British Institute of International and Comparative Law

REGULATING TRANSNATIONAL DISSIDENT CYBER ESPIONAGE

SIENA ANSTIS

University of Oslo, Oslo, Norway and Senior Legal Advisor, The Citizen Lab, The University of Toronto
Email: ssanstis@uio.no

Abstract Remote-access cyber espionage operations against activists, dissidents or human rights defenders abroad are increasingly a feature of digital transnational repression. This arises when State or State-related actors use digital technologies to silence or stifle dissent from human rights defenders, activists and dissidents abroad through the collection of confidential information that is then weaponized against the target or their networks. Examples include the targeting of Ghanem Al-Masarir (a Saudi dissident living in the United Kingdom), Carine Kanimba (a United States–Belgian dual citizen and daughter of Rwandan activist Paul Rusesabagina living in the United States) and Omar Abdulaziz (another Saudi dissident living in Canada) with NSO Group's mercenary spyware. This practice erodes human rights, democracy and the rule of law and has a negative impact on targeted communities, including social isolation, self-censorship, the fragmentation and impairment of transnational political and social advocacy networks, and psychological and social harm. Despite this, international law does little to restrain this practice. Building on momentum around the regulation of mercenary spyware and transnational repression, this article elaborates on how States could consider regulating dissident cyber espionage and streamlines a unified approach among ratifying States addressing issues such as State immunity, burden of proof, export control and international and public–private sector collaboration.

Keywords: human rights, surveillance, espionage, transnational repression, dissidents.

I. INTRODUCTION

Ghanem Al-Masarir is a Saudi human rights activist and satirist.[1] He was granted asylum in the United Kingdom (UK) in 2018.[2] He runs a popular YouTube channel called 'The Ghanem Show' which includes criticism of the Saudi royal family.[3] In November 2019,

[1] *Ghanem Al-Masarir v Kingdom of Saudi Arabia* [2022] EWHC 2199 (QB) para 13.
[2] ibid.
[3] D Akkad, 'Digital Nightmare: The Arab Dissidents Ruined by Phone Hacking' (Middle East Eye, 28 July 2022) <http://www.middleeasteye.net/big-story/digital-nightmare-arab-dissidents-lives-torn-apart-hacking>.

[*ICLQ* vol 73, January 2024 pp 259–274] doi:10.1017/S0020589323000532

Al-Masarir sued the Kingdom of Saudi Arabia alleging that it infected his phone with Pegasus spyware.[4] Pegasus, which is developed and sold by an Israeli company called NSO Group, grants the operator access to the targeted phone including access to the contents of encrypted applications like Signal and WhatsApp and use of the device's microphone and camera.[5] It has been described as a technology posing 'unprecedented risks' by the European Data Protection Supervisor,[6] and its use against human rights defenders (HRDs), journalists and other members of civil society has been widely condemned.[7] In addition to his device being infected with spyware, Al-Masarir was attacked in London by two men, with footage of the assault appearing on social media accounts linked to the Saudi government.[8] He was warned by the police that there was a credible threat against his life.[9] These events had a profound impact on Al-Masarir, affecting his personal life and work and shattering his 'appetite to do anything'.[10]

Al-Masarir is not alone in experiencing such an invasion of privacy. In the past few years, numerous reports of HRDs, activists and dissidents[11] abroad being similarly subjected to surveillance—often linked to their country of origin—have come to the surface, including: the targeting of Bahraini activists in the UK;[12] the surveillance of Omar Abdulaziz, a Saudi dissident in Montreal;[13] and the infection of the phone of Carine Kanimba in the United States (US). Kanimba's father is Paul Rusesabagina, a Rwandan dissident who was forcibly rendered back to Rwanda, prosecuted and jailed.[14] Kanimba, who worked to secure her father's eventual release, was targeted with spyware during a meeting with the Belgian Minister of Foreign Affairs and during calls with the US Presidential Envoy for Hostage Affairs and the US State Department.[15] Kanimba's cousin, a Belgian citizen, was also hacked nearly a dozen times with Pegasus spyware.[16]

[4] *Ghanem Al-Masarir v Kingdom of Saudi Arabia* (n 1).

[5] B Marczak et al, 'The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil' (The Citizen Lab, 1 October 2018) <https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/>.

[6] European Data Protection Supervisor, *EDPS Preliminary Remarks on Modern Spyware* (European Data Protection Supervisor 2022) <https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf>.

[7] See, eg, United 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' (28 May 2019) UN Doc A/HRC/41/35; F Ní Aoláin and AE Jones, 'Spyware Out of the Shadows: The Need for A New International Regulatory Approach' (Just Security, 16 May 2023) <https://www.justsecurity.org/86558/spyware-out-of-the-shadows-the-need-for-a-new-international-regulatory-approach/>.

[8] Akkad (n 3).

[9] ibid.

[10] ibid.

[11] For the sake of brevity, this article sometimes refers to the targets of dissident cyber espionage as 'activists' or 'dissidents', but this should be understood to include all individuals who engage in different forms of lawful activism or dissent (eg journalists, HRDs and other members of civil society).

[12] *Shehabi & Anor v Kingdom of Bahrain* [2023] EWHC 89 (QB).

[13] Marczak et al (n 5).

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

[15] C Kanimba, 'Statement of Carine Kanimba to the US House Permanent Select Committee on Intelligence' (27 July 2022) <https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-KanimbaC-20220727.pdf>.

[16] S Kirchgaessner and D Taylor, 'Nephew of Jailed Hotel Rwanda Dissident Hacked by NSO Spyware' *The Guardian* (London, 18 July 2022) <https://www.theguardian.com/world/2022/jul/18/nephew-of-jailed-hotel-rwanda-dissident-hacked-by-nso-spyware>.

This article examines the practice of the transnational cyber espionage of dissidents (which is referred to in this article as 'transnational dissident cyber espionage' or simply 'dissident cyber espionage' and which has also been described as 'refugee espionage' in other contexts[17]) by States and proposes the contours of an international agreement to unify and streamline host State responses. The growing number of documented cases of such acts of dissident cyber espionage suggests that this practice constitutes a serious risk to fundamental rights, including the rights to freedom of expression and privacy, and poses a complex policy problem for States where targeted individuals reside.[18] Dissident cyber espionage is not an isolated strategy of authoritarian regimes, but falls within the broader framework of digital transnational repression (DTR), which describes the range of tactics used by—usually authoritarian—States to silence dissent abroad through the use of digital technologies.[19] It is part of a broader pattern in States that engage in transnational repression (TR).[20] As Al-Masarir's story illustrates, dissident cyber espionage has serious consequences for targeted individuals and for the success of social and political advocacy—of which those outside the country of origin are an important part[21]—leading to self-censorship, social and professional isolation and psychological harm, among other negative outcomes.[22]

Despite the impact of dissident cyber espionage on human rights, democracy and the rule of law,[23] there remains significant uncertainty regarding the legality of remote-access cyber espionage in international law and, by extension, dissident cyber espionage. Considering this gap and the importance of addressing the practice of dissident cyber espionage, this article argues that States need to respond to this category of espionage at the international level through the development of a common definition and a set of measures intended to deter this practice and facilitate access to a remedy. In addition to being the cornerstone of an effective global response to a transnational problem like dissident cyber espionage, international agreements—even in the absence of perfect compliance by ratifying States—can have a powerful

[17] Unrepresented Nations & Peoples Organization, 'The Recognition and Criminalization of "Refugee Espionage" in Europe' (Unrepresented Nations & Peoples Organization, March 2022) <https://unpo.org/downloads/2748.pdf>. The focus on refugees as a target is a misnomer as the practice affects not just individuals who are accepted as refugees in their host States, but also political and social activists, dissidents, HRDs and others who seek to challenge authoritarian regimes.

[18] M Michaelsen, 'The Digital Transnational Repression Toolkit, and Its Silencing Effects' (Freedom House, 2020) <https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects>.

[19] N Schenkkan and I Linzer, *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression* (Freedom House 2021) <https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf>.

[20] TR is broadly understood by social scientists as the practice, by States, of targeting individuals located abroad (in particular, activists, HRDs, journalists, members of the political opposition, or other individuals who challenge the power of a regime) in order to silence, stifle or stop dissent. See, eg, DM Moss, *The Arab Spring Abroad* (CUP 2021) 35.

[21] ibid.

[22] N Al-Jizawi et al, 'Psychological and Emotional War: Digital Transnational Repression in Canada' (The Citizen Lab, 1 March 2022) <https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/>.

[23] RJ Deibert, 'The Autocrat in Your iPhone' (Foreign Affairs, 12 December 2022) <https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert>.

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

expressive function sending the message that an activity is broadly condemned and leading States to modify their behaviour.[24]

Further, this article builds on the work of scholars who have argued that international law is not agnostic to the practice of espionage and that there is momentum for developing international rules that address different categories of espionage.[25] The focus on dissident cyber espionage is an opening for States to craft international norms addressing remote-access cyber espionage without impinging on State-on-State political espionage, which has been defended by States and scholars alike. There are also several factors that suggest that this is a propitious time to engage in the development of new rules around dissident cyber espionage. The Snowden documents ignited a discussion around the boundaries of permissible cyber espionage activities with growing concern over States' widespread intrusions into privacy. The national security risks posed by the proliferation of cyber technologies such as Pegasus and other forms of mercenary spyware and the obligations of host States under international human rights law (IHRL) to protect individuals within their borders[26] offer additional reasons for international coordination and regulation around this form of cyber espionage.[27]

To unpack the practice of dissident cyber espionage and its relationship with both international law and cyber espionage more generally, this article proceeds as follows: Section II defines dissident cyber espionage and compares it to other categories of espionage, such as political and economic or industrial espionage. It situates it within the broader field of TR and the spread of domestic authoritarian practices in transnational spaces. Section III reviews the muddy waters of international law as it relates to espionage and cyber espionage, concluding—as others have—that there remain normative gaps in whether remote-access cyber espionage, or by extension dissident cyber espionage, is legal under international law. Section IV concludes, arguing that the proliferation of surveillance technologies and the impact of dissident cyber espionage on human rights, democracy and the rule of law create a growing need and opportunity to develop specific rules that address this category of cyber espionage.

II. DEFINITIONS AND CONTEXT SETTING

A. Defining Transnational Dissident Cyber Espionage

There is no definition of transnational dissident cyber espionage in international law. Building from definitions of refugee espionage, this article understands dissident

[24] A Geisinger and MA Stein, 'A Theory of Expressive International Law' (2007) 60 VandLRev 77, 78. However, *contra*, see OA Hathaway, 'Do Human Rights Treaties Make a Difference?' (2002) 111 YaleLJ 1935.

[25] eg, see W Banks, 'Cyber Espionage, Surveillance, and International Law: Finding Common Ground' (Keynote address delivered to the Texas A&M Law Review Symposium, Forth Worth, October 2014) <https://papers.ssrn.com/abstract=2558155>; R Buchan, *Cyber Espionage and International Law* (1st edn, Hart Publishing 2018); A Lubin, 'The Liberty to Spy' (2020) 61 HarvIntlLJ 185.

[26] S Anstis and S Barnett, 'Digital Transnational Repression and Host States' Obligation to Protect Against Human Rights Abuses' (2022) 14(2) JHumRtsPrac 698.

[27] I Dodds, 'US Officials in Uganda Had Their Phones Hacked with Israeli Spyware, Reports Say' *The Independent* (London, 5 December 2021) <https://www.independent.co.uk/news/world/americas/uganda-pegasus-us-embassy-hack-b1970278.html>.

cyber espionage to arise where (1) States, (2) engage in the remote collection of confidential information, (3) targeting activists and dissidents living in exile or the diaspora, (4) with the aim of trying to undermine, neutralize, eliminate or stifle political or social opposition, (5) while using cyber capabilities and (6) (setting aside issues of extraterritoriality) in violation of IHRL.[28]

Dissident cyber espionage is distinguishable from other categories of espionage by its purpose and its targets. In terms of purpose, a State's intent in political cyber espionage is to understand better the capabilities of and threats posed by other States. This has been justified on the basis of international peace and stability.[29] In economic espionage the State's intent is to capture trade secrets that can be leveraged by the recipient State's business sector.[30] In contrast, the intent behind dissident cyber espionage is to silence or neutralize any perceived threat to the regime through the weaponization of confidential information. This cannot be squared with peace and stability in an international order underpinned by principles aimed at protecting human rights.[31] As regards targets, in political espionage, the target is another State; in industrial cyber espionage, the targets are corporate actors with the intent to obtain commercial or business-related information. In dissident cyber espionage, confidential information is sought that can be leveraged against a human rights defender, activist or dissident, in order to silence them or others involved in activities that challenge the regime.

While dissident cyber espionage can be distinguished from political and industrial espionage in both its purpose and targets, it does rely on a shared method—cyber espionage. The *Tallinn Manual 2.0* defines cyber espionage as 'any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather, or attempt to gather, information'.[32] Cyber espionage 'involves, but is not limited to, the use of cyber capabilities to surveil, monitor, capture, or exfiltrate electronically transmitted or stored communications, data, or other information'.[33] Dissident cyber espionage, like much of contemporary cyber espionage, is usually accomplished through remote access, which refers to 'operations that are "launched at some distance from the adversary computer or network of interest"'.[34] Such operations are of 'virtually unlimited reach', posing a broad risk to human infrastructure while being 'extraordinarily difficult to defend against'.[35]

This article, which is focused exclusively on dissident cyber espionage that is carried out by or attributable to States, proceeds on the assumption that the term espionage is broad enough to cover not only State-on-State activity, but also State-on-company or State-on-individual activity.[36] The targeting of non-State actors is increasingly part of the espionage nomenclature.[37] Domestic criminal law similarly suggests that some States already view the targeting of individuals in order to extract information not related to the host State's intelligence or military capabilities for the benefit of a

[28] Unrepresented Nations & Peoples Organization (n 17).
[29] Buchan (n 25) 28–41.
[30] ibid 42.
[31] ibid 35.
[32] MN Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) 168.
[33] ibid.
[34] Buchan (n 25) 18.
[35] DA Wallace, AH McCarthy and M Visger, 'Peeling Back the Onion of Cyber Espionage after *Tallinn 2.0*' (2019) 78 MdLRev 205, 215, 216.
[36] For example, one might argue that situations where States are targeting non-State actors should be referred to as surveillance or information collection not espionage. However, this article argues that espionage is broadly understood to include State activity not only against other States, but also non-State actors. See, eg, Buchan (n 25) 21–4.
[37] ibid 22.

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

foreign State as a form of espionage. For example, Sweden has criminalized 'refugee espionage' ('*flyktingspionage*').[38]

B. Placing Transnational Dissident Cyber Espionage in Context: (Digital) Transnational Repression

Transnational dissident cyber espionage takes place in the broader context of the expanding practice of TR, which arises where States target nationals outside their territory in order to intimidate or coerce them with the purpose of silencing or stifling dissent or otherwise advancing State interests.[39] The term TR originates in social sciences literature and captures the methods that States use to silence dissent abroad, including extrajudicial and extraterritorial assassinations, in-person harassment, physical assaults, renditions, unlawful deportations, physical surveillance, passport cancellations or control over other government-issued documents, among others.[40] TR is not formally defined under international law. However, the rapidity with which the term is being mainstreamed into scholarship[41] and broader policy discourse[42]—and into domestic legislation[43]—suggests an appetite for terminology highlighting specific harms associated with targeting dissidents abroad.

Digital methods of TR are increasingly prevalent. This maps with cyber threats becoming 'more sophisticated and multifaceted'[44] and the growing importance of exiled digital transnational advocacy networks in challenging authoritarian regimes' domestic policies and practices.[45] DTR describes the use of digital technologies by States to achieve the aims of TR—in other words, to silence or prevent dissent originating abroad. It includes a broad range of tools, such as State monitoring and surveillance of digital communications and social media accounts, the use of online harassment and smear campaigns, or even distributed-denial-of-service attacks. Researchers have noted that instances of DTR are 'vastly more common' than physical ones and represent a cornerstone of campaigns of TR.[46]

Transnational dissident cyber espionage does not encompass all acts of DTR, but specifically captures situations where States engage in the remote, non-consensual, collection of confidential information using cyber capabilities such as mercenary spyware (or intrusion software). This can be distinguished from government surveillance of public social media posts or 'electronic armies' engaging in

[38] Freedom House, 'Sweden: Transnational Repression Host Country Case Study' (Freedom House, 2022) <https://freedomhouse.org/report/transnational-repression/sweden>.

[39] Schenkkan and Linzer (n 19); Y Gorokhovskaia and I Linzer, *Defending Democracy in Exile: Policy Responses to Transnational Repression* (Freedom House 2022) <https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf>.

[40] Schenkkan and Linzer (n 19); Moss (n 20) 35.

[41] See, eg, DM Moss, 'Transnational Repression, Diaspora Mobilization, and the Case of the Arab Spring' (2016) 63 SocProb 480; A Dukalskis et al, 'Transnational Repression: Data Advances, Comparisons, and Challenges' (2022) 4 PolResEx 2104651; M Michaelsen and J Thumfart, 'Drawing a Line: Digital Transnational Repression against Political Exiles and Host State Sovereignty' (2023) 8(2) EurJIntlSec 151.

[42] See, eg, Federal Bureau of Investigation, 'Transnational Repression' (Federal Bureau of Investigation, 2022) <https://www.fbi.gov/investigate/counterintelligence/transnational-repression>.

[43] A Schiff, 'A Bill to Criminalize Transnational Repression, and for Other Purposes' (Schiff, 14 November 2022) <https://schiff.house.gov/imo/media/doc/transnational_repression_bill.pdf>.

[44] Buchan (n 25) 2. [45] Moss (n 20). [46] Gorokhovskaia and Linzer (n 39).

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

coordinated campaigns of online harassment and intimidation. It also excludes acts which affect the 'availability or integrity of data or the networks and systems upon which that data resides'.[47] Further, while mercenary spyware is increasingly associated with transnational dissident cyber espionage, this is only one mechanism by which States may engage in remote-access collection of confidential information from dissidents. Other, cheaper technologies exist such as the use of spear-phishing to gain access to email or social media accounts.[48]

Studies around DTR show that dissident cyber espionage, like other forms of DTR, leads to self-censorship, social isolation, stress and burnout. It allows the State to intervene in activists' personal and professional lives, despite a physical distance.[49] Such digital threats and attacks may happen alongside physical threats;[50] for example, confidential information collected by States can be used to track the location of a dissident abroad to carry out their assassination or rendition.[51] Transnational dissident cyber espionage is characterized by a high level of intrusiveness. The remote and covert collection of confidential information from the target may be undertaken through cyber capabilities that provide total access to the target's electronic devices or accounts. On a systemic level, in addition to human rights violations, dissident cyber espionage contributes to the erosion of democracy and the rule of law through the impairment of transnational advocacy work.

C. *Ambiguity Around International Law and the Regulation of Transnational Dissident Cyber Espionage*

Scholarship on cross-border espionage (including cyber espionage) under international law has generally been divided into three categories: espionage is legal, espionage is illegal, or espionage is neither legal nor illegal under international law.[52] Proponents of the view that espionage is legal argue that there is no general prohibitive rule against espionage under international law[53] and further that States have not concluded treaties that regulate or render illegal the practice of espionage.[54] This argument—which has been characterized as a 'majority' view[55]—hinges on the *Lotus* principle, namely that, in the absence of a prohibitive rule under international law, a State is free to act.[56] Supporters of the view that espionage is illegal argue that it is a clear breach of

[47] Buchan (n 25) 18.

[48] Spear-phishing is a targeted form of phishing where attackers tailor deceptive messages to a specific individual or organization, aiming to obtain sensitive information or access. Schmitt (n 32) 169; Michaelsen (n 18).

[49] Michaelsen ibid.

[50] Al-Jizawi et al (n 22); DM Moss, 'The Ties That Bind: Internet Communication Technologies, Networked Authoritarianism, and "Voice" in the Syrian Diaspora' (2018) 15 Globalizations 265.

[51] DD Kirkpatrick, 'Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says' *The New York Times* (New York, 3 December 2018) <https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html>.

[52] AJ Radsan, 'The Unresolved Equation of Espionage and International Law Symposium: State Intelligence Gathering and International Law' (2006) 28 MichJIntlL 595, 603.

[53] D Pun, 'Rethinking Espionage in the Modern Era' (2017) 18 ChiJIntlL 353, 361–2.

[54] PCR Terry, '"The Riddle of the Sands" – Peacetime Espionage and Public International Law' (2020) 51 GeoJIntlL 377, 381; Radsan (n 52) 603–4.

[55] F Dubuisson and A Verdebout, *Espionage in International Law* (OUP 2018).

[56] Buchan (n 25) 5; Pun (n 53) 362; Terry (n 54) 381.

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

territorial sovereignty and thus illegal under international law. Proponents of the view that espionage is neither legal nor illegal take the view that espionage exists in a grey zone where it is neither explicitly forbidden, nor clearly authorized by States and thus operates 'outside the boundaries of international law'.[57] More recent analysis argues that there is no specific rule of international law that renders espionage lawful or unlawful but that one must refer to general principles of international law to identify the relevant norms, and specific acts of espionage may violate them.[58]

Assuming that the last view is the 'most' correct, there remain significant gaps in the regulation of cross-border *cyber* espionage—as a method of espionage—under international law. The literature reveals continuing uncertainty regarding when and how remote-access cyber espionage that involves the exfiltration of confidential data leads to violations of international law.[59] While the International Group of Experts consulted in the *Tallinn Manual 2.0* agreed that the principles of sovereignty and non-intervention apply in cyberspace and that some situations lead to clear violations of the sovereignty principle, they could not achieve consensus as to whether remote cyber espionage reaching a particular threshold of severity violates international law.[60] For example, in a situation where a State exfiltrates data from another State's military systems, the majority of Experts concluded that such exfiltration does not violate any prohibition under international law regardless of severity.[61] This conclusion suggests that remote-access transnational dissident cyber espionage would not violate the principle of territorial sovereignty. International law scholars have also arrived at different conclusions regarding the application of international law to remote-access cyber espionage operations.[62]

The application of IHRL as a regulatory instrument must briefly be considered. Transnational dissident cyber espionage leads to the impairment of human rights, such as the rights to privacy and freedom of expression, and thus might also be appropriately considered through the lens of IHRL. However, even if the issue of dissident cyber espionage is tackled through IHRL, a normative gap remains. There continues to be debate around the extraterritorial application of IHRL and the responsibility of States for rights-infringing acts outside their territorial boundaries.[63] In the *Tallin Manual 2.0*, the Experts noted these disagreements, concluding that 'no consensus could be reached as to whether State activities conducted through cyberspace can give rise, as a matter of law, to power or effective control over an individual located abroad, thereby triggering the extraterritorial applicability of that State's IHRL obligations'.[64] Further, IHRL does not state how a State should respond to prevent such a practice. This

[57] Dubuisson and Verdebout (n 55); Lubin (n 25) 196; Radsan (n 52) 597, 605.
[58] Lubin (n 25) 197; Schmitt (n 32) 170. [59] Buchan (n 25). [60] Schmitt (n 32) 170.
[61] ibid 171.
[62] R Buchan and I Navarrete, 'Cyber Espionage and International Law' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Elgar Publishing 2021); Terry (n 54) 404; Buchan (n 25) 9; E Watt, *State Sponsored Cyber Surveillance* (Edward Elgar Publishing 2021). The argument has been made that DTR, which includes transnational dissident cyber espionage, gives rise to extraterritorial enforcement jurisdiction which is prohibited under international law and thus violates State sovereignty; see Michaelsen and Thumfart (n 41) 160–161.
[63] M Gibney et al, *The Routledge Handbook on Extraterritorial Human Rights Obligations* (1st edn, Routledge 2021). However, see *Wieder and Guarnieri v UK* App Nos 64371/16 and 64407/16 (European Court of Human Rights 12 September 2023) which suggests that we may see more clarity on this point over time. [64] Schmitt (n 32) 185.

article integrates IHRL into a proposed international regulatory framework addressing transnational dissident cyber espionage. As noted by the Experts, IHRL obliges host States to act to protect the rights of individuals within their territory, even against cross-border or transnational human rights violations, and host States are required 'to take action in relation to third parties that is necessary and reasonable in the circumstances to ensure that individuals are able to enjoy their rights online'.[65] Thus, IHRL also provides an argument that States must consider such a regulatory framework and ensure that domestic law protects against rights violations, including transnational dissident cyber espionage.

III. REGULATING TRANSNATIONAL DISSIDENT CYBER ESPIONAGE: AN INTERNATIONAL TREATY?

The absence of clear rules[66] regarding cyber espionage is an opportunity for States: it provides a legal vacuum in which dissident cyber espionage can take place with few restraints. As Wallace et al observe:

> [i]n the absence of voluntary change in practice, international agreement, or emerging legal custom, states will likely continue to comfortably operate within the uncertain sphere of cyber espionage, conducting intelligence-gathering operations against foreign nations, institutions, and individuals.[67]

This section elaborates on how States could consider regulating transnational dissident cyber espionage at the international level and discusses some of the key issues (although not an exhaustive list) that need to be considered in such an international instrument. This article does not discuss at length the pros and cons of a treaty, but it is acknowledged that there remain significant barriers to States concluding new treaties, particularly around cyber issues. While such barriers exist, this section also serves to further stimulate discussion around spyware, cross-border espionage and possible regulatory responses.

A. Setting the Stage: Growing Momentum Towards Regulating Cyber Espionage and Mercenary Spyware Technology

The regulation of cyber espionage at the international level has now become a plausible notion.[68] While many argue that espionage plays a role in maintaining international peace and security, others point out that States are moving towards the development of norms to limit cyber espionage.[69] States have begun to condemn specific instances of this activity.[70] Others pinpoint the Snowden documents as a turning point in international policy around transnational surveillance.[71] Further, national security arguments for curtailing remote-access cyber espionage practices are growing as more States acquire technology to undertake such operations.[72] The proliferation of offensive cyber capabilities is a topic increasingly in the public eye and one that States

[65] ibid 197. [66] Buchan (n 25) 12. [67] Wallace, McCarthy and Visger (n 35) 235.
[68] Buchan (n 25) 12; Lubin (n 25).
[69] M Libicki, 'The Coming of Cyber Espionage Norms' (9th International Conference on Cyber Conflict, IEEE, 2017) <http://ieeexplore.ieee.org/document/8240325/>. [70] ibid.
[71] A Deeks, 'An International Legal Framework for Surveillance' (2014) 55 VaJIntlL 291, 327; Banks (n 25). [72] Deeks ibid 318.

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

have started to consider more specifically, particularly with respect to the use of spyware.[73]

Further, there has been significant momentum building over the past few years around the regulation of mercenary spyware—one of the key technologies that facilitate remote-access cyber dissident espionage. In March 2023, the US announced the *Presidential Initiative for Democratic Renewal*. One pillar of this call to action is US-led efforts to 'counter[] the misuse of technology and rise of digital authoritarianism'.[74] The announcement referred to a 'comprehensive package of actions meant to combat digital repression' including an Executive Order prohibiting the use of commercial spyware that poses 'risks to national security or has been misused by foreign actors to enable human rights abuses around the world',[75] restrictions on post-service employment with foreign entities of concern that develop commercial spyware and the listing of several spyware companies on the Entity List restricting US exports to those companies.[76] The US has also started transnational coalition-building around spyware regulation through the issuance of a set of *Guiding Principles on Government Use of Surveillance Technologies and a Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware* intended to deepen international cooperation around spyware proliferation, which has been signed by ten other countries.[77] It has also established the EU–US Trade and Technology Council, including a specific working group on the 'misuse of technology threatening security and human rights'.[78] The European Parliament Committee investigating the use and abuse of mercenary spyware in the European Union (EU) also called for stringent regulation in their final report on the issue.[79] More recently, the United Nations Special Rapporteur on Counter-Terrorism and Human Rights called for an international legal response to the issue of spyware proliferation.[80]

There has also been growing policy discussion regarding the best means to address the broader practice of TR. The US is also a leader here. There are two pending bills on TR in

[73] European Parliament, 'Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware' (European Parliament, 2 June 2023) <https://www.europarl.europa.eu/committees/en/pega/home/highlights>.

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

[75] The White House, 'FACT SHEET: President Biden Signs Executive Order to Prohibit U.S. Government Use of Commercial Spyware that Poses Risks to National Security' (The White House, 27 March 2023) <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/>. 'Executive Order on Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security' (The White House, 27 March 2023) <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/>;

[76] The White House FACT SHEET (n 75).

[77] The White House FACT SHEET (n 74).

[78] European Commission, 'EU–US Trade and Technology Council Inaugural Joint Statement' (European Commission, 29 October 2021) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_4951>.

[79] J Rankin, 'EU Urged to Tighten Spyware Safeguards in Wake of Pegasus Revelations' *The Guardian* (London, 9 May 2023) <https://www.theguardian.com/world/2023/may/09/eu-parliament-report-calls-for-tighter-regulation-of-spyware>.

[80] Ní Aoláin and Jones (n 7).

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

the US, one to define and criminalize TR in domestic law and the second to establish several policy initiatives. The Department of Justice has also been active in issuing criminal indictments in situations described as TR.[81]

In short, there are a confluence of factors making this an appropriate time to start a discussion regarding the international regulation of dissident cyber espionage, despite States' prior reluctance to regulate on cyber issues. First, there are growing concerns regarding States' unchecked cyber espionage practices, and dissident cyber espionage is the least defensible practice under existing justifications for not regulating political cyber espionage—it does not further international stability and security. Second, there is a building consensus that one of the key technologies that underpins dissident cyber espionage—mercenary spyware—needs to be tackled through comprehensive domestic, regional and international regulation in order to prevent the further proliferation of this technology and the possibility that States use this technology in order to engage in political espionage. At the core of recent discussions towards regulating mercenary spyware is the realization that this technology is not 'just' used to conduct transnational dissident cyber espionage, but also to engage in political espionage against government targets such as US government officials working in embassies and consulates abroad.[82]

With this background in mind, dissident cyber espionage is an area ripe for international regulation. Further, transnational dissident cyber espionage is sufficiently distinct from other categories of espionage in that it does not raise the risk of regulating State-on-State political espionage, which has been identified as a deterrent to any form of regulation.[83] The following section reviews some of the key elements of a potential international treaty addressing transnational dissident cyber espionage.

B. Key Elements of an International Treaty on the Issue of Dissident Cyber Espionage

1. Aims of the treaty

The aims of such a treaty would be multi-fold. One would be to demonstrate normative consensus around the issue of transnational dissident cyber espionage and establish rules that such activity—despite the murky nature of international law on this issue and States' permissive approach to cross-border political espionage—will be prohibited. A second aim would be to ensure that States which ratify the treaty have adopted or amended domestic laws to ensure that acts of dissident cyber espionage can be addressed through civil and criminal action, as well as other measures that ensure targets with government support and judicial remedies. A third aim would be to facilitate international cooperation around dissident cyber espionage, such as formal information exchanges between ratifying States, the development of human-rights

[81] See, eg, US Department of Justice, 'U.S. Citizen and Four Chinese Intelligence Officers Charged with Spying on Prominent Dissidents, Human Rights Leaders and Pro-Democracy Activists' (US Department of Justice, 18 May 2022) <https://www.justice.gov/opa/pr/us-citizen-and-four-chinese-intelligence-officers-charged-spying-prominent-dissidents-human>.

[82] C Bing, 'At Least 50 US Govt Employees Hit with Spyware, Prompting New Rules' (Reuters, 27 March 2023) <https://www.reuters.com/technology/least-50-us-govt-employees-hit-with-spyware-prompting-new-rules-2023-03-27/>.

[83] Banks argues that States, in starting to regulate espionage, 'could agree to distinguish national security espionage from all other forms, and tolerate only the former'. See Banks (n 25) 9.

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

centred export control norms and to provide a place for an international dialogue on the issue. A final aim of the treaty would be to incentivize the private sector to investigate, disclose and collaborate with States.

2. *Defining dissident cyber espionage*

Present definitions of 'refugee espionage'[84] are a good starting point to build from. As discussed in Section II of this article, transnational dissident cyber espionage can be understood to arise where (1) States, (2) engage in the remote collection of confidential information, (3) targeting activists and dissidents living in exile or the diaspora, (4) with the aim of trying to undermine, neutralize, eliminate or stifle political or social opposition, (5) while using remote-access cyber capabilities and (6) (setting aside the issue of extraterritoriality) in violation of IHRL. Where a State targets activists or dissidents living in exile or in the diaspora in such a manner, the presumption must be that such targeting is illegal under IHRL and is carried out with the intent of acquiring confidential information to be used in a manner that silences dissent.

3. *Some measures to be taken by ratifying States at the national level*

a) Access to legal remedies in court

i. Criminal prosecutions

A key aim of a treaty would be ensuring that ratifying States have adapted domestic law to ensure that targets of dissident cyber espionage can access judicial remedies. One option is to require ratifying States to ensure that their domestic criminal laws describe dissident cyber espionage as a criminal offence. Most States will already have criminalized espionage or the unauthorized interception of electronic communications. However, espionage provisions may be too narrow to capture situations where the espionage at issue is information gathering from non-State actors in the host State (such as foreign nationals in the host State) and transmitting that information to a foreign State. The criminalization of dissident cyber espionage (or refugee espionage more broadly, as in Sweden) sends the message that such activities will not be tolerated. The inclusion of such a crime would not be a particularly novel extension of criminal law.[85] That said, criminal law may be hard to utilize in remote-access cyber operations where the operator is outside the host State and thus outside the enforcement jurisdiction of the court. Thus, access to civil remedies against the perpetrating State remains particularly important.

ii. Civil litigation

One of the significant challenges faced by targets of dissident cyber espionage has been the lack of access to a civil remedy in the courts of their host State. This is illustrated by the Court of Appeals for the District of Columbia Circuit decision in

[84] Unrepresented Nations & Peoples Organization (n 17).
[85] eg, Canada already criminalizes different forms of espionage, such as economic espionage. See *Security of Information Act* 1985 (RSC) section 19(1).

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

Doe v Ethiopia.[86] In that case, the plaintiff, an Ethiopian dissident, alleged that he was tricked into downloading a spyware program that enabled the Ethiopian government to spy on him from abroad.[87] He sought to sue Ethiopia in the US. However, under US law, foreign States are immune from suit unless an exception to the Foreign Sovereign Immunities Act applies. Kidane argued that the non-commercial tort exception applied. However, the court concluded this was not the case, finding that the exception 'abrogates sovereign immunity for a tort occurring *entirely* in the United States' while the plaintiff alleged a 'transnational tort'. The court confirmed the lower court's dismissal for lack of subject matter jurisdiction.[88] Thus, it appears that—at least for now—civil claims of dissident cyber espionage in the US will be unsuccessful.

However, there have been promising developments in the UK, which could be concretized through a treaty and consequent statutory amendments in ratifying States. In 2022, the High Court of England and Wales addressed the interpretation of the State Immunity Act 1978 (SIA) in the context of a case of dissident cyber espionage. In that case, Al-Masarir, a Saudi dissident, sued the Kingdom of Saudi Arabia for personal injury.[89] Saudi Arabia argued that it was immune under the SIA and thus the court should set aside the order for service.[90] Section 1 of the SIA provides that States are immune from the jurisdiction of UK courts in the absence of an exception to immunity listed in the statute. Al-Masarir argued that Saudi Arabia was not immune because of the exception for territorial personal injury in section 5 of the statute.[91] He alleged that psychiatric injury arose after learning that the Saudi government sent him malicious messages, that he was subject to surveillance through spyware installed on his iPhones, and that he suffered injury after he was physically attacked.[92] The court held in the plaintiff's favour, finding that even if the act of spyware installation was a sovereign act, section 5 of the SIA 'operates to remove the immunity' in this case.[93] The court concluded that the plaintiff's claim of personal injury was covered by the exceptions in section 5 even though the acts were not all located within the UK.[94] A year later, the same judge concluded that two Bahraini dissidents could sue the Kingdom of Bahrain for damages for personal injury in the form of psychiatric injury which they alleged to have suffered as a result of 'the infection of their laptop computers with spyware by the Defendant, which enabled it to conduct surreptitious surveillance on them'.[95] The same judge held that there was no requirement under section 5 of the SIA that the infringing State had to be present in the UK or that all of the defendant's acts had to have occurred in the UK. It was sufficient that '*an* act takes place in the UK, which is more than a minimal cause of the injury'.[96]

The US and UK decisions illustrate that there has been debate regarding the application of State immunity in the face of transnational dissident cyber espionage. A treaty addressing this practice could specifically require that ratifying States amend their domestic law to ensure that State immunity will not act as a barrier to these kinds of cases. This is not a novel approach; the US, for example, has enacted such an exception to State immunity in terrorism cases.[97] The treaty could also specifically stipulate that domestic

[86] *Doe v Federal Democratic Republic of Ethiopia* (2017) 189 F. Supp. 3d 6 (Court of Appeals for the DC Circuit) 2. [87] ibid. [88] ibid.
[89] *Ghanem Al-Masarir v Kingdom of Saudi Arabia* (n 1) para 4. [90] ibid.
[91] ibid, para 7. [92] ibid, para 20. [93] ibid, para 116. [94] ibid, para 144.
[95] *Shehabi & Anor v Kingdom of Bahrain* (n 12) para 1. [96] ibid, para 80.
[97] Terrorism Exception to the Jurisdictional Immunity of a Foreign State (28 USC 1605A).

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

law must allow for claims to proceed based on psychiatric injury as a form of personal injury and where there are violations of IHRL. The latter is important to ensure that all targets of dissident cyber espionage are able to make a claim. For example, journalists working on human rights issues and subject to dissident cyber espionage may not be in a position to argue that they have suffered psychiatric injury in the same way as an activist, but they can show that their privacy has been violated contrary to IHRL.

iii. A note on the question of attribution of cyber espionage operations

Much has been written on the challenge of attribution in cyber cases. However, countering this scholarship is a growing body of case law showing that attribution is not a barrier. In *Al-Masarir v the Kingdom of Saudi Arabia*, the High Court of Justice concluded that the plaintiff met his burden, on a balance of probabilities, to demonstrate that the exception under section 5 of the SIA applied.[98] The plaintiff served expert evidence that his iPhones had been hacked with spyware by the defendant.[99] The defendant claimed that this evidence was insufficient to attribute the claim properly, but the court observed that Saudi Arabia failed to serve any 'direct evidence in response to the Defendant's expert evidence'.[100] The court reviewed the expert evidence filed by the plaintiff, concluding that it 'demonstrates to the requisite standard that the Claimant's iPhones were infected with spyware, and that the Defendant and/or those for whom it was vicariously liable, were responsible'.[101] This decision, and the *Shehabi and Anor v the Kingdom of Bahrain* case,[102] show that sufficient technical expertise exists to demonstrate on a balance of probabilities that a device has been hacked by a government.

Further, the fact that any 'smoking gun' evidence is likely to be in the possession of the perpetrating State is not a bar to litigation. This was demonstrated in *Al-Masarir*, where the court noted the relatively thin response from the defendant in the face of the hacking claim. This seems to have weighed in favour of the court's conclusion that the claim had been sufficiently made out as the defendant did not present anything persuasive to the contrary.[103] *Carter v Russia* is also instructive on the issue of burden of proof. The case dealt with an act of TR: the transnational poisoning and killing of Alexander Litvinenko in London by Russian State agents. The European Court of Human Rights concluded that it could shift the burden of proof to the Russian authorities in situations where the government was in possession of the necessary information to corroborate the allegation of the killing being a rogue operation. The court drew an adverse inference from the State's refusal to disclose documents related to its domestic investigation into the killing. Considering the government's 'failure to displace the *prima facie* evidence of State involvement', the court had to conclude that the killing was undertaken by individuals acting as State agents for Russia.[104] In short, in cases where a plaintiff alleges that a foreign State engaged in an act of transnational dissident cyber-espionage, it could be specified in the treaty that

[98] *Ghanem Al-Masarir v Kingdom of Saudi Arabia* (n 1) para 152.
[99] ibid, para 154.
[100] ibid, para 155.
[101] ibid, para 160.
[102] *Shehabi & Anor v Kingdom of Bahrain* (n 12).
[103] *Ghanem Al-Masarir v Kingdom of Saudi Arabia* (n 1) para 161.
[104] *Carter v Russia* App No 20914/07 (European Court of Human Rights 28 February 2022) para 40.

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

ratifying States must, once the plaintiff has met a certain threshold, provide for a reversal of the burden of proof through domestic law placing the onus on the State to offer disproving evidence. Legislative reversals of the burden of proof are not novel.

iv. Training and support

Another aspect of a potential treaty would be a commitment by States to dedicate resources and training to addressing the issue of dissident cyber espionage. This would be a 'due diligence' obligation, such that States who ratify the treaty can report and justify decisions taken and resources allocated based on the means available to them. Including this in a treaty would provide a starting point for a common set of initiatives among host States to mitigate dissident cyber espionage. Training and support may take many forms. One option is for States to agree to task domestic cybersecurity agencies with monitoring for transnational dissident cyber espionage and implementing a 'duty to warn' system that has emerged in the context of threats to life.[105] This could be coordinated and implemented through government bodies that deal with cybersecurity and infrastructure in the host State. The US has announced such an approach through the US Cybersecurity and Infrastructure Security Agency.[106]

4. International cooperation

A key component would be ensuring effective international cooperation around transnational dissident cyber espionage. A treaty could provide a structured forum for States to engage in information and evidence exchange in the context of dissident cyber espionage. While there may currently be *ad hoc* sharing among States, inclusion of the requirement to cooperate internationally on this issue and creation of a forum for such exchanges to happen on a regular basis would be likely to lead to more streamlined and consistent information-sharing. Such exchanges may also result in States receiving useful technical information regarding emerging surveillance technologies that are used not only in dissident cyber espionage, but also in acts of political espionage. Information-sharing mechanisms could also facilitate human-rights centred export control norms and coordinated sanctions enforcement by providing a specific space in which to ensure regular exchange on these topics.

5. Public–private sector collaboration

A final component of this treaty would be developing a framework for public–private collaboration. The ongoing Pegasus spyware scandal shows that States are insufficiently resourced in terms of technical expertise to detect cyber capabilities and that private companies and groups are in possession of relevant information regarding

[105] Police Scotland, 'Threats to Life Warnings: Standard Operating Procedure' (Scotland Police, 25 May 2018) <https://www.scotland.police.uk/spa-media/vgsluhjj/threat-to-life-warnings-sop.pdf>.

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

https://doi.org/10.1017/S0020589323000532 Published online by Cambridge University Press

acts of transnational dissident cyber espionage. Developing a route for collaboration and cooperation between the two would greatly increase the efficacy of efforts to tackle cyber espionage.

IV. CONCLUSION

Transnational dissident cyber espionage is not currently addressed or defined under international law, and is not covered by international regulation or agreement. Yet, it poses a significant threat to human rights, democracy and the rule of law. Addressing this practice sets an important precedent for tackling TR and DTR more broadly. While international law applies to cyber espionage, and thus to dissident cyber espionage, there are normative gaps that allow this practice to continue while States struggle to respond. If recent negotiations around other digital technology-related treaties are any indication, there are significant hurdles to the drafting of such a treaty. However, there is presently a window of opportunity for the drafting of an international treaty that defines dissident cyber espionage and specifically outlines how ratifying States should be required to respond. And—even if States fall short of a binding instrument[107]—this article contributes to the debate by outlining key issues that need to be discussed and addressed in any global framework.

ACKNOWLEDGEMENTS

I am grateful to my colleagues at the University of Oslo's Faculty of Law who reviewed prior drafts of this article and to Dr Ronald J Deibert for his comments.

[107] The existence of intelligence alliances like the Five Eyes alliance is a complicating factor. Members, who should be strong proponents for the regulation of dissident cyber espionage, may still remain reluctant to engage in formal treaty-making addressing dissident cyber espionage if there is any concern that it could encroach on their practices of surveillance and cross-border espionage.