Data Protection (CPDP), 14 (London, UK: Hart Publishing, 2021), pp. 1–44.

¹¹David Lewis, ‘“Illiberal spaces”: Uzbekistan’s extraterritorial security practices and the spatial politics of contemporary authoritarianism’, *Nationalities Papers*, 43:1 (2015), pp. 140–59 (p. 142).

¹²Robert Jackson, ‘Sovereignty in world politics: A glance at the conceptual and historical landscape’, *Political Studies*, 47 (1999), pp. 431–56 (p. 456).

¹³Krasner, *Sovereignty*.

¹⁴Lene Hansen and Helen Nissenbaum, ‘Digital disaster, cyber security, and the Copenhagen School’, *International Studies Quarterly*, 53:4 (2009), pp. 1155–75; Bryan C. Taylor, ‘Defending the state from digital deceit: The reflexive securitization of deepfake’, *Critical Studies in Media Communication*, 38:1 (2021), pp. 1–17; Joyce Hakmeh et al., ‘The COVID-19 Pandemic and Trends in Technology: Transformations in Governance and Society’ (Chatham House, February 2021), p. 30, available at: {<https://www.chathamhouse.org/sites/default/files/2021-02/2021-02-16-covid-19p.-trends-technology-hakmeh-et-al.pdf>}.

¹⁵Keith Krause, ‘Towards a Practical Human Security Agenda’, DCAF Policy Paper 26 (Geneva, 2007), available at: {<https://www.dcaf.ch/sites/default/files/publications/documents/PP26.pdf>}; Anne Peters, ‘Humanity as the A and Ω of sovereignty’, *European Journal for International Law*, 20:3 (2009), pp. 513–44; Jeremy Waldron, ‘Are sovereigns entitled to the benefit of the international rule of law?’, *European Journal for International Law*, 22:2 (2011), pp. 315–43.

¹⁶Ronald J. Deibert, ‘Toward a human-centric approach to cybersecurity’, *Ethics & International Affairs*, 32:4 (2018), pp. 411–24.

Second, while focusing on sovereignty, we acknowledge that the transnational nature of digital networks is principally in tension with the concept of territorially bounded sovereignty. In cases of DTR, we will show, conventional notions of sovereignty mean that perpetrators remain unpunished because they never physically enter another state's geographical territory when committing these acts. However, we reject assumptions that sovereignty is particularly threatened or obsolete because of the Internet's global diffusion.¹⁷ Such arguments 'represent classical "Westphalian" sovereignty as far more complete than even the most powerful state ever managed to achieve historically'.¹⁸ In contrast, we build on 'post-territorial'¹⁹ or 'elastic'²⁰ conceptualisations of sovereignty that adapt and reconfigure sovereign authority in order to meet the challenges of the digital age.

Third, and following from the above, we concur with approaches that view sovereignty as a social construct; as a result of practices that 'produce, reform, and redefine sovereignty and its constitutive elements: population, recognition, authority, and territory'.²¹ The construction of state sovereignty is a process of drawing boundaries – not only to demarcate a specific territory or determine political authority, but also to impose 'meanings about who belongs and who does not belong to the nation'.²² Research in critical migration and security studies has analysed this inclusionary/exclusionary function of sovereignty as a mechanism for 'othering' and securitising immigrants.²³ As a consequence, exiles and diasporas often find themselves in a grey zone between the authoritarian home state that 'treats its subjects abroad as if they were still under territorial jurisdiction'²⁴ and the host state failing to accord them full access to a political community 'that defends and upholds one's right to have rights'.²⁵ Instead of marginalising immigrants and their security needs, we suggest stretching the protective boundaries drawn by sovereignty to exclude the authoritarian practices that often follow them across borders.

Our article brings research on globalised authoritarian repression in dialogue with international law and scholarship on digital sovereignty and cyber security. After summarising the relevant debates, our empirical section provides a more detailed picture of DTR, its methods and effects on diasporas and their host societies. We then present three legal arguments and one political argument clarifying the ways in which DTR can be understood as a sovereignty violation. We also outline possible pathways for countering DTR, focusing on distributed cyber security, law enforcement activities, sanctions, and international norm development. In concluding, we discuss the political conditions that would facilitate a more stringent countering of DTR and outline a horizon for further research.

¹⁷Milton Mueller, 'Against sovereignty in cyberspace', *International Studies Review*, 22:4 (2020), pp. 779–80; Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, *Digital Futures* (Cambridge, UK: Polity Press, 2017); Jack L. Goldsmith, 'Against cyberanarchy', *The University of Chicago Law Review*, 65:4 (1998), pp. 1199–250.

¹⁸Daniel R. McCarthy, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and the Internet* (New York, NY: Palgrave Macmillan, 2015), p. 32.

¹⁹Paul De Hert and Johannes Thumfart, 'The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma: Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies', Brussels Privacy Hub Working Papers 4, No. 11 (July 2018), available at: <https://brusselsprivacyhub.eu/publications/BPH-Working-Paper-VOLA-N11.pdf>.

²⁰Roxana Vatanparast, 'Data governance and the elasticity of sovereignty', *Brooklyn Journal of International Law*, 46:1 (2020), available at: <https://brooklynworks.brooklaw.edu/bjil/vol46/iss1/1/>.

²¹Thomas J. Biersteker and Cynthia Weber (eds), *State Sovereignty as Social Construct*, Cambridge Studies in International Relations, 46 (Cambridge, UK: Cambridge University Press, 1996), p. 11.

²²Roxanne L. Doty, 'Sovereignty and the nation: Constructing the boundaries of national identity', in Biersteker and Weber, *State Sovereignty*, pp. 121–47 (p. 142).

²³Didier Bigo, 'Security and immigration: Toward a critique of the governmentality of unease', *Alternatives*, 27 (2002), pp. 63–92; Bastian A. Vollmer, 'Categories, practices and the self: Reflections on bordering, ordering and othering', *Tijdschrift voor economische en sociale geografie*, 112 (2021), pp. 4–10.

²⁴Marlies Glasius, 'The extraterritorial gap', in Emanuela Dalmasso, Adele Del Sordi, Marlies Glasius, Nicole Hirt, Marcus Michaelsen, Abdulkader S. Mohamud, and Dana Moss, 'Intervention: Extraterritorial authoritarian power', *Political Geography*, 64 (2018), pp. 95–104 (p. 96).

²⁵Seyla Benhabib, *Exile, Statelessness, and Migration: Playing Chess with History from Hannah Arendt to Isaiah Berlin* (Princeton, NJ: Princeton University Press, 2018), p. 20.

Extraterritorial authoritarian rule and transnational repression

Transnational repression is considered a response of authoritarian governments to intensified cross-border flows of migration and information.²⁶ A fundamental aim of regimes who coerce populations abroad is ‘to enhance regime security’ and to strengthen their position, both domestically and on the international level.²⁷ Authoritarian rulers seek to contain exiles whose positions risk to gain traction and mobilise challengers inside the country. They also try to silence critics whose claims may increase international pressure and shape the international environment in ways opposing regime interests.²⁸ Among the targets of transnational repression are exiled human rights defenders, journalists, and political opponents as well as former regime insiders, ethnic and religious minorities; they range from recent refugees and emigrants to second-generation diaspora members.²⁹

Extending domestic coercion across borders, ‘contemporary authoritarian rule structures socio-political space in ways that partially transcend both territorial jurisdiction and geographical distance.’³⁰ At the same time, authoritarian extraterritorial rule highlights a power shift in the international system. Global freedom declined for the fifteenth consecutive year in 2020, continuing a trend of democratic recession.³¹ As emboldened authoritarian rulers persecute their opponents across borders, they challenge the norms and values of liberal democracies and the rules-based multilateral order.³² Acts of transnational repression are typically embedded in practices that include ‘media and disinformation campaigns, the co-optation and corruption of host country officials and elites, building alliances with antiliberal parties and movements, and sponsoring cyberattacks’.³³

While the literature shows how transnational repression reproduces the coercive power of the state outside its territorial boundaries, it does not raise the question of how these practices interfere with the security and sovereignty of the host state in which the targeted migrants reside. Mainstream state-centric approaches in international relations and security studies have difficulties to capture state repression against individuals in other countries because these practices do not match established categories of interstate competition.³⁴ Shifting from a national to an ‘entangled global’ perspective on security, however, opens up ‘new possibilities for understanding a range of security relationships and issues, bringing new actors and spaces into our understanding of global security’.³⁵ Considering security as a sociospatial practice permits disaggregating how host states are affected by and responding to acts of transnational repression. Digital threats, in particular, unfold in constellations of actors, networks, and infrastructures that span across

²⁶Gerasimos Tsourapas, ‘Global autocracies: Strategies of transnational repression, legitimation, and co-optation in world politics’, *International Studies Review*, 23:3 (2021), pp. 616–44.

²⁷Alexander Dukalskis, *Making the World Safe for Dictatorship* (Oxford, UK: Oxford University Press, 2021), p. 25.

²⁸Ibid.

²⁹When diasporas are targeted with transnational repression by an authoritarian government in their origin country, it is often for exercising their fundamental rights and expressing some form of dissent. However, not all politically active diasporas are engaging in anti-authoritarian activism nor do their political goals necessarily align with the interests and values of the host country. See, for example, Fiona Adamson, ‘Non-state authoritarianism and diaspora politics’, *Global Networks*, 20:1 (2020), pp. 150–69.

³⁰Glasius, ‘Extraterritorial gap’, p. 96.

³¹Freedom House, ‘Democracy under Siege’ (2021), available at: <https://freedomhouse.org/report/freedom-world/2021/democracy-under-siege>.

³²Alexander Cooley, ‘Authoritarianism goes global: Countering democratic norms’, *Journal of Democracy*, 26:3 (2015), pp. 49–63; Nate Schenkkan, ‘The authoritarian assault on exiles’, *Foreign Affairs* (May 2021), available at: <https://www.foreignaffairs.com/articles/belarus/2021-05-27/authoritarian-assault-exiles>.

³³Schenkkan and Linzer, *Out of Sight Not Out of Reach*, p. 7.

³⁴Fiona Adamson, ‘No Escape: Long-Distance Repression, Extraterritorial States and the Underworld of IR’, paper presented at the 2019 European Consortium of Political Research Joint Sessions of Workshops, April 2019.

³⁵Fiona Adamson and Kelly M. Greenhill, ‘Globality and entangled security: Rethinking the post-1945 order’, *New Global Studies*, 15:2–3 (2021), pp. 165–80 (p. 166).

divides between democratic and authoritarian governments, private and non-state actors.³⁶ Examining acts of DTR as sovereignty violations is thus closely linked to ongoing debates about the conceptual tension between the Internet as a globally distributed network and the sovereignty of states, commonly conceived of as territorially bounded.

Territory and sovereignty in cyberspace

While respect for state sovereignty in cyberspace constitutes a broad consensus across geopolitical fronts, it remains a contested issue, both conceptually and practically. The contrast between the networked character of the Internet and the territorially bounded nature of the nation-state even led to assertions that cyberspace establishes a form of transnational technological sovereignty distinct from the nation-state.³⁷ This idea has been labelled *cyberspace exceptionalism*.³⁸ In popular culture, it found expression in John Perry Barlow's famous 'Declaration of the Independence of Cyberspace'.³⁹ Others argued that cyberspace poses a 'threat to sovereignty'⁴⁰ or could bring about 'cyber anarchy'.⁴¹ In practical terms, the relation between sovereignty and cyberspace raises a number of concrete jurisdictional conflicts concerning the regulation of domains as diverse as law enforcement, taxation, hate speech, and product piracy.⁴²

Diagnosing a 'jurisdictional paradox', Milton Mueller argues that if states enforced their sovereignty in the context of digital technologies, they would need to act extraterritorially, thus destroying 'the whole model of national sovereignty'.⁴³ While this view is obviously exaggerated and grounded in a traditional notion of territorial sovereignty, it is correct that states can hardly protect the rights of their citizens online without resorting to extraterritorial jurisdiction. Relying on a so-called destination approach, the European Union's General Data Protection Regulation (GDPR), for instance, regulates websites accessible from within the Union's borders rather than only those hosted on servers located in the EU. In contrast, the 'data-controller approach' of the CLOUD act in the United States allows law enforcement to access data stored by US-based cloud services, regardless of where the data is physically located. Another example is taxation that touches upon the economic essence of sovereignty: the government of France currently leads an initiative to tax companies offering services in the country's digital market but not necessarily based on French territory.⁴⁴

What these emerging approaches to the regulation of digital data and services have in common is that they move beyond the 'monopolistic spatiality of territorial sovereignty'.⁴⁵ Adapting state authority and jurisdiction to a new technological environment, they create 'regulatory territories

³⁶Marlies Glasius and Marcus Michaelsen, 'Illiberal and authoritarian practices in the digital sphere', *International Journal of Communication*, 12 (2018), pp. 3795–813, available at: {<https://ijoc.org/index.php/ijoc/article/view/8899>}; Johannes Thumfart, 'Public and private just wars: Distributed cyber deterrence based on Vitoria and Grotius', *Internet Policy Review* (2020), available at: {<https://policyreview.info/articles/analysis/public-and-private-just-wars-distributed-cyber-deterrence-based-vitoria-and>}.

³⁷Tim Wu, 'Cyberspace sovereignty? The Internet and the international system', *Harvard Journal of Law & Technology*, 10:3 (1997), pp. 647–66.

³⁸Julie Cohen, 'Cyberspace as/and space', *Georgetown Law Faculty Publications* (January 2007), available at: {<https://scholarship.law.georgetown.edu/facpub/807/>}; Mireille Hildebrandt, 'Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace', *University of Toronto Law Journal*, 63:2 (2013), pp. 196–224 (p. 202).

³⁹John Perry Barlow, 'A Declaration of the Independence of Cyberspace', Electronic Frontier Foundation, available at: {<https://www.eff.org/de/cyberspace-independence>}.

⁴⁰Henry Perritt, 'The Internet as a threat to sovereignty? Thoughts on the Internet's role in strengthening national and global governance', *Indiana Journal of Global Legal Studies*, 423 (1998), available at: {<https://www.repository.law.indiana.edu/ijgl/vol5/iss2/4/>}.

⁴¹Jack L. Goldsmith, 'Against cyberanarchy', *The University of Chicago Law Review*, 65:4 (1998), pp. 1199–250.

⁴²Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge, UK: Cambridge University Press, 2007).

⁴³Mueller, *Will the Internet Fragment?*, p. 92.

⁴⁴Wei Cui, 'The digital services tax: A conceptual defense', *Tax Law Review*, 73 (2019), pp. 69–112.

⁴⁵Hildebrandt, 'Extraterritorial jurisdiction'.

of extraterritorial reach'.⁴⁶ The flexible exercise of sovereignty is not new and unique to data governance. States frequently modify their spatial reach, bending and stretching their authority in relation to geographical space.⁴⁷ The geographical understanding of territory itself is only a simplifying reification of a far more complex reality of social practices that actively construct territory by communicating boundaries, asserting power, and claiming authority.⁴⁸ In the context of digital technologies, sovereignty is conceptualised as 'elastic'⁴⁹ and 'post-territorial'⁵⁰ because the limits of state jurisdiction are not based on the mere factuality of geographical territoriality, but on specific normative principles, such as the protection of the fundamental rights of 'data subjects' in the case of the GDPR.

Sovereignty violations and countermeasures in the digital age

The demarcation of state sovereignty in the digital realm is closely linked to questions of how to define sovereignty violations and legitimate countermeasures in cyberspace. There is broad consensus on the legitimacy of direct reprisals to cyberattacks destroying physical infrastructure on foreign soil, such as the Stuxnet-attacks on Iran's nuclear facilities. More relevant for the discussion of DTR, however, are sovereignty violations below the threshold of physical impact, such as Russia's interference in the campaign for the 2016 US presidential elections. Although the NATO's Tallinn Manual on the application of international law to cyber conflict affirms that 'a State may not intervene, including by cyber means, in the internal or external affairs of another State', it does not elaborate in more detail on sovereignty violations without physically violent effects.⁵¹ While some consider the Russian meddling as part of an espionage operation without a coercive element, others argue that such interference still constitutes a violation of self-determination because 'the election process is the ultimate expression of a people's sovereign will'.⁵² Nicholas Tsagourias goes even further and points to the potential coerciveness of election interference in that it allows for external control over a state.⁵³

Assessing digitally enabled non-violent sovereignty violations is not only complicated by the wide scope of international law for interpretation, but also the problem of attribution. The anonymity that the Internet offers facilitates false-flag operations. States also deliberately send ambiguous signals, when being accused of a cyberattack in order to shape perceptions of their capabilities and resolve.⁵⁴ Moreover, governments are often unwilling to publicly reveal evidence leading to attribution when it is obtained in intelligence operations. In general, the public attribution of cyber intrusions is a complex process with considerable risks, which requires 'a clear understanding of the attributed cyber operation and the cyber threat actor, but also the broader geopolitical environment, allied positions and activities, and the legal context'.⁵⁵

⁴⁶Daniel Lambach, 'The territorialization of cyberspace', *International Studies Review*, 22:3 (2020), pp. 482–506.

⁴⁷Ran Hirsch and Ayelet Shachar, 'Spatial statism', *International Journal of Constitutional Law*, 17:2 (2019), pp. 387–438.

⁴⁸Lambach, 'The territorialization of cyberspace', p. 488.

⁴⁹Vatanparast, 'Data governance and the elasticity of sovereignty'.

⁵⁰De Hert and Thumfart, 'The Microsoft Ireland Case'.

⁵¹Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017), p. 312; Przemysław Roguski, 'Violations of territorial sovereignty in cyberspace: An intrusion-based approach', in D. Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy, Digital Technologies and Global Politics* (Lanham, MD: Rowman & Littlefield, 2020), pp. 65–84.

⁵²Jens David Ohlin, 'Did Russian cyber interference in the 2016 election violate international law?', *Texas Law Review*, 95:7 (2017), pp. 1579–98; William Banks, 'State responsibility and attribution of cyber intrusions after Tallinn 2.0', *Texas Law Review*, 95:7 (2017).

⁵³Nicholas Tsagourias, 'Electoral cyber interference, self-determination, and the principle of non-intervention in cyberspace', in Broeders and van den Berg (eds), *Governing Cyberspace*, pp. 45–63 (p. 46).

⁵⁴Joseph M. Brown and Tanisha M. Fazal, '#SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations', *European Journal of International Security*, 6:4 (2021), pp. 1–17.

⁵⁵Florian J. Egloff and Max Smeets, 'Publicly attributing cyber attacks: A framework', *Journal of Strategic Studies* (2021), pp. 1–32.

Current scholarship on cyber security broadly agrees that the attribution problem as well as the proliferation of state and non-state threat actors, low thresholds for executing potentially damaging attacks and other factors thwart the effectiveness of conventional deterrence mechanisms that seek to prevent attacks by threatening retaliation with comparable means and severity.⁵⁶ Most cyberattacks resemble less a military confrontation than intelligence and subversion operations.⁵⁷ Much like traditional campaigns of espionage and sabotage, cyber operations exploit vulnerabilities to ‘secretly infiltrate a system of rules and practices in order to control, manipulate, and use the system to produce detrimental effects against an adversary’.⁵⁸ Consequently, some authors recommend strategies of ‘deterrence by denial’ aiming ‘to increase an adversary’s difficulty in conducting its own offensive cyber operations’.⁵⁹ Means range from improved resilience and defence mechanisms to the exposure of adversary tactics and the active disruption of their ability to carry out attacks.

Complementary approaches to cyber deterrence emphasise the necessary contribution of the private sector and civil society.⁶⁰ Taking orientation from concepts of civilian-based deterrence developed during the Cold War, a system of ‘distributed cyber deterrence’⁶¹ could involve even individuals with particular resources and impact, such as hackers and whistleblowers, to convince ‘potential attackers not to commit an aggressive or hostile act because certain consequences would follow which they would prefer to avoid’.⁶² Comparable ideas are also reflected in policy approaches such as the ‘whole-of-society-approach’ promoted in the EU, which emphasise the involvement of the technology sector and civil society to counter cyber operations and other hybrid threats.⁶³ Although these approaches stress the role of civil society, they primarily focus on attacks on public and private infrastructure and nation-state conflicts and thereby largely ignore state-sponsored transnational attacks targeting individual actors in civil society. Our investigation of how digital repression against exiled dissidents and diasporas undermines the security and sovereignty of their host states addresses this gap.

Silencing across borders: Digital transnational repression

Digital threats have become a core component in the repertoire of authoritarian governments engaging in transnational repression. Of the 31 states a Freedom House investigation documented having committed acts like assaults, renditions, and assassinations against exiles between 2014 and 2020, 21 also used some form of digital threat and at least 17 relied on spyware to target individuals outside their territory. Perpetrators included global players such as Russia and

⁵⁶Mariarosaria Taddeo, ‘Deterrence and norms to foster stability in cyberspace’, *Philosophy & Technology*, 31:3 (2018), pp. 323–9; Joseph S. Nye, ‘Deterrence and dissuasion in cyberspace’, *International Security*, 41:3 (2017), pp. 44–71.

⁵⁷Erik Gartzke and Jon R. Lindsay, ‘Weaving tangled webs: Offense, defense, and deception in cyberspace’, *Security Studies*, 24:2 (2015), pp. 316–48; Joshua Rovner, ‘Cyber war as intelligence contest’, *War on the Rocks* (16 September 2019), available at: {<https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest>}.

⁵⁸Lennart Maschmeyer, ‘The subversive trilemma: Why cyber operations fall short of expectations’, *International Security*, 46:2 (2021), pp. 51–90 (p. 54).

⁵⁹Erica D. Borghard and Shawn W. Lonergan, ‘Deterrence by denial in cyberspace’, *Journal of Strategic Studies* (2021), p. 22.

⁶⁰Eugenio Lilli, ‘Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence’, *Contemporary Security Policy*, 42:2 (2021), pp. 163–88.

⁶¹Thumfart, ‘Public and private just wars’.

⁶²Gene Sharp, *Making Europe Unconquerable: The Potential of Civilian-Based Deterrence and Defence* (Cambridge, MA: Ballinger Publishing Company, 1985), p. 34.

⁶³Mikael Wigell, Harri Mikkola, and Tapio Juntunen, ‘Best Practices in the Whole of Society Approach in Countering Hybrid Threats’ (European Parliament, May 2021), available at: {<https://www.europarl.europa.eu/committees/de/best-practices-in-the-whole-of-society-a/product-details/20210531CAN61132>}. In the United States, a similar approach to cyber security involving national security agencies and the private sector is termed ‘layered security’. Cyberspace Solarium Commission, Final Report (March 2020), available at: {https://drive.google.com/file/d/1ryMCIL_dZ30QyFqFkkf10MxIXJGT4yv/view}.

China, regional powers like Saudi Arabia, and smaller states, such as Kazakhstan and Vietnam.⁶⁴ For these regimes, digital threats against exiled opponents reduce the costs of extraterritorial political control. They no longer need to send agents abroad to spy on and intimidate critics in the diaspora. With minimal costs and risk of consequences, a successful hacking attack against a single activist in the diaspora can expose a trove of confidential communications and unravel entire networks, including home country associates in direct reach of regime authorities.⁶⁵ The combination with other methods of transnational repression increases the effects of digital threats so that they often succeed in fostering uncertainty, fear, and mistrust within diaspora communities, reinforcing dynamics of self-censorship and silencing.⁶⁶

DTR also impacts the position, relations, and activities of individuals with ties to authoritarian contexts in their society of residence. Members of the Uyghur diaspora across the world, for instance, are reluctant to speak openly about China's extensive repression campaign against their people for fear of severe repercussions for their families in Xinjiang. Uyghur exiles reported that their calls and social media communications were being monitored; they even received threatening phone calls from police agents using the accounts and devices of family members. Chinese authorities have used surveillance and threats against relatives to silence publicly outspoken Uyghur activists in countries like Germany, France, and the United States.⁶⁷ These cases highlight that, in addition to infringing on the privacy and autonomy of targeted exiles, practices of transnational repression curtail their ability to partake in the social and political life of host countries, sabotaging public debate and accountability processes.⁶⁸

The authoritarian reach across borders is not limited to exile and diaspora communities. The tools and techniques that regimes deploy against their populations abroad can also spill over into host countries. In fact, cyber threat actors attacking civil society and diaspora groups are often identical or overlap with those going after foreign targets. Vietnamese human rights defenders and journalists based in Germany, for instance, were persistently attacked with malware attributed to the 'Ocean Lotus' group which is suspected of working in alignment with the Vietnamese government since at least 2012 and has also targeted foreign officials and companies.⁶⁹ Iranian hacking groups are known to hone their methods on civil society before reaching for more complex targets abroad.⁷⁰ The revelations around the widespread abuse of the NSO Group's Pegasus

⁶⁴Schenkkan and Linzer, *Out of Sight Not Out of Reach*.

⁶⁵Fiona B. Adamson and Gerasimos Tsourapas, 'At Home and Abroad: Coercion-by-Proxy as a Tool of Transnational Repression', Freedom House Special Report (2020), available at: <https://freedomhouse.org/report/special-report/2020/home-and-abroad-coercion-proxy-tool-transnational-repression>; Dana M. Moss, Marcus Michaelsen, and Gillian Kennedy, 'Going after the family: Transnational repression and the proxy punishment of Middle Eastern diasporas', *Global Networks*, 22:4 (2022), pp. 735–51.

⁶⁶Noura Aljizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonardt, Adam Senft, and Ron Deibert, 'Digital transnational repression in Canada', *The Citizen Lab* (2020), available at: https://citizenlab.ca/wp-content/uploads/2022/03/Report151-dtr_022822.pdf; Michaelsen, *Silencing Across Borders*.

⁶⁷Amnesty International, 'Nowhere Feels Safe: Uyghurs Tell of China-Led Intimidation Campaign Abroad' (21 February 2020), available at: <https://www.amnesty.org/en/latest/research/2020/02/china-uyghurs-abroad-living-in-fear/>; Bradley Jardine and Natalie Hall, 'Your Family Will Suffer: How China is Hacking, Surveilling, and Intimidating Uyghurs in Liberal Democracies' (Uyghur Human Rights Project (UHRP) and Oxus Society for Central Asian Affairs, 2021), available at: <https://uhrp.org/report/your-family-will-suffer-how-china-is-hacking-surveilling-and-intimidating-uyghurs-in-liberal-democracies/>.

⁶⁸Glasius and Michaelsen, 'Illiberal and authoritarian practices'; see also Marlies Glasius, 'What authoritarianism is ... and is not: A practice perspective', *International Affairs*, 94:3 (2018), pp. 515–33.

⁶⁹Amnesty International, 'Click and Bait: Vietnamese Human Rights Defenders Targeted with Spyware Attacks' (24 February 2021), available at: <https://www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-targeted-with-spyware-attacks/>; 'Facebook tracks "OceanLotus" hackers to IT firm in Vietnam', *Reuters* (11 December 2020), available at: <https://www.reuters.com/article/facebook-vietnam-cyber-idUSKBN28L03Y>.

⁷⁰Karim Sadjadpour and Collin Anderson, 'Iran's Cyber Threat: Espionage, Sabotage, and Revenge' (Carnegie Endowment for International Peace, 2018), available at: <https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-espionage-sabotage-and-revenge-pub-75134>.

surveillance tool provide the most striking illustration of how closely digital threats against individual dissidents are linked to the security of their broader host society. A number of authoritarian governments used the powerful spyware not only against their own nationals, at home and abroad, but also a range of foreign targets, including journalists, lawyers, and high-ranking politicians.⁷¹ The Saudi regime infiltrated the smartphone of Jeff Bezos, CEO of Amazon and owner of the *Washington Post*, the newspaper in which Khashoggi published his articles before being murdered.⁷² Moroccan authorities are suspected to be behind digital surveillance operations against leading French journalists and government officials.⁷³

Digital transnational repression as a sovereignty violation

Building on our outline of the conceptual scope of state sovereignty in cyberspace and the empirical reality of DTR, we present three arguments grounded in international law on why these practices can be considered as violating the sovereignty of the countries in which the targeted individuals reside. Next to these normative claims, we outline one political argument that concerns the immediate self-interest of host states affected by DTR.

First argument: DTR is extraterritorial enforcement jurisdiction

Per definition, DTR constitutes governmental action on another state's territory. While states generally benefit from significant latitude regarding intelligence operations abroad, extraterritorial enforcement jurisdiction is tightly restricted under international law: 'The exercise of enforcement jurisdiction is an exercise of State sovereignty, and the rule that governs it is simple. No State may exercise its enforcement jurisdiction in the territory of another State without that State's permission.'⁷⁴

Although a significant overlap between DTR and intelligence activities cannot be denied, DTR appears to be closer to enforcement as it is not motivated by issues of interstate competition, but rather by the perpetrating state's domestic security interests. The prohibition of extraterritorial enforcement jurisdiction is non-controversial regarding non-digital modes of enforcement as it 'violates the fundamental principle of territorial sovereignty that restricts the reach of the police forces of one sovereign into the territorial jurisdiction of another'.⁷⁵ For instance, even in the case of the morally justifiable abduction of former Nazi official Adolf Eichmann by Israeli security officers from Argentina, it was concluded that the operation violated Argentine sovereignty.⁷⁶

While DTR has not been discussed as extraterritorial enforcement yet, the 2014 case *Kidane v. Federal Democratic Republic of Ethiopia*, dealing with an act of DTR in the United States, was dismissed on the grounds of sovereign immunity. In the trial, an Ethiopian dissident with US citizenship living in Maryland sued the government of Ethiopia for infecting his computer with spyware produced by the German-British FinFisher company. The plaintiff made the case that the Foreign Sovereign Immunities Act (FSIA) did not apply because the Ethiopian government had committed a tort on US territory, which is one of the Act's exceptions to immunity. However, the Court argued that the Ethiopian government had planned, prepared, and executed

⁷¹See the Pegasus Project's article collection, available at: {<https://forbiddenstories.org/pegasus-project-articles/>}.

⁷²Stephanie Kirchgaessner, 'Jeff Bezos hack: Amazon boss's phone "hacked by Saudi crown prince"', *The Guardian* (22 January 2020), available at: {<https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince>}.

⁷³Angelique Chrisafis et al., 'Emmanuel Macron identified in leaked Pegasus Project data', *The Guardian* (20 July 2021), available at: {<https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data>}.

⁷⁴Vaughan Lowe, *International Law* (Oxford, UK: Oxford University Press, 2007), p. 184.

⁷⁵Jack I. Garvey, 'Repression of the political emigre: The underground to international law: A proposal for remedy', *The Yale Law Journal*, 90:1 (1980), pp. 78–120 (p. 284).

⁷⁶See Attorney-General of Israel v. *Eichman*, 36 I.L.R. 5 (District Court of Jerusalem, Israel, 1968).

the hacking of the computer from abroad: ‘all of the acts by Ethiopia or its agents that allegedly precipitated the tort occurred outside the United States’.⁷⁷ Therefore, the exception to immunity was considered not applicable, highlighting the tension between a successful persecution of DTR and territorial jurisdiction.⁷⁸ A similar argument might be brought forward to refute our claim that DTR constitutes extraterritorial enforcement jurisdiction. However, digital modes of enforcement can be compared to physical enforcement and should be treated equally. In criminal law it is acknowledged that obtaining e-evidence from servers abroad constitutes a physical intrusion in a different jurisdiction:

Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location.⁷⁹

Such intrusions usually require a Mutual Legal Assistance Treaty (MLAT) or similar bilateral agreements. In the cases of DTR outlined above, such as Saudi Arabia’s hacking into the phones of exiled dissidents, the enforcement aspect is much stronger than in the transborder obtaining of e-evidence as the obtained information is used to further threaten, pressure and punish targets. Therefore, DTR amounts to extraterritorial enforcement jurisdiction prohibited by international law, if committed without the knowledge or agreement of the host state. This is also the case if the information accessed or manipulated in acts of DTR is actually stored in a distributed manner in the cloud so that a link to a specific jurisdiction cannot be established. Similar to the destination approach in the GDPR, the place where the rights violation through DTR occurs should be decisive, rather than the place where the breached or manipulated information is stored.⁸⁰

Second argument: DTR interferes with national self-determination

DTR can be regarded as an illegal interference with a state’s *domaine réservé*, ‘the areas of State activity that are internal or domestic affairs of a State and are therefore within its domestic jurisdiction or competence’.⁸¹ Self-determination is usually understood as regarding the constitution, that is, the founding of a state. However, as Jens David Ohlin argues, this emphasis is owed to an outdated state-centred understanding that ignores the continuous constitutive role of deliberative processes in society.⁸² Especially in democracies, self-determination through deliberation is a permanent and open-ended process. Even in authoritarian societies, such deliberative practices can play an important role in stabilising and legitimising sovereignty.⁸³

Political emigrants often participate actively in host state processes of public deliberation, seeking to influence foreign policymaking with regard to their home country.⁸⁴ As outlined above, DTR can have ‘chilling effects’ on diaspora activists, muting or distorting their voices. By intimidating and silencing exiled dissidents who often possess detailed knowledge on political developments in their home countries, therefore, practices of DTR indirectly interfere in the

⁷⁷*Doe v. Fed. Democratic Republic of Eth.*, 189 F. Supp. 3d 6, 21 (D.D.C. 2016).

⁷⁸*Doe v. Federal Democratic Republic of Ethiopia*, *Harvard Law Review*, 131:1179, available at: {<https://harvardlawreview.org/2018/02/doe-v-federal-democratic-republic-of-ethiopia/>}; Ryan Hayward, ‘Misinterpreting the “Entire Tort” Requirement of the FISA’s Noncommercial Tort Exception: A Critique of the D.C. Circuit’s Opinion in *Kidane v. Ethiopia*’, *Social Science Research Network* (2017), available at: {<https://papers.ssrn.com/abstract=2966775>}.

⁷⁹In reference to Warrant to Search Target Computer at Premises Unknown. 958 F. Supp. 2d 753 (S.D. Tex, 2013).

⁸⁰De Hert and Thumfart, ‘Microsoft Ireland Case’, p. 16.

⁸¹Katja S. Ziegler, ‘Domaine réservé’, Encyclopedia Entry, *Max Planck Encyclopedia of Public International Law*, available at: {<https://opil.ouplaw.com/view/10.1093/law/epil/9780199231690/law-9780199231690-e1398>}.

⁸²Ohlin, ‘Did Russian cyber interference in the 2016 election violate international law?’, p. 1596.

⁸³Baogang He and Mark E. Warren, ‘Authoritarian deliberation: The deliberative turn in Chinese political development’, *Perspectives on Politics*, 9:2 (2011), pp. 269–89.

⁸⁴Dana M. Moss, ‘Voice after exit: Explaining diaspora mobilization for the Arab Spring’, *Social Forces*, 98:4 (2020), pp. 1669–94.

self-determination of the host state. This close link between transnational repression and the national self-determination of the host state was already emphasised by Jack I. Garvey when referring to the activities of the Iranian secret police against Iranians living in the US before the revolution of 1979. He argues that the repression of exiled dissidents was so effective that it obscured the extent of dissatisfaction with the Shah's rule and the likelihood of imminent revolution. Hence, the Iranian state's practices of extraterritorial coercion affected the foreign policies and geopolitical interests of the US government.⁸⁵ In the same way, it can be argued that the surveillance and repression against the Uyghur diaspora impedes European governments to apprehend the full scale and scope of China's extensive efforts to control the Uyghur population in its Xinjiang region. In this case, transnational repression against Uyghurs is clearly part of the attempt to shape political decision-making in Europe and elsewhere.

The prohibition of cyber intervention, as outlined in the *Tallinn Manual*, is not only based on the interference with another state's *domaine réservé*, but also on the coerciveness of this interference: 'The term intervention ... is limited to acts of interference with a sovereign prerogative of another State that have coercive effect.'⁸⁶ Coerciveness is defined as being 'designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State'.⁸⁷ Further, 'the coercive act must have the potential for compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action it would otherwise take)'.⁸⁸ Given these qualifications, DTR against individual exiles does not, per se, amount to coerciveness. However, it could be of coercive nature if undertaken with the intention to alter the host state's political agency, rather than the political agency of the individual dissident. This might require a certain number or prominence of exiles targeted by DTR, in relation to the host state's public sphere. In response to this caveat, however, it can be argued that transnational repression often targets individuals precisely for their outreach and public presence in host societies – consider the example of Jamal Khashoggi, a regular contributor to the *Washington Post* where he published his criticism of the Saudi government. The Chinese campaign against Uyghurs abroad certainly fulfils the criterion of extensive scope. Moreover, surveillance and digital threats, especially when coupled with other more extreme methods of transnational repression, have ripple effects promoting uncertainty and fear throughout entire diaspora communities.

Third Argument: DTR's violation of fundamental and human rights interferes with a state's sovereign to uphold these norms

As argued by human rights approaches, DTR interferes with core fundamental and human rights, such as the right to privacy and free speech.⁸⁹ The popular sovereignty and legitimacy of a state are closely connected with its capacity to guarantee these very rights on its territory so as to safeguard an open public debate and flourishing civil society. In addition, DTR interferes with provisions in the EU Charter of Fundamental Rights and the Universal Declaration of Human Rights that stipulate the right to seek and enjoy political asylum.⁹⁰ Many national legislations include similar articles. Particularly in Western democracies the right to seek asylum is an integrative

⁸⁵Garvey, 'Repression of the political emigre'.

⁸⁶Schmitt (ed.), *Tallinn Manual 2.0*, p. 313.

⁸⁷*Ibid.*, p. 318.

⁸⁸*Ibid.*, p. 319.

⁸⁹Anstis and Barnett, 'Digital transnational repression'.

⁹⁰European Union Agency for Fundamental Rights, 'Article 18: Right to Asylum' (2015), available at: {<https://fra.europa.eu/en/eu-charter/article/18-right-asylum>}; Office of the High Commissioner for Human Rights, 'Universal Declaration of Human Rights at 70: 30 Articles on 30 Articles: Article 14', available at: {<https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23923&LangID=E>}.

part of political culture and identity.⁹¹ The commitment to upholding such fundamental norms is clearly the expression of a state's sovereign decision making. Given the high importance of the right to asylum and other fundamental and human rights, any form of transnational repression against political emigrants, including its digital forms, must be regarded as an interference with the political will and the sources of legitimacy of a state and, hence, a violation of its sovereignty.

Appealing to the self-interest of host states: Political reasons to consider DTR a challenge to sovereignty

While the preceding arguments proceed normatively on the basis of international law, they do not necessarily speak to a state's self-interest. Particularly if facing a powerful authoritarian state committing DTR, less influential host states might prefer to turn a blind eye to norm violations because they do not consider threats to individual migrants as existential for their own pragmatic interests. Therefore, complementing our three principal arguments, we outline an additional rationale focusing primarily on the self-interest of a state. We argue that any challenge by another state to the host state's ability to guarantee the safety and rights of political exiles on its territory also signifies a challenge to its ability to maintain *domestic* sovereignty which refers 'to the organisation of public authority within a state and to the level of effective control exercised by those holding authority.'⁹² We illustrate this point with two empirical examples:

First, surveillance in combination with threats against the home country families of exiles interfered in the first criminal trial on atrocity crimes of Syrian regime officials in Koblenz, Germany. Witnesses withdrew or altered their testimonies after their participation in the hearings became known and family members in Syria were threatened by supporters and agents of the Assad regime. The judge in court expressed resignation as to their limited capability to provide protection for witnesses testifying against a repressive regime still in power.⁹³ Potential witnesses in investigations against former Syrian regime officials in Sweden and the Netherlands were intimidated through similar tactics.⁹⁴ Here, practices of DTR obstructed the host state's judicial processes, which is a central element in the exercise of domestic sovereignty.

In a second example, the Turkish government encouraged the denunciation of government opponents among the Turkish diaspora in Germany, providing even a digital tool to streamline surveillance and reporting. The smartphone application provided by the Turkish Interior Ministry allowed loyal diaspora members to upload photos and contact details of alleged dissidents for reporting them to law enforcement agencies. Those reported risked arrest and interrogation when traveling to Turkey. A briefing of the German parliament saw potential violations of German law by this application, including laws on data protection, against foreign espionage, and political defamation.⁹⁵ With its strategies of diaspora engagement and instrumentalisation, the government of President Erdogan was thus actively inciting its supporters to act against legislation of the host country.

In such cases, practices of DTR go beyond single acts of extraterritorial enforcement jurisdiction, as discussed under our first argument above. Their effects reach further than constituting an obstacle to the capacity of migrants to participate in the host state's public sphere, as outlined in

⁹¹Dana Schmalz, *Refugees, Democracy and the Law: Political Rights at the Margins of the State* (London, UK: Routledge, 2020).

⁹²Krasner, *Sovereignty*, p. 9.

⁹³Hannah El-Hitami, 'Koblenz: Prozess gegen syrische Kriegsverbrecher bringt Familien der Opfer in Gefahr', *Der Spiegel* (28 December 2020), available at: {<https://www.spiegel.de/ausland/koblenz-prozess-gegen-syrische-kriegsverbrecher-bringt-familien-der-opfer-in-gefahr-a-00000000-0002-0001-0000-000174629128>}.

⁹⁴Human Rights Watch, "'These Are the Crimes We Are Fleeing': Justice for Syria in Swedish and German Courts' (3 October 2017), available at: {<https://www.hrw.org/report/2017/10/03/these-are-crimes-we-are-fleeing/justice-syria-swedish-and-german-courts>}.

⁹⁵Deutscher Bundestag, 'Rechtliche Erwägungen Zur App "EGM Mobil"' (23 April 2019), available at: {<https://www.bundestag.de/resource/blob/648946/231017c93eb032926b226765b0073d5e/WD-10-001-19-pdf-data.pdf>}.

argument two. Their implications for the security dimension of sovereignty are also much clearer than in human rights violations affecting the targeted individuals and a host state's legitimacy, which we laid out in our third argument. Rather, these practices undermine *the credibility* of the host state as the holder of effective control over the monopoly on enforcement jurisdiction and the guarantee of fundamental rights. Thereby, they challenge the host state's *authority*. In this regard they resemble other types of foreign interference and hybrid threats, such as election manipulation and disinformation campaigns that seek to undermine trust in public institutions and sow societal division.⁹⁶

The effects of weakened authority are arguably too complex to be measured in empirical terms so that it seems difficult to set a threshold for when they would constitute a sovereignty violation in and of themselves. Yet, from a perspective of the mere self-interest of a state, the potential risks for the social cohesion and security of the host country are obvious. A lack of belief in functioning state institutions and the rule of law might hamper the adherence of affected migrant communities to the social and political norms of the host country and their successful inclusion as equal members of society. This, in turn, could have negative effects on migrants' social and economic participation with implications for the security within diaspora communities and their broader host society. In their research on Eritrean refugees in Canada, Berhane and Tyyskä highlight that intimidation, threats, and surveillance not only 'put the peace and mental stability of some refugees at risk', but also contravene the efforts of the Canadian government to 'create a secure system to protect refugees and ensure that their integration process moves smoothly.' Similar to the example of Turkey mentioned above, some Eritrean refugees are pushed to break Canadian law as embassy staff force them to donate money for military activities in their country of origin. Such coerced allegiance to the state in the origin country that is contrary to the law of the host state will likely lower the host societies' capacity to integrate the targeted migrants. An action plan of the European Commission, for example, underlines the importance of the rule of law and security for integration processes.⁹⁷

Host state responses to DTR

Regimes engaging in DTR benefit from a considerable extent of impunity. The political reactions of host states to even the most flagrant acts of physical transnational repression are often subordinated to economic and geostrategic priorities, as evidenced in the international responses to the murder of Jamal Khashoggi.⁹⁸ Digital threats against diasporas are executed at still lower costs and consequences. As we have shown, practices of DTR not only threaten the personal security of diasporas with ties to authoritarian contexts, but can also violate the sovereignty of their host states. To deter perpetrators from engaging in digital threats against diasporas, some form of legal, political, or operational consequences is crucial for 'making them believe that the costs to them will exceed their expected benefits.'⁹⁹ In response to DTR, host states could take a number of steps to change the opportunity structures and cost-benefit calculations of perpetrating regime actors. The suggestions outlined below are not meant as an exhaustive programme for defending state sovereignty against digitally enabled interventions of authoritarian rulers. Rather we indicate four possible pathways of practices and policies that appear instrumental to curtail DTR.

⁹⁶Eitvydas Bajarūnas, 'Addressing hybrid threats: Priorities for the EU in 2020 and beyond', *European View*, 19:1 (2020), pp. 62–70.

⁹⁷'Action Plan on Integration and Inclusion 2021–2027', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (Brussels, 24 November 2020), available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0758&rid=3>.

⁹⁸Julian E. Barnes and David E. Sanger, 'Saudi crown prince is held responsible for Khashoggi killing in U.S. report', *New York Times* (26 February 2021), available at: <https://www.nytimes.com/2021/02/26/us/politics/jamal-khashoggi-killing-cia-report.html>.

⁹⁹Joseph S. Nye, 'Deterrence and dissuasion in cyberspace', *International Security*, 41:3 (2017), pp. 44–71 (p. 45).

First Pathway: Strengthen the digital resilience of civil society and build distributed cyber deterrence

Strengthening a consistently under-resourced civil society against the powerful state actors relying on DTR corresponds to the logic of distributed deterrence and deterrence by denial outlined above. Enhanced capacities for privacy protection and data security within civil society will not prevent attacks altogether, but make them more difficult. As potential targets of DTR become more resilient, capable of defending against and recovering from attacks, digital threats will be less appealing in the first place. As well as effective interventions educating on digital hygiene and information security, inclusive networks for emergency support and security advice will help diaspora activists to maintain agency under conditions of evolving sociotechnical risks.¹⁰⁰

In addition to these defensive strategies, civil society can also be part of offensive measures aiming to curtail the capabilities of perpetrators. Exposing the tools, methods and enablers of digital repression are important steps to patch vulnerabilities and disable attacks. In September 2021, for instance, researchers at the Citizen Lab discovered that the NSO Group's Pegasus spyware used a vulnerability in Apple products to infect devices without targets even opening a compromised link. Identified on the device of a Saudi activist, this rare 'zero-click' method exposed more than 1.65 billion Apple products to spyware infections. In response, Apple not only issued an emergency software update but also pledged financial support to organisations pursuing cybersecurity research.¹⁰¹

There is still limited awareness on and documentation of cyber operations against civil society, including cases of DTR. To a large extent, knowledge on cyberthreats in policy circles and cybersecurity scholarship is shaped by commercial threat reporting, which 'primarily focuses on cyber-crime, economic espionage and sabotage of critical infrastructure'.¹⁰² Threats against civil society organisations (and even less so individual political exiles) are largely underreported. The increasing scope and detrimental effects of DTR are known only as a result of investigations by a handful of independent researchers, non-governmental organisations, and journalists. More participatory and cross-sectoral mechanisms are needed for documenting and investigating cyber operations against civil society. Private sector resources could provide more accurate intelligence on the tools and techniques of threat actors, facilitating attribution and risk mitigation. In turn, the involvement of civil society in oversight and attribution processes increases their legitimacy, eventually supporting government decisions on policy responses. Public attribution combined with a 'naming and shaming' of perpetrators could work as an effective deterrent and even help reversing some of DTR's 'chilling effects'. As Ronald J. Deibert points out, independent Computer Emergency Response Teams (CERTs) that combine the expertise and resources of different actors could form an important backbone for such approaches to a more distributed and human-centred security for the digital environment.¹⁰³

Second Pathway: Use counterintelligence and law enforcement activities to protect against DTR

Practices of DTR represent a distinct threat within a broader array of foreign interference tactics that aim to influence the political process and undermine the rule of law in target countries. Given the similarity and overlaps with espionage operations, host country law enforcement and counterintelligence agencies play a key role in detecting, constraining, and disrupting the activities of perpetrators and, wherever possible, bring them to accountability. In the United States, the Department of Justice has repeatedly pressed charges against Chinese nationals for

¹⁰⁰Stephanie Hankey and Daniel Ó Clunaigh, 'Rethinking risk and security of human rights defenders in the digital age', *Journal of Human Rights Practice*, 5:3 (2013), pp. 535–47.

¹⁰¹Nicole Perloth, 'Apple issues emergency security updates to close a spyware flaw', *New York Times* (13 September 2021), available at: {<https://www.nytimes.com/2021/09/13/technology/apple-software-update-spyware-nso-group.html>}.

¹⁰²Lennart Maschmeyer, Ronald J. Deibert, and Jon R. Lindsay, 'A tale of two cyber: How threat reporting by cybersecurity firms systematically underrepresents threats to civil society', *Journal of Information Technology & Politics*, 18:1 (2021), pp. 1–20 (p. 3).

¹⁰³Deibert, 'Toward a human-centric approach', p. 421.

acting as foreign agents in operations of transnational repression with methods that included digital surveillance and disrupting online meetings.¹⁰⁴ Two former Twitter employees were charged for spying on behalf of Saudi Arabia by using their access to collect private, identifying information on Twitter users critical of the Saudi government.¹⁰⁵ In Sweden, foreign intelligence activities targeting dissidents in exile, so-called ‘refugee espionage’, represent a distinct crime. The German domestic intelligence agency in its annual public reports documents activities which count as acts of transnational repression from countries like Turkey, China, and Iran.

While these established counterintelligence and law enforcement mechanisms may capture attempts of digital repression, they are not specifically aimed at DTR. Concurrently, dedicated cyber operations could be used to disable infrastructure used for digital threats against diasporas, curtailing perpetrators’ capabilities and increasing their operational costs. To prevent interference in the 2019 midterm elections, for instance, the US Cyber Command blocked Internet access to a ‘troll factory’ in St Petersburg that played a key role in the Russian influence operation against the presidential elections in 2016. Similar offensive measures could target individuals and entities known to engage in DTR. These efforts should also include working with the technology sector. In 2021, for instance, Facebook was able to disrupt Chinese espionage operations against Uyghur activists overseas.¹⁰⁶ Moreover, in order for such measures to serve the purpose of deterrence, they need to be communicated clearly as actions countering practices of DTR.¹⁰⁷

Finally, law enforcement strategies against DTR will have to include measures of outreach to and support of targeted communities. Research for the European Parliament on countering hybrid threats and foreign interference identifies diasporas at risk of ‘being used as proxies’ and recommends targeted programmes for awareness-raising, media literacy, and strengthening cybersecurity skills.¹⁰⁸ Authorities in Germany warn refugees, especially from Syria and Iran, of foreign government pressure and espionage within immigrant communities.¹⁰⁹ For such efforts to be credible and have the desired effects, however, it is important to establish trusted relationships and refrain from framing migrants as a national security risk instead of acknowledging them as persons at risk of cross-border repression.

Third Pathway: Sanctions against perpetrators and enablers of DTR

Sanctions are an important tool to constrain and punish the perpetrators and enablers of DTR, while highlighting their inappropriate behaviour to a wider international audience. Sanctions could target individuals, organisations, and companies involved in or facilitating significant acts of DTR. For instance, the ‘Khashoggi Ban’, introduced in 2021 in the United States, allows imposing visa restrictions on ‘individuals who, acting on behalf of a foreign government, are

¹⁰⁴Federal Bureau of Investigations, ‘What We Investigate: Transnational Repression’, available at: {<https://www.fbi.gov/investigate/counterintelligence/transnational-repression>}.

¹⁰⁵United States Department of Justice, ‘Two Former Twitter Employees and a Saudi National Charged as Acting as Illegal Agents of Saudi Arabia’ (7 November 2019), available at: {<https://www.justice.gov/opa/pr/two-former-twitter-employees-and-saudi-national-charged-acting-illegal-agents-saudi-arabia>}.

¹⁰⁶E. Nakashima, ‘Facebook disrupts China-based hackers it says spied on Uyghur Muslim dissidents and journalists living outside China, including in the U.S.’, *Washington Post* (24 March 2021), available at: {https://www.washingtonpost.com/national-security/china-espionage-uyghurs-facebook/2021/03/24/7f2978d2-8c38-11eb-a6bd-0eb91c03305a_story.html}.

¹⁰⁷Borghard and Loneran, ‘Deterrence by denial in cyberspace’, p. 27.

¹⁰⁸Wigell, Mikkola, and Juntunen, ‘Best Practices in the Whole of Society Approach’, p. 16. See also ‘Foreign Interference in all democratic processes in the European Union’, European Parliament resolution (9 March 2022), available at: {https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.pdf}.

¹⁰⁹Bundesamt für Verfassungsschutz, ‘How Can I Identify Extremists and Members of Foreign Secret Services within my Environment?’, Information Brochure (2018), available at: {<https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/allgemein/2017-08-wie-erkenne-ich-extremistische-und-geheimdienstliche-aktivitaeten.pdf>}.

believed to have been directly engaged in serious, extraterritorial counter-dissident activities'.¹¹⁰ The measure implicitly brings up the principle of territorial sovereignty as perpetrators 'should not be permitted to reach American soil'.¹¹¹ The European Union has yet to introduce a similar instrument. Its global human rights sanctions regime targets individuals and entities involved in serious human rights violations and abuses worldwide, including if these are 'of serious concern as regards the objectives of the EU common foreign and security policy', but has not been applied to acts of transnational repression yet.¹¹²

Other than human rights related restrictions, sanctions in response to malicious cyber activities could be adapted to capture severe cases of DTR. Under its newly established cyber sanction regime, the EU has imposed two rounds of restrictive measures against individuals and legal entities in China, Russia, and North Korea for their engagement in cyberattacks against the Union and its member states.¹¹³ A more comprehensive and consistent application of this instrument, however, seems to have been hampered by a lack of intelligence sharing and coordination among member states.¹¹⁴ To be used in cases of DTR, the thresholds for triggering these restrictions would have to be lowered as the sanction regime currently captures only severe national security threats, such as attacks on critical infrastructure and election interference. Yet, the actors targeting diasporas and those conducting malicious cyber activities against foreign targets often overlap. A more stringent application of these sanctions could also impact the capabilities of DTR perpetrators.

Judicial scrutiny, political pressure, and sanctions will also affect the companies providing the tools and infrastructure for DTR. Authoritarian regimes increasingly rely on commercial spyware furnished by a burgeoning and largely unregulated private industry. In these partnerships, authoritarian states and the private sector are drawn into a dangerous spiral of mutual incentivisation as companies competing for lucrative contracts answer the demands of intrusive regime agents, raise the market's standards by constantly improving the effectiveness of their products, and shun public scrutiny to protect their client relations. As already outlined, in addition to targeting their nationals abroad, authoritarian regimes have not shied away from using the newly purchased capabilities against foreign targets too. The commodification of surveillance technologies thus ultimately threatens the security interests and rule of law in the countries they originated from. Former operatives of the US National Security Agency (NSA), for instance, who were contracted by the United Arab Emirates intelligence agency through a private consultancy, admitted to violating US hacking laws and prohibitions on selling sensitive military technology, after an investigation of the federal police.¹¹⁵ To curtail the capabilities of authoritarian regimes for engaging in DTR, it is important to bring more oversight into the business practices of the surveillance industry and, whenever possible, sanction their servicing of rights-abusing regimes. In June 2021, for instance, judges in France indicted executives of the companies Amesys and Nexa Technologies, which supplied surveillance equipment to the Egyptian and Libyan regimes, for

¹¹⁰United States Department of State, 'Accountability for the Murder of Jamal Khashoggi' (26 February 2021), available at: <https://www.state.gov/accountability-for-the-murder-of-jamal-khashoggi/>.

¹¹¹Nate Schenkkan, Isabel Linzer, and Annie Wilcox Boyajian, 'The "Khashoggi Ban" and What It Does and Doesn't Mean', *Just Security* (3 March 2021), available at: <https://www.justsecurity.org/75117/the-khashoggi-ban-and-what-it-does-and-doesnt-mean/>.

¹¹²Commission Publishes Guidance on Key Provisions of EU Global Human Rights Sanction Regime (18 December 2020), available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2419.

¹¹³Franck Dumortier, Vagelis Papanikolaou, and Paul de Hert, 'EU Sanctions against Cyber-Attacks and Defense Rights: Wanna Cry?', *European Law Blog* (28 September 2020), available at: <https://europeanlawblog.eu/2020/09/28/eu-sanctions-against-cyber-attacks-imposed-and-defense-rights-wanna-cry/>.

¹¹⁴Stefan Soesanto, 'After a Year of Silence, Are EU Cyber Sanctions Dead?', *Lawfare* (26 October 2021), available at: <https://www.lawfareblog.com/after-year-silence-are-eu-cyber-sanctions-dead>.

¹¹⁵Joel Schectman and Christopher Bing, 'Ex-U.S. intel operatives admit hacking American networks for UAE', *Reuters* (15 September 2021), available at: <https://www.reuters.com/world/us/american-hacker-mercenaries-face-us-charges-work-uae-2021-09-14/>.

complicity in torture and enforced disappearances.¹¹⁶ In November 2021, the US government blacklisted the NSO Group, effectively barring the company from receiving American technologies, ‘for engaging in activities that are contrary to the national security or foreign policy interests of the United States’. Such steps send important signals to companies in the surveillance sector and their investors.

Fourth Pathway: International agreements and norm development

Our arguments highlight several normative blind spots that facilitate a proliferation of DTR and hamper its condemnation and curtailment. A first issue that needs tackling is the unclarity of frameworks applying international law to cyberconflict, such as the *Tallinn Manual 2.0*. The *Manual* took a step in the right direction by classifying cyberattacks with violent effects as a use of force. However, as discussed above, it is far from clear on sovereignty interference below the use of force threshold. This problem mostly stems from the imprecise criterion of ‘coerciveness’. In addition, the fact that the attribution of cyberattacks is complex whereas legitimate reprisals require a certain degree of swiftness still constitutes a conundrum that needs to be solved, for instance by defining rigorous standards for attribution and the maximum time lapse of a legitimate reprisal. To address cyberthreats and enforce binding rules at a global level, it has been suggested to create an independent institution for the examination and attribution of cyberattacks, modelled after the International Atomic Energy Agency.¹¹⁷

A second issue are regulations like the Foreign Sovereign Immunities Act and the very similar European Convention on State Immunity that connect state immunity to territoriality. Accordingly, legitimate exemptions from state immunity depend on whether a rights violation by a state occurred on the territory of the state where the trial is held. As discussed with the example of *Kidane v. Federal Democratic Republic of Ethiopia*, such an understanding of territory solely focusing on the physical location of actors no longer fits the reality of transnational digital technologies. Rather, the physical location of the acts that occur should be decisive, for example the intrusion in digital networks or access to stored information on the host state’s territory.

Third, international agreements and controls are needed to contain the proliferation of offensive cyber capabilities and bring more transparency into the largely unregulated private market for surveillance technologies.¹¹⁸ In 2019, the UN Special Rapporteur on freedom of opinion and expression concluded his review on the surveillance industry with a call for an immediate moratorium on the sale, transfer, and use of surveillance technology until human rights-compliant regulatory frameworks were in place.¹¹⁹ Governments need to tightly regulate the export of equipment and knowledge for surveillance to other countries where it is likely to be used for transnational repression. The revised EU export controls, for instance, aim to bring more transparency into the spyware trade. However, civil society organisations criticise that restrictions foreseen in previous drafts were watered down following pressure from private industry and member states with stakes in the exports.¹²⁰

A final fundamental issue that undergirds the reach of state repression across borders is the current weakness of sovereignty. In fact, Western democracies, led by the US government,

¹¹⁶International Federation for Human Rights, ‘Surveillance and Torture in Egypt and Libya: Amesys and Nexa Technologies Executives Indicted’ (22 June 2021), available at: {<https://www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa>}.

¹¹⁷Brad Smith, ‘The Need for a Digital Geneva Convention’, Microsoft On the Issues (14 February 2017), available at: {<https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>}.

¹¹⁸Ben Wagner, ‘Whose politics? Whose rights? Transparency, capture and dual-use export controls’, *Security and Human Rights* (2021), pp. 1–12.

¹¹⁹United Nations Human Rights Council, ‘Surveillance and Torture in Egypt and Libya’.

¹²⁰Lucie Krahlucova, ‘EU Member States Are Watering down Spyware Regulation’, Access Now (15 November 2018), available at: {<https://www.accessnow.org/eu-member-states-are-watering-down-spyware-regulation/>}.

contributed significantly to this normative decline with measures under the ‘global war on terror’ after 11 September 2001. The renditions, targeted killings, and designations of ‘ungoverned spaces’ for anti-terror operations on foreign territory effectively ‘conditioned’ sovereignty and paved the way for a more assertive behaviour of states in extraterritorial space.¹²¹ Law enforcement and security agencies extended their reach across national borders in complex set-ups of international surveillance and security collaboration. Particularly, Russia and China were close partners of the US in the ‘war on terror’.¹²² Initiated in the Global North, these developments ‘have given rise to understandings and technologies of security with global impacts’.¹²³ Authoritarian regimes now make ample use of the label of terrorism to persecute their opponents abroad. They also benefit from a burgeoning private industry for purchasing advanced surveillance capabilities.¹²⁴ The ‘war on terror’ and its consequences exemplify that often ‘[p]ower, more than legal concepts, seems to determine the weight given to sovereignty’.¹²⁵ Although sovereignty is recognised as a fundamental cornerstone of the international order by governments across the political spectrum, there is no higher authority to arbitrate and sanction any interference. In order to strengthen sovereignty’s protective functions under the realities of globalisation and digitalisation, states thus need to restrain themselves, for instance, by imposing strong mechanisms of oversight and public transparency onto their security agencies and surveillance practices.¹²⁶

Conclusion

Digital technologies have given authoritarian governments new tools for political control and coercion beyond borders. With surveillance, malware attacks, online harassment, and other forms of digital transnational repression, these regimes aim to prevent, constrain, and punish dissent among exiles and diaspora populations. DTR is an essentially globalised form of repression: it is committed by state agents and their affiliates against individuals on other territories; perpetrators rely on platforms and infrastructures that do not necessarily overlap with the geographical territory of neither home nor host state; and they use the services of private companies and non-state actors enabling digital threats and augmenting their effectiveness.

Examining these extraterritorial authoritarian practices as sovereignty violations against the state hosting the targeted diasporas, we presented three arguments grounded in international law to show potential interference. First, as governmental action on another state’s territory, acts of DTR represent extraterritorial enforcement jurisdiction which is illegal under international law. Second, DTR interferes in sovereign self-determination by silencing diaspora voices in the public debate of host societies, which risks, among others, distorting deliberations on foreign policy. Third, DTR violates host state sovereignty because it affects the government’s capacity to protect fundamental and human rights on its territory, which goes against the sovereign choice of a state to adhere to such norms. In addition to these normative arguments, we appeal to the self-interest of host states by arguing that DTR can be understood as a violation of domestic sovereignty because it counteracts the authority of host state institutions in the maintenance of

¹²¹Janosch Prinz and Conrad Schetter, ‘Conditioned sovereignty: The creation and legitimation of spaces of violence in counterterrorism operations of the “War on Terror”’, *Alternatives*, 41:3 (2016), pp. 119–36.

¹²²Ben Rhodes, ‘Them and us: How America lets its enemy hijack its foreign policy’, *Foreign Affairs* (September/October 2021), available at: {<https://www.foreignaffairs.com/articles/united-states/2021-08-24/foreign-policy-them-and-us>}.

¹²³Rita Abrahamsen and Michael Williams, ‘Security privatization and global security assemblages’, *The Brown Journal of World Affairs*, 18 (2011), pp. 171–80.

¹²⁴Schenkkan and Linzer, *Out of Sight Not Out of Reach*, p. 7.

¹²⁵Paul de Hert, Cihan Parlar, and Johannes Thumfart, ‘Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland’, *New Journal of European Criminal Law*, 9:3 (September 2018), pp. 326–52 (p. 9).

¹²⁶Ronald J. Deibert, *Reset. Reclaiming the Internet for Civil Society*, (Toronto: House of Anansi Press, 2020), pp. 284–96.

the rule of law and its integrative functions. This can have a range of ripple effects in terms of security and the societal participation of individuals with ties to authoritarian countries.

In practice, many everyday incidents of DTR will likely not cross the line of formal sovereignty violations. Yet the recurrent silencing of critical exiles, the spreading of fear and uncertainty within diaspora communities are stretching limits. Gradually, these practices may amount to the erosion of host state authority and sovereignty we describe. Our arguments thus highlight DTR's subversive effects on the broader host societies – beyond the immediate threat to the personal security of exiles.

To counter DTR, we outlined a strategy of distributed deterrence that will involve public, private, and civil society actors to deny perpetrators the opportunity for attacks and signal that costs outweigh the benefits. This includes, among other measures, investigative research to expose threat actors and their methods, interventions for building the digital resilience of civil society, and counterintelligence activities extending protection to communities at risk. In addition, targeted sanctions and other punitive instruments will constrain the perpetrators and enablers of DTR, stressing their rules-violating actions. Finally, we highlighted several issues of necessary norm development: the rules for cyberconflict that are too state-centred to be applicable to low-intensity attacks on civil society; a global regime for the use and sale of offensive cyber capabilities; and the adaptation of current notions on sovereign immunity to a transnational digital environment.

For host governments to actually act upon this threat and protect targeted migrants under the premise of sovereignty enforcement, a shift in perception and practice is required. Migrants are frequently perceived as a threat to host states' security and therefore subjected to processes of securitisation and exclusion. Instead, host states need to come to an understanding of migrants as referent objects of security and recognise the authoritarian practices that follow them as the actual threat.¹²⁷ Recent policy documents reveal an increasing awareness of the issue among governments who tie the curtailment of transnational repression to strategies of democratic resilience.¹²⁸ In fact, political exiles from authoritarian contexts are often persecuted for upholding their liberal rights and could be considered as strategic allies in the fight against disinformation and authoritarian interference.¹²⁹

In her critical examination of current Western migration regimes and their 'shifting' borders, Ayelet Shachar highlights that the reconfiguration of the boundary-drawing functions of state sovereignty in response to global migration flows needs to be 'matched by a corresponding expansion of responsibilities'.¹³⁰ What she describes as a 'fixation on territorial access as a precondition for securing refuge and protection'¹³¹ frequently results in the exclusion of political refugees who are unable to reach the soil of countries promising asylum. But this fixation also means that those who made it to the territory of liberal host states are falsely assumed to be safe, and often left with a minimum of rights and protection. The rights-extending dimensions of sovereignty, therefore, need to be detached from geographical territory in order to shield individuals from the digitally enhanced transnational reach of authoritarians. In this sense, the 'sovereignty effect' of governance practices that 'seek to reaffirm the foundational elements of belonging to one group as opposed to another'¹³² could be turned into a means for guaranteeing exiles' safety and fundamental rights, free from internal *and* external coercion.

¹²⁷Matt McDonald, 'Whose security? Ethics and the referent', in Jonna Nyman and Anthony Burke (eds), *Ethical Security Studies: A New Research Agenda* (New York, NY: Routledge, 2016), pp. 32–45.

¹²⁸'G7 2022 Resilient Democracies Statement' (27 June 2022), available at: {<https://www.g7germany.de/resource/blob/974430/2057608/61edf594f5ca30fb7b2ae4b79d16f1e6/2022-06-27-g7-resilient-democracies-statement-data.pdf>}.

¹²⁹Andrei Soldatov and Irina Borogan, 'Escape from Moscow', *Foreign Affairs* (13 May 2022), available at: {<https://www.foreignaffairs.com/articles/russian-federation/2022-05-13/escape-moscow>}.

¹³⁰Ayelet Shachar, *The Shifting Border: Legal Cartographies of Migration and Mobility* (Manchester, UK: Manchester University Press, 2020), p. 19.

¹³¹*Ibid.*, p. 75.

¹³²Doty, 'Sovereignty and the nation', p. 142.

Our article highlights some of the manifold ways in which the border-blurring nature of cyberspace challenges established notions of territory, jurisdiction, and sovereignty. Malicious actors exploit gaps in a still emerging normative order for cyberspace, undermining rule of law and security across territorial borders and in transnational space. Cyberspace clearly is a domain for political competition and conflict. However, as research in this field primarily focuses on interstate dynamics and cyberattacks on critical state assets, it has left aside the issue of transnational threats against civil society, and how these might be linked to broader questions of security and sovereignty. This is the gap our article addresses. In doing so, we open up avenues for further research into the security implications of digital transnational repression for host states. Empirical investigations need to further disaggregate the corrosive effects of transnational repression on host societies, such as hampering migrants' successful integration and social inclusion or interfering in public debate and political decision making. On the conceptual and normative level, further reflections are needed about how to exercise and protect state sovereignty in the digital age while safeguarding fundamental rights and human security.

Acknowledgements. The authors are deeply grateful to Paul De Hert (Vrije Universiteit Brussel) for encouraging the formation of this article and commenting on an earlier draft. We also thank the three anonymous reviewers whose constructive comments helped to significantly strengthen the manuscript. The research of Marcus Michaelsen was funded by the European Union's Horizon 2020 Research and Innovation Program under the Marie Skłodowska-Curie Grant Agreement No. 845988 (DIGIACT). During this research, Johannes Thumfart received funding from Gerda Henkel Stiftung's special programme Security, Society, and the State and the European Union Horizon 2020 research programme under MSCA COFUND grant agreement 101034352 with co-funding from the VUB-Industrial Research Fund.

Marcus Michaelsen (PhD) is an independent researcher working on digital authoritarianism and transnational repression. From 2019 until 2022, he was a Marie Skłodowska-Curie Fellow in the Research Group on Law, Science, Technology and Society (LSTS) at Vrije Universiteit Brussel. Previously, he held a Senior Information Controls Fellowship of the Open Technology Fund for a research project on digital transnational repression against exiled Middle Eastern activists. Author's email: email@marcusmichaelsen.eu

Johannes Thumfart (PhD) is a Fellow in the Research Group on Law, Science, Technology and Society (LSTS) at Vrije Universiteit Brussel where he currently works on a project about Internet shutdowns within the Horizon 2020 Marie Skłodowska-Curie COFUND Action IMPACT. From 2020 to 2022, his research on digital sovereignty at LSTS was funded by the Gerda Henkel Stiftung. He is also teaching ethics of international security management at the Berlin School of Economics and Law. Author's email: Johannes.Thumfart@vub.be