ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Targeting the Weak: Exploring Transnational Digital Repression

Aaron Brantly | Department of Political Science, Virginia Tech, US |
ORCID: 0000-0003-4193-3985

Abstract

Much of the cyber conflict literature is heavily focused on state-on-state cyber conflict. Yet, data is available indicating that the most vulnerable are the non-state actors who comprise civil-society organisations, religious, cultural, or political minorities who seek refuge in diaspora communities. The communities and individuals who seek refuge in third-party nations with more permissive legal environments are increasingly being targeted by the regimes in their origin states via cyber means. These attacks meant to safeguard the 'sovereignty' or will of the attacking (home) nation, undermine the sovereignty and security of the harbouring nation, and the rights of the people residing within it. This analysis examines how cyber conflict extending across borders, but not targeting foreign governments, is an increasingly common and pernicious phenomenon. These attacks are clandestine in nature and meant to undermine domestic adversaries residing abroad. This paper examines why and how states target these populations and the implications of these attacks on host nation sovereignty. The analysis seeks to expand the cyber conflict literature by presenting data and cases on cyber conflicts targeting the weakest members of the global community, those seeking refuge from oppressive regimes.

Keywords

human rights, cybersecurity, sovereignty, transnational repression

Received: 07.01.2025

Accepted: 07.04.2025

Published: 02.05.2025

Cite this article as:
A. Brantly, "Targeting the Weak: Exploring Transnational Digital Repression," ACIG, vol. 4, no. 1, 2025, doi: 10.60097/ ACIG/203788

Corresponding author:
Aaron Brantly,
Department of Political Science, Virginia Tech, US;
E-mail: abrantly@vt.edu
0000-0003-4193-3985

1. Shifting the Focus

Cyberspace is often referred to as a global domain. This global nature that connects and facilitates the creation of ad hoc networks that is both the source of its value and its threat to nation states. Much of the literature on cyber conflict focuses on state-on-state [1–4] or even proxy actors operating on behalf of the state [5, 6]. Yet when the black box of the state is opened, and the level of analysis shifts downward, therein resides a category of actors who are frequently overlooked within discussions of state-on-state cyber conflict. These actors comprise human and democracy rights activists, dissidents, non-national political opposition figures, and others who are often forced to seek refuge outside their home states but are nonetheless subject to external exertions of state power via networked technologies. While the connectivity of cyberspace has enabled new forms of conflict [7, 8] and intelligence [9, 10], a smaller group of scholars has focused on the impact of evolving digitally networked actors who frequently become the targets of states but are not states themselves [11–16]. Broadly, this category of actors constitutes what is best termed as digitally enabled civil society actors residing in third-party states. These actors have long been targeted by the state outside of digital spaces [17, 18]. Yet the rise of connected networked digital technologies has provided foreign states new tools to target individuals deemed to be threats to national security. At the same time, these individuals are frequently unprepared and unable to maintain a level of digital security commensurate with the threats they face.

Understanding the threats that refuge-seeking civil society actors face in third-party nations constitutes a critical and underexamined area of cyber conflict studies. The targeting of these individuals undermines norms of sovereignty, results in violations of human rights, and poses spillover risks that threaten both the national security of the host state and its citizens. This analysis examines the concept of sovereignty in cyberspace and the logic of state actions within the context of transnational digital repression. The paper asks three related research questions: why are states so willing to engage transnational targeting; how do they conduct this targeting; and does the extraterritorial targeting of individuals in cyberspace constitute a violation of established norms of sovereignty? This paper answers these three questions through an examination of the logic of extraterritorial targeting, case examples of targeting, and secondary source data analysis on the use of cyber-enabled means to target nationals residing in foreign jurisdictions.

The paper proceeds in three sections below. The first section examines why nations engage in transnational digital repression against

non-state actors. The second section examines how nations engage in transnational digital repression. This section uses cases and data to demonstrate both how individuals and groups are targeted and reinforces why these groups are targeted. The final section draws the why and how together and builds an argument for understanding transnational digital repression as a violation of the sovereignty of the host nation and discusses the implications of ignoring cyber-attacks against non-state refuge-seeking actors.

2. Why nation states use cyber means to target non-state actors?

At first glance, it might be surprising that states devote any resources towards targeting non-state actors seeking refuge in third-party states. Yet the act of targeting is both not new and not surprising when considering the role and influence of such actors on the stability of the domestic polity within authoritarian and authoritarian-leaning regimes. The targeting of what we now refer to as civil society actors in foreign states has been ongoing for centuries. Refuge-seeking civil society actors in third-party nations play a role in the domestic politics of the state from which they are seeking refuge [19, 20]. They also often play a role in the domestic politics and foreign policy of the state in which they are seeking refuge [21]. The increased targeting of these individuals via digital means is a form of cyber conflict that strikes at the core of liberal democratic principles, and undermines the protections of the rule of law and the sovereignty of a host state.

Bueno de Mesquita famously outlined the logic of authoritarian survival by distinguishing between the winning coalition, the selectorate, and the residents of a state [22]. In his analysis, he defines the winning coalition as those persons essential to the political survival of a regime, and the selectorate as the pool of individuals who can vote or participate in the election of a ruling party or individual. In authoritarian states, this selectorate becomes nominal in nature. Bueno de Mesquita and Smith go on to further refine their analysis by providing five rules a leader (dictator) should utilise to retain power. Among the groups identified are the nominal selectorate, not as a voting block, but rather as a group of individuals capable of replacing dissenters within the winning coalition [23]. The selectorate acts as a group of potentially willing replacements to those in positions of power. Yet, it is Zimmerman who outlines the fourth group, the 'ejectorate', as 'those people with the power to remove through extralegal means such as rallies and coups' the individual(s) in power [24]. For the purposes of this paper, the term

'ejectorate' is extended. It is extended in part because members within this grouping are often not true threats to regime's stability. Rather it is their significance as individual or collective voices that positions them as real or imagined members of this group. Members of the ejectorate need not be political, rather they can be religious, social, cultural, and at times athletic icons who either implicitly or explicitly challenge or are perceived to challenge the home state's winning coalition. For the purposes of this analysis, many of the individuals, or groups targeted extraterritorially, are rightly or wrongly, identified by the targeting state as members of this ejectorate. These individuals alone or in organisational structures are in some way perceived to threaten regime's survival or the stability of the winning coalition or the viability of a nominal or co-opted selectorate.

These fears are not without merit. There is ample evidence on the role and influence of foreign-based members of the ejectorate who engage in civil society or journalism-related activities to challenge actively the legitimacy of the ruling regime from which they seek refuge. Individuals and groups within the diaspora or seeking refuge from a targeting state can and do influence the foreign policy of the host state [21]. Moreover, these groups, as will be demonstrated here, often play a central role in the domestic politics of the targeting state [19, 20, 25]. It is not uncommon for members of the ejectorate to co-opt the resources of the host state with either implicit or explicit support.

The ejectorate class is an inclusive category that comprises politicians, athletes, artists, musicians, intellectuals, journalists, and religious figures. The unifying characteristic of each of these individuals is their ability to inspire or mobilise collective actions that run counter to the stated objectives of the ruling regime. Collective actions do not need to be mobilisations to protest in physical or digital space. Often, those most threatening to a regime are individuals whose actions challenge the social or political order as defined by the state. The Cold War presented numerous examples of individuals whose creativity and openness on issues of social and political importance undermined the narrative of the state and thereby constituted a threat to the established order. Individuals, such as Poet Joseph Brodsky, physicist Andrei Sakharov, writer Alexander Ginzburg, poet Mykola Rudenko, writer Vasyl Stus, and many others, were sentenced to gulags, and many were subsequently exiled. There are numerous post-Soviet examples of exiles, including Queer artist Slava Mogutin, and even chess champion Gary Kasparov. Soviet and Russian exiles are not alone, and the same phenomena

of intellectuals and artists being targeted by the state is plainly visible within Chinese dissident circles as well. The list of famous intellectuals and artists from China is as long as the Russian/Soviet lists and includes the famous artist Ai Weiwei, author and musician Bei Ling, writer Gui Minhai, poet Bei Dao, and many others. Iran too has many artists in exile, including artist Alireza Shojaian, artist Shirin Neshat, and Tereneh Hemami. The point is not to write an exhaustive list, but rather to highlight the diversity of actors who comprise the community of individuals within the ejectorate.

What is the logic of targeting these individuals? The literature is replete with a multitude of answers ranging from econometric calculations of cost-benefit analysis that weighs the cost of punishment against the cost of inaction [26] to historical lessons or experiences with dissidents [27]. Examples abound of multiple types of actors, each requiring home government responses based on both real and imagined sources of risk. States that arose from revolutionary movements born or cultivated abroad in exile are likely to be extremely concerned about similar movements threatening regime stability [28]. Generally, the concern that plagues members of the ejectorate class is their potential risk to the stability of the regime from which they seek protection. The extent to which the home government will expend resources to attack them in the nation of refuge is context-dependent and predicated on the perceived risk a given individual or group of individuals pose to the survivability of the state, the reputational damage an individual or group can cause to a state, or their influence within international discourses that affect the international politics of other states which interact with the home government.

Refuge-seeking actors can and are often used by their host states for self-interested political gains, which can be deleterious to the home government. This often leads to calls for individuals in refuge-granting states to be returned [28]. It is not uncommon for less-than-democratic refuge-providing states to acquiesce to authoritarian state requests for the return of citizens deemed hostile by a home government. One population that has suffered increasingly under such requests are the Uyghurs, who, at the request of the Chinese state, have been forcibly returned by multiple countries, including Turkey [29]. What's more is that while some actors have clearly defined political or cultural significance, most Uyghurs who seek refuge abroad have little-to-no political or cultural influence within China or in their nations of refuge. Yet, their very presence is deemed by the Chinese state to be a potential threat. The targeting and identification of Uyghur populations are

largely facilitated through digital means, including directed digital surveillance and social engineering [29].

Targeting non-impactful, non-ejectorate individuals residing outside their home state is also increasing. This suggests that the cost-benefit ratio of such targeting is shifting. Whereas previously individuals targeted by the state had some relative political, economic, or socio-cultural influence, shifts in technology are enabling home states to exert their power extraterritorially more efficiently through both physical and digital spaces. This expanded targeting is having broad-reaching effects well beyond individuals and is instead focused on entire communities and broad swaths of the diaspora [30]. China's targeting of Uyghurs who have sought refuge as described above serves as both a mechanism to dampen social activism with diaspora communities and as a mechanism of social control for domestic populations who might still be in contact with members of the diaspora.

The question as to why nation states use cyber means to target non-state actors extraterritorially is answered in two parts. First, networked technologies enable members of the ejectorate and extended communities to amplify their voices both internationally and within the home nation. Networked technologies have elevated once obscure voices of dissent in ways that pose a direct challenge to the winning coalition of the home state. This challenge is both real in its ability to enable collective action or undermine political, social, or cultural constraints imposed by the home government. It is also imagined in its scale of impact translatable to actual physical mobilisation. The reality of translating online connectivity into offline repertoires of contention [31, 32] is at best mixed or overblown. At times, these digitally enabled repertoires of contention are filled with hyperbole and need to be rooted in more concrete social and political analysis [33–36]. Frequently, there are direct correlations or implicit causal relationships between ejectorate mobilisation and domestic physical mobilisation [37]. Sometimes the relationship between online mobilisation and physical mobilisation results in increasing physical turnout and broader public knowledge on political or social issues both domestically and globally. This was the case in Ukraine in 2013–2014 during the Revolution of Dignity (also known as Euromaidan). As social media posts in Ukrainian, Russian, and English amplified knowledge of the political situation on the ground, they garnered both international and domestic political support in the form international mediation efforts and physical protestor turnout [37]. At other times, the mobilising

power of online repertoires of contention fails to align with the reality on the ground, as was the case in Egypt and Tunisia [34].

Distinguishing between social mobilisation in domestic and foreign digital spaces is difficult. Authoritarian regimes often view collective action as a threat to their power and stability. The result is that states, fearing collective action, frequently implement domestic controls over the information communications technologies within the domestic digital space to prevent collective action [38, 39]. Yet, these controls are often insufficient to prevent all forms of collective action. Domestic actors and members of the ejectorate are increasingly skilled in the use of circumvention technologies to avoid domestic censorship, surveillance, and network controls using proxies, virtual private networks (VPNs), The Onion Router (TOR), and encrypted messaging applications. The result is the blending of foreign and domestic digital spaces. Because communications can flow in and out of domestic and foreign spaces, the state views actors residing beyond in territorial jurisdictions as an inherent threat to the regime. They can and often do view information communications technologies as mechanisms for collective social action. Differentiating between real and imagined threats is difficult in an increasingly networked world. The result is that states, fearing the impact of the ejectorate on the survivability of the winning coalition and the nominal selectorate, can and often do increase the targeting of individuals and groups within and potential members of and beyond the ejectorate. Where digital controls are incomplete or unable to control completely the domestic digital environment, it becomes increasingly necessary to exert control extraterritorially. By constraining both domestic and foreign digital spaces, regimes attempt to further strengthen domestic controls. In this sense the more fearful a regime is of regime change, the more likely they are to aggressively target members of the ejectorate abroad, even where such targeting may constitute a violation of the sovereignty of the state in which the member of the ejectorate resides.

Targeting often occurs because of the issues identified above pertaining to the linking of domestic and foreign digital spaces. The targeting of individuals in the ejectorate and beyond is enabled by contributing factors, including convenience, and efficiency. States can and have reduced the relative costs of targeting members of the ejectorate and broader communities that might pose or challenge the power structure of the home state through attacks originating in or proceeding through networked technologies [40, 41].

Large surveillance programmes using social engineering, spyware, and other techniques enable a broad and sweeping approach to both identifying and targeting members of both the known ejectorate and individuals beyond that ejectorate who might be deemed a potential threat. Large-scale surveillance programmes combined with data analytics and machine learning can help the regime sift through large volumes of data and prioritise targets. In effect, a state can tailor their approach to repression based on the perceived risk posed by different types of actors and their ability to foster collective action. Generally, mild levels of surveillance and repression have an immense chilling effect on diaspora populations. The result is that for a limited cost, members of diaspora groups can be effectively silenced through efforts to discredit their message, undermine social or cultural connections, or through social pressures exerted on family, friends, or community members who remained within the home country. When these nudges towards regime conformity fail, particularly with more outspoken members of the ejectorate, more robust targeting is often deemed warranted. Such targeting can and often does begin in digital spaces through targeted malware attacks. These attacks are of low cost relative to the use of human surveillance and can help a regime in dismantling networks of contention. Targeted attacks can also provide valuable information, resulting in physical targeting of individuals.

Controlling, minimising, undermining, or eliminating members of the ejectorate and their extended networks or potential networks of supporters extraterritorially remain the same as it did prior to the advent of the Internet. Moreover, the resources of the state in comparison to the resources of individuals within the ejectorate are incommensurate. This resource imbalance between the targeted and the targeting parties makes an eventual breach of members of the ejectorate's digital systems a near certainty. Often members of the ejectorate will seek or be offered assistance from civil society organisations or non-governmental organisations with digital security expertise within the nation of refuge. Organisations such as the National Democratic Institute, Electronic Frontier Foundation (EFF), Guardian Project, and numerous others provide resources and trainings to dissidents and opposition members. Yet the threat is ever-present, and the reality is that even with consistent security efforts, individuals targeted by a state are usually compromised in the long run.

Understanding that members of the ejectorate utilise networked technologies, and that home states similarly use these same technologies to cross purposes, the stage is set for a conflict of interests that results in the undermining of the norms of sovereignty

and human rights. Yet simply recognising this imbalance fails to elucidate how this imbalance comes to fruition. The next section examines the means of exploitation. How states undermine human rights will become increasingly clear as the means of state targeting of ejectorate members residing abroad are analysed.

3. How nation states target non-state actors?

The technical realities of networked environments can be beneficial to both members of the winning coalition and the ejectorate. But the capacity of the winning coalition of the home state can generally be assumed to exceed the capacity of members of the ejectorate. This is not a new phenomenon and has been demonstrated previously in analyses examining the rise of state-based oppression in online environments [42]. There is a fundamental imbalance in capacity arising from both *de jure* and *de facto* reality of networked environments. Despite early prognostications or utopian visions of networks being a great equaliser [43] or of the power of networked technologies to elevate the voices of the oppressed [44, 45], the reality has been quite different [46]. Instead, what has arisen is a world in which the collection of data on individuals has become increasingly ubiquitous [47]. The collection, aggregation, and analysis of data is of benefit to both the firm and the state and has fostered what many in the US intelligence community have referred to as a 'new golden age' of espionage [48]. This new golden age arises out of the ability for the state in collaboration with, or often in opposition to firm involvement, to collect large amounts of data on individuals with minimal effort relative to prior intelligence collection methods [10]. Moreover, the state can not only collect data on individuals or groups but it can limit the reach of the information disseminated by them through extensive social and technical censorship efforts [49].

The capacity of states to leverage large-scale data collection from firms both within and beyond their sovereign boundaries creates efficiencies of scale in surveillance and repression. Although some states or transnational bodies have begun to implement programmes to reduce the individual exposure to data collection and by extension surveillance and exploitation, the effects of these efforts are uncertain [50]. Despite rapid advances in data protection, there is a disconnect between concepts of human rights and privacy in digital spaces and those same rights in physical spaces [51, 52]. The persistent and pervasive intrusion of digital devices into the daily lives of individuals is often obscured and exposes members of the ejectorate and the extended community to a host of technologies [53, 54]. Even within liberal democracies, debates

pertaining to the constraint of the state are extensive [55]. These same constraints are not present in authoritarian regimes, which seek to consistently collect, analyse, and control both their domestic and international information environments [56].

There are a wide range of tools and techniques available to oppressive states who repress members of the ejectorate and extended networks. The most basic framework for digital or digitally enabled extraterritorial repression revolves around three core strategies: social, technical, and diplomatic. These strategies roughly approximate to the Diplomatic Informational Military Economic (DIME) framework used by the US Military but notably exclude military actions that would fall outside of the types of targeting being examined here. Figure 1 provides some examples of each repression strategy, tactic, and severity.

Repression Strategy	Attack Tactic Examples	Description	Severity
Social	Disinformation	The deliberate dissemination through overt and covert means of knowingly false information to manipulate public opinion on a topic, person(s) or group(s).	High
	Misinformation	The deliberate or accidental dissemination through overt and covert means of incorrect or misleading information designed to manipulate public opinion on a topic, person(s), or group(s)	Medium
	Domestic contact harassment	Actions that demean, humiliate, or embarrass family, friends, or acquaintances of individuals residing home country of the being targeted abroad. Actions can include physical harassment in the form of searches of persons and property, removal from positions of employment, restrictions on travel, the conduct of active digital or physical surveillance, and imprisonment or detention without reasonable cause.	High
Technical	Social engineering	The psychological manipulation of individuals to gain private information or access.	High
	Spyware	A subset of malware designed to undermine the security of a device and exfiltrate information.	High
	Big data surveillance	The systematic collection and analysis of all public actions of an individual in digital spaces.	Medium
	Malware	The umbrella term for code that undermines the confidentiality, integrity, or availability of a target's devices or systems.	High
Diplomatic	Ministerial	The use of intergovernmental discussions/actions to force the host state to acquiesce to the targeting state's demands.	High
	Economic	The use of intergovernmental discussion/actions or nongovernmental, commonly business-related issues/interests to force the host state to acquiesce to the targeting state's demands.	High

Figure 1. Repression Strategy Framework.

Figure 1 is not an exhaustive framework. The first two repression strategies have unambiguous digital methods and directly relate to the informational attribute of the DIME framework. This analysis disaggregates the informational component between social and technical to provide greater insights into the specific strategies and tactics being employed by the targeting state. The third strategy identified here pairs the diplomatic and economic attributes of the framework. Whereas the information portion of the framework is disaggregated, the diplomatic and economic are often intricately interwoven and can be subtle tools to undermine the ejectorate. Rarely are targeting states likely to impose sanctions to gain access to members of an ejectorate. Yet their assertion of a combined diplomatic/economic pressure can be extremely impactful and undermine the position of members of an ejectorate residing within certain host states. States seeking to target their ejectorate can leverage a wide range of technical, social, and diplomatic/economic tools.

One of the best-known cases of a state targeting its ejectorate arose with the discovery of a tailored social engineering and malware dissemination campaign directed against the Dalai Lama and extended Tibetan opposition networks and institutions. The investigation first initiated at the Computer Laboratory at Cambridge University [57] and concurrently with the Citizen Lab and The SecDev Group resulted in the publication of a series of reports detailing what eventually became known as the GhostNet campaign [58].[1] Through direct interactions with the Tibetan Government-in-Exile, the private office of the Dalai Lama, and Tibetan non-governmental organisations (NGOs), the Cambridge Computer Laboratory, Citizen Lab and The SecDev Group teams were able to identify the extensive compromise of networks and systems. These systems compromised a targeted piece of malware known as gh0st RAT (Remote Access Trojan). This trojan allowed the perpetrator to gain access to and control infected systems [58]. The teams identified e-mail as the point source of the infection and its subsequent proliferation within the network. By the conclusion of the investigation, thousands of systems were discovered to have been compromised. This compromise highlights the increased efficiency enabled by networked technologies. Where once a human agent or more tailored intelligence collection methods might have been used to gain information on the Dalai Lama and his network, by 2009, social engineering and malware exposed nearly the entire network in a matter of months. By all measures, the Dalai Lama and the Tibetan Government-in-Exile are not the typical weak actors. Yet, they highlight the power of networked technologies to enable

1 There is some contention over where the investigation of the cyberattack on the Office of His Holiness the Dalai Lama (OHHDL) began. This paper aligns with the timeline of technical reports released by both the University of Cambridge Computer Laboratory and the Citizen Lab/The SecDev Group. Both organisations claim to have been approached by the OHHDL. Cambridge claims, the approach was made through the Open Net Initiative Asia (ONI Asia), while Citizen Lab/The SecDev Group claim, they were approached through a representative in Geneva. Both organisations give attribution to the technical findings of the other in their respective technical reports. Both technical reports were released on the same day, 29 March 2009.

the extraterritorial targeting of members of the ejectorate. In total, the teams discovered breaches of systems in more than 103 countries [58]. Moreover, rather than simply leveraging the existing data sources, the Chinese government utilised the networks themselves to deliver tailored code to targeted systems, which subsequently provided immense insights into the targeted network. All the perpetrators of this action needed to do was to wait until the data began to flow back to their own servers. Once control was achieved and data was flowing, analysis could be done domestically within China. This case is a clear and demonstrated example of a type of malware, a RAT, being used to gain a beachhead into the digital systems of an ejectorate group. GhostNet constituted an advanced persistent threat (APT) capable of infecting systems and staying in those systems over a long period of time. This aligns with the logic of state targeting of ejectorates that indicates not simple one and done surveillance practices but rather a long-term effort to control actors both extraterritorially and domestically. The Dalai Lama was and is seen as a threat to Chinese rule over Tibet and its state-imposed selection of a religious leader. The case confirms the expectation that states are more likely to target individuals it sees as a threat to the ruling regime, even if those individuals reside in a third-party state.

GhostNet was not unique and in the years to follow many more members of Chinese, Russian, Iranian, and dozens of other ejectorates would be targeted using both state-developed malware, social engineering programmes, and privately acquired malware. The intervening time between GhostNet and 2022 corresponded with the increasing centrality of mobile phones as devices containing immense repositories of information on their owners. As mobile phones grew in popularity, their ability to facilitate the activities of the ejectorate also increased. Tufekci documented the role of mobile phones in social and political movements in Turkey and elsewhere across the Middle East and found these devices and associated platforms held enormous benefit to members of the ejectorate [59]. Yet, as mobile phones rose to prominence as tools of the ejectorate, states interested in constraining these newly empowered voices took notice. As states took notice, private firms saw financial opportunities.

The NSO Group is one of the most prominent firms seeking to profit from privatised surveillance. The NSO Group, founded in 2010, is a private firm with close ties to the Israeli military. Its most famous software product, Pegasus, evolved into a unique ‘zero click’ exploit that gave clients access to their targets’ mobile devices [60]. Unlike

the previous exploit of Tibetan computer systems, Pegasus gave extensive access to the individual mobile devices of users at a time when those devices carried everything from personal, financial, geolocation, and multiple other types of information [61]. Pegasus gave states an efficient technical attack strategy leveraging a comprehensive form of spyware that could be used against nearly any mobile product. This product was sold primarily to countries that lacked substantial endogenous digital capabilities to conduct extraterritorial digital surveillance. New exposures of hundreds of human rights activists, dissidents, journalists, artists, and actors around the world followed quickly [62].

One of the most notorious uses of this malware was the extraterritorial targeting and subsequent assassination of *Washington Post* journalist Jamal Khashoggi [63]. Khashoggi was an important member of the ejectorate of Saudi Arabia. His brutal assassination by the Saudi government was facilitated in part through digital means. Although it is unknown whether Khashoggi's phone was penetrated with Pegasus, it is known that members of his family were found to have Pegasus on their phones. He was targeted because of his outspoken commentary on Crown Prince Mohammad Bin Salman and the future direction of Saudi Arabia. As a journalist and a target of Saudi Arabia, Khashoggi illustrates one of the main arguments of this article, that the individual or even group members of a potential ejectorate are technically weak, relative to the power of their home state. As in the case of the Dalai Lama, Jamal Khashoggi was seen as threatening to the Saudi regime. He spoke and wrote frequently about regime practices and human rights abuses. The case also demonstrates that digital repression is distinguished from physical repression or murder, and while most of the repression occurred while Khashoggi was in one country, the physical repression occurred in another, where the risks to the state for such actions were perceived to be less consequential.

The Khashoggi case was an early bellwether of the use of advanced spyware against journalists, human rights activists, and even politicians. In 2021, Forbidden Stories and a consortium of journalists released a series of investigative reports into a leaked list of 50,000 numbers targeted by Pegasus [64, 65]. The list included hundreds of journalists and activists who were targeted by their home governments. The attack showed a progression in the ability of states to leverage malware to gain access to information on individuals within their respective ejectorates. Pegasus shows a dramatic leap in technical capacity over previous malware used to surveil developed by the Hacking Team, and Lench IT Solutions Plc. The unique

nature of Pegasus was not in its exfiltration of data so much as in its ability to exploit security measures on devices and enable the installation of the malware [66].

Above were two public incidents of transnational targeting of members of the ejectorate. Yet data from Freedom House and other sources suggests that the phenomenon is more widespread than is appreciated. Freedom House has developed a dataset indicating 854 direct transnational repression incidents between 2014 and 2022 [67]. In a 2020 report, Freedom House found 'digital tools make it easier than ever for authoritarian governments to control, silence, and punish dissent across borders' [68]. Freedom House data suggests that China is the largest perpetrator of targeted transnational repression and constitutes a sizeable 253 of the 854 incidents, while Turkey comes in second [69]. Other studies suggest that high levels of transnational repression through digital means are being undertaken by Iran [70] and other Middle Eastern and North African states [71]. Nearly all states engaging in transnational repression of ejectorates are less-than-democratic and more likely to fear regime change. Below is the data from different sources that helps to illustrate the scale and scope of transnational digital repression. Figures 2A and 2B show the country of origin and host country for individuals seeking refuge based on the data collected by Freedom House.

Figures 2A and 2B highlight the geographic diversity of the issue of transnational repression and the places to which many of those seeking respite from repressive home states move. Interestingly, often individuals repressed by their home state end up in equally or near equally repressive states. Moving from one repressive state to another might reduces direct domestic repression but makes them more susceptible to transnational repression than if these same individuals went to a liberal democracy.

Figure 3 identifies the profile characteristics of individuals seeking refuge in host states. The data is non-exclusive, meaning that an individual can be targeted across multiple dimensions. Yet, the data indicates what has been discussed in above sections, that individuals are targeted because of individual activities or on the basis of personal characteristics that put them in direct opposition to the status quo of their home state. It is these profile characteristics that likely result in the home state perceiving these individuals as a threat. This data helps to reinforce the reality that transnational targeting is extremely broad in scope.

Figure 2. (A) Country of origin from which Individuals are seeking refuge (darker region indicates more individuals seeking refuge) [67]. (B) Host country of individuals seeking refuge (darker region indicates hosting of more individuals) [67].

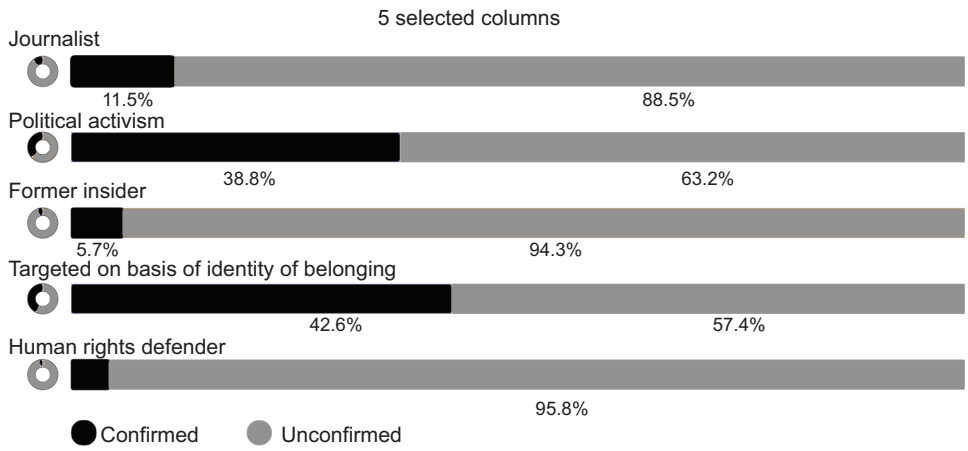

Figure 3. Targeted individual profile data [67].

The literature on transnational repression documents the continuation and adaptation of historical legacies of extraterritorial repression to modern digital contexts and is shifting towards a combination of physical and information control with substantial emphasis being placed on the later [72]. Despite a growing literature on the subject, accurate data collection and analysis remains difficult [73]. The data on transnational repression spans qualitative case analyses and quantitative collections. The most extensive database on transnational digital repression centres on Chinese repression of Uyghur populations and has a collection of 7106 event data points [73]. The Oxus Society for Central Asian Affairs developed the Uyghur Human Rights Project (UHRP) and collected data on various forms of transnational repression and categorised them into three stages [74]. Oxus categorises their data into three distinct stages of repression. Stage 1 constitutes 'warnings and threats to individuals and family members and arrest requests issued bilaterally or through international organisations, such as Interpol'; stage 2 constitutes 'long and short detention, imprisonment and conviction overseas associated with suspected activities at home'; and stage 3 constitutes formal extradition, informal rendition, disappearance, serious attack, and assassination' [11, 74]. Out of 7106 event data points, 5332 were documented in stage 1. This data makes it clear that early-stage transnational digital repression is a function of cost and convenience. Figure 4 illustrates the distribution of repression type across 227 actors or actor groups from 2002 to 2021. Approximately 96% of these documented repression attempts involve some digital component, with 50% including the use of cyberattacks and malware. The data also aligns with the

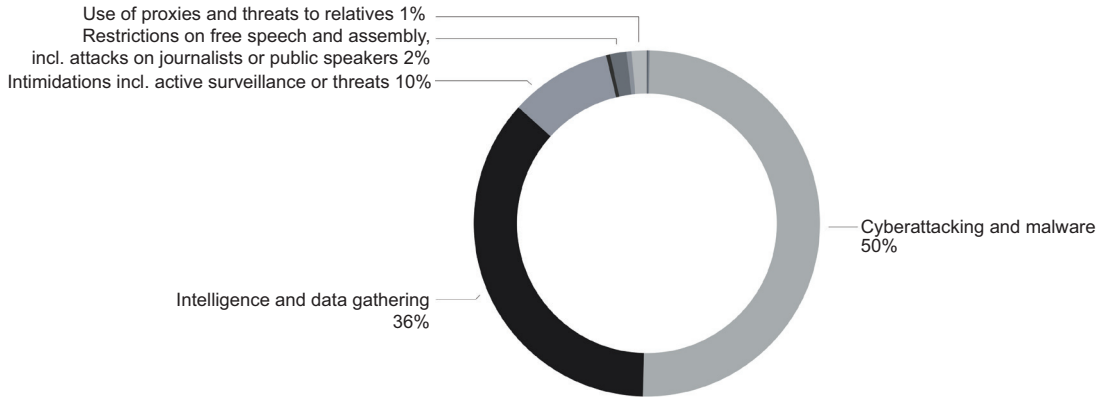

Figure 4. Percentage of stage 1 repression attempts by repression type (out of 5532 documented repression attempts, there are over 227 actors/actor groups).

above-proposed social, technical, and diplomatic/economic repression strategy framework in Figure 1.

Figure 5 illustrates the volume of stage 1 repression attempts by year. According to the data authors, the dataset is incomplete and is only a representative collection of all potential repression attempts. Yet the data aligns with the work on transnational repression documented in other sources, including the work of Cain, who highlighted a substantial rise in police repression of Uyghur populations in China and abroad. The volume of targeting attempts also largely corresponds with collective actions by Uyghur groups, including the Uyghur World Congress.

A macro view of digital transnational repressive activities against ejectorates suggests an increasing mix of big data and targeted campaigns. While the expansion of digitally enabled repressive activities has substantially increased, it has not obviated all physical incidents of repression. The pairing of physical and digitally repressive activities fosters a perfect storm that undermines the human rights of members of the ejectorate and the sovereign rights of the host nations in which they reside. By all measures and across all datasets, the volume and severity of transnational targeting of individuals via digital means is on the rise [75].

The technical sophistication of malware and big data efforts have increased. Evolution in the use-targeted malware has progressed significantly since Italy-based Hacking Team sold basic spyware to states [76]. The targeting of individuals has even included the

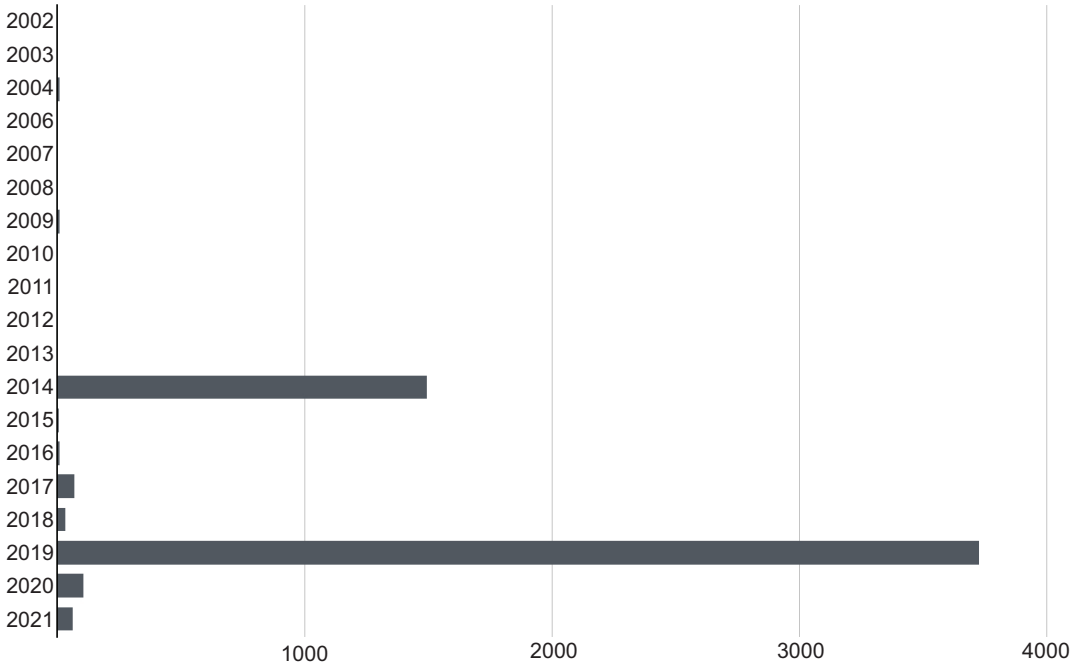

Figure 5. Volume of documented stage 1 repression attempts by year.

manipulation of hardware infrastructures through the use of international mobile subscriber identity (IMSI) catchers that spoof mobile towers in a hack that forces mobile phones to connect to hostile networks in foreign capitals [77]. Such hacks had previously been used to target Ukrainian service members engaged on the front lines of the 2014–2022 conflict in the Donbas of Ukraine [78]. The persistence and complexity with which some states engage in the targeting of actors who might constitute a threat to the ruling regime establishes a concrete dynamics of cyberattacks that is exceeded only by national security espionage attacks and cybercriminal activities. The cases above and the data suggest that states are increasingly turning to digital means when they feel threatened.

In contrast to attacks against state actors, the targeting of individuals within diaspora and dissident communities who are perceived to challenge the social, political, economic, cultural, or even athletic dynamics of the home state are vulnerable in ways that on a case-by-case basis resemble a Doctorow novel [79]. Individuals and groups targeted by states lack the financial and human capital resources to engage in sustained cyber defences against increasingly well-equipped states. The process of cyber defence

for individuals and groups who fall within this potential ejectorate requires constant adaptation. Ejectorate members must maintain constant vigilance, often with minimal financial resources and with the assistance of often underfunded NGOs, such as Amnesty International, Access Now, the Electronic Frontier Foundation, and other similar entities. Each of these entities builds tailored recommendations for those who seek their assistance, yet they too are ill-equipped to combat a motivated and resourced state intent on targeting individuals deemed a threat in foreign host states. Not only are the relative budgets of these defensive organisations insufficient to provide sustained defence, their human capital resources are also constrained. Their best efforts are generally limited to providing trainings and recommendations that minimise risks.

This section focused on attacks that seek to collect data on or penetrate the devices of members of the real or perceived ejectorate. Yet, an entire category of informational attacks has not been addressed, dis-and-misinformation targeting members of the ejectorate abroad. These types of attacks seek to discredit ejectorate members residing within third-party states. The rapidity and scale with which states can counter the narratives and the information generated by individuals deemed a threat to the state have increased in scale and complexity. Advances in artificial intelligence have led to new techniques to create and disseminate fake images, videos, and text [80, 81]. These attacks are constitutive of cyber-enabled information attacks but fall largely outside the scope of this analysis. Their existence is raised here to demonstrate that even within the narrow scope of cyberattacks and surveillance, there remain multiple other vectors through which the home state attempts to undermine and repress individuals and groups it deems to be threats.

This section has demonstrated some of the many ways in which states can and do target ejectorate actors that it deems threats. By combining the logic of *why* states target members of the real or perceived ejectorate with the *how* they target these individuals and groups, the final section discusses the normative and national security implications arising from the targeting of non-state actors via cyber means and surveillance activities. Both prior sections were constrained in scope and limited to those activities that most closely approximated state-on-state cyberattacks but were instead targeted against non-state 'weak' actors. The goal of the final section is to link the levels of analysis – state and substate – to make a robust case for the necessity of considering the ramifications of cyber conflict beyond the commonly examined narratives.

4. The normative and national security implications of transnational targeting of non-state actors via cyber means

Cyberspace complicates notions of sovereignty. Despite well-established and codified international legal precedents outlining both *de jure* and *de facto* attributes of sovereignty, the application and understanding of sovereignty in digital spaces remains contested. Although sovereignty remains contested, the fundamental assumption as indicated by the Tallin Manual 2.0 is that the principle of state sovereignty applies in cyberspace [82]. Yet, unlike state-on-state cyberattacks, which often cross national boundaries through respective domestic Internet service providers, the targeting of non-state actors across boundaries remains complex. This complexity is rooted in both the actor type and the logic with which states justify cyberattacks. It is important to note that a member of an ejectorate engaging via networked devices with individuals within the home country can and often is interpreted as a perpetrator of a cyberattack that violates what has increasingly been termed information sovereignty [83]. The view that the transmission of information and not the degradation, manipulation, or destruction of networks or systems is a violation of sovereignty is not shared between states. Most liberal democracies view freedom of speech as extending beyond the rules and regulations of a single state's right to information sovereignty. Yet most authoritarian states see that a conflict arises out of Internet-based free expression that is incommensurate with the views of liberal democracies [84]. As a result, the free speech practices engaged in by members of the ejectorate and affiliated or extended networks is seen as a violation of sovereignty and a direct threat to regime's security and stability.

Starting with the understanding that there is a fundamental difference of perspective on what constitutes a cyberattack and what does not, places the actions of ejectorate members and extended networks in a legal grey zone. While legally permitted to speak out about issues of concern from their place of refuge, these speech acts are considered attacks by the home government. The Tallin Manual 2.0 further introduces complexity into this discussion in Rule 2 – Internal Sovereignty:

> A state enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations [11, 82].

Due to the transboundary and extraterritorial nature of online activism by members of an ejectorate, diaspora, or network, the

home government can and often does interpret itself as being targeted. To combat this, it engages in activities via networked environments to safeguard its domestic information environment. Whereas these activities extend beyond the territorial jurisdictions of the home state and into the networks and systems of actors behind sovereign borders constitutes a violation of the norms of sovereignty. Just as historically, the extraterritorial physical targeting of individuals was considered a violation of norms, so too is the digital targeting of individuals. The result is a tit-for-tat exchange of information and cyberattacks that leaves both sides feeling violated. Both home state and individual actors root their actions in legal justifications. That these justifications are often at odds with one another should not be surprising. The level of suffering is not proportionate between members of the ejectorate and members of the home state. The overwhelming accumulation of evidence suggests that individuals violating the notion of information sovereignty of their home state are likely to be targeted and exposed to substantial cyber, physical, and informational attacks.

The impact of the violation of norms of sovereignty is unlikely to provoke a more widespread conflict [1]. This is an important point. While much of the early discussion on cyber conflict focused on escalation and the potential for wider cyber conflicts [85–87], the reality remains that targeting members of real or imagined ejectorate communities is unlikely to provoke conflict and often transpires below the public consciousness. The targeting of weak actors is not completely out of sight and out of mind. There is a robust community of NGOs and government organisations that continually strive to raise awareness about issues of state targeting [88].

The effect targeting of individuals across boundaries is not isolated to those being targeted. Rather, evidence suggests that directed targeting against select or even more expansive groups of members of the ejectorate or diaspora communities within refuge-providing states can and does result in a 'chilling effect' [89]. This silencing effect is widespread and affects diverse groups within refuge-providing states, including members of Chinese, Iranian, Russian, Belarusian, Bahraini, Saudi, Palestinian, and other similar communities [90–92]. The explicit targeting via cyber means of individuals constituting real or imagined ejectorates sends a signal to wider socially and culturally affiliated groups that they are not safe from the reach of the home state. This extended reach of the home state can have political, social, cultural, and economic ramifications in the state of refuge, in third-party states, and for family and friends within the home state. Russian and Saudi incidents in recent years have

demonstrated the interconnection between the digital targeting of individuals in refuge-providing states and the physical targeting of the same individuals in both refuge-providing state and third-party states. Few examples of this interconnected targeting are more brutal than that of the case of Jamal Khashoggi examined above.

The reach of states beyond their borders into diaspora and ejectorate communities is consequential within both the refuge-granting state and the home state. Starting with the former, the ability of a foreign power to stifle public debate [93], academic research [94], cultural activities [93], or political involvement [93] undermines the basic tenets of liberal democracies and harms political and social freedoms. In contrast to the experiences arising from state-sponsored cyberattacks against critical infrastructures, financial systems, or entertainment enterprises, the effect of targeting members of the ejectorate and extended communities are pervasive and long-lasting. The lasting effect of these attacks is an aggregate reduction of civil liberties and the shifting of public discourse away from the topics of national and geopolitical importance. Even the topics that are not directly related to the survival or public interest of the targeting state can be subsumed into an 'all or nothing strategy' of control. As a result, foreign exchange students, visiting scholars, scientists, and businesspersons who are not involved in commentary or activities related to the state can and are still subjected to intense state surveillance via digital and non-digital means [95].

When the lens is widened, the impact of targeting foreign-based members of real or imagined ejectorates extends back to the home state and undermines the potential for plural and inclusive societies rooted in civil discourse. The result is the hardening of authoritarianism within the home state. A consequence of transnational digital repression is a further reduction of internal dissent. The pairing of external and internal repression results in the near complete collapse of communities of dissent [96]. As dissent is eliminated, the diversity of intellectual, political, economic, social, and cultural views is constrained. This constraint is important both domestically and in its impact on international relations.

Targeting the 'weak' is increasingly a function of convenience. The relative costs of targeting individuals and groups has decreased as networked technologies and the attack surfaces of individuals through the utilisation of mobile and other devices have increased. *How* individuals are targeted is situated within the broader context of *why* they are targeted. Their targeting is of significance. The pernicious nature of the targeting of the weak is unlikely to raise alarm

bells at the US Cyber Command, but its significance should not be understated. The impact of such targeting on the norms of sovereignty is important, as are its impacts on broader social and political stability within home and host nations.

Emphasis is frequently placed on cyberattacks occurring between states. Fears of 'cyberwar', 'cyber escalation', 'cyber espionage', and attacks against critical infrastructures are important and significant to an evolving debate on cyber conflict. Yet, this paper argues that it is the cyber-enabled targeting of 'weak' actors, those actors who seek refuge from a home government, whose voices of dissent, religious, social, or cultural differences suffer severely and with long-lasting impact. Moreover, this analysis identifies the targeting of the 'weak' as a function of both the logic of state survival and the relative efficiency gains achieved using networked technologies. The targeting of individuals extraterritorially is a violation of the norms of sovereignty as outlined by the Tallin Manual 2.0. This violation of the norms of sovereignty is not new. It has been occurring since prior to the advent of the Internet, yet the scale and scope of violation has increased in volume and breadth. State violations of norms of sovereignty in digital spaces while not directly undermining the physical infrastructure of the state in which individuals are being targeted does undermine the social, cultural, and political infrastructures that are critical to societal resilience, plurality, and inclusion. Regimes that feel threatened are more likely to engage in transnational repression of members of the ejectorate. They are also more likely to privilege domestic security concerns and regime survival over perceived violations of sovereign of harbouring nations.

References

[1] B. Valeriano, B.M. Jensen, R.C. Maness, *Cyber strategy: The evolving character of power and coercion.* Oxford: Oxford University Press, 2018.

[2] A. Brantly, *The decision to attack: Military and intelligence cyber decision-making*. Athens, GA: University of Georgia Press, 2016.

[3] L. Kello, *The virtual weapon and international order*. New Haven, CT: Yale University Press, 2017, doi: 10.2307/j.ctt1trkjd1.

[4] A. Segal, *The hacked world order : How nations fight, trade, maneuver, and manipulate in the digital age*. New York, NY: Public Affairs, 2016.

[5] E.D. Borghard, S.W. Lonergan, "Can states calculate the risks of using cyber proxies?," *Orbis*, vol. 60, pp. 395–416, 2016, doi: 10.1016/j.orbis.2016.05.009.

[6] T. Maurer, *Cyber mercenaries*: *The state, hackers, and power*. Cambridge: Cambridge University Press, 2018.

[7] R.A. Clarke, R.K. Knake, *Cyber war: The next threat to national security and what to do about it*. New York, NY: Harper Collins, 2010.

[8] M.C. Libicki, *Cyberspace in peace and war*. Annapolis, MD: Naval Institute Press, 2016.

[9] J.R. Lindsay, "Cyber conflict vs. cyber command: Hidden dangers in the American military solution to a large-scale intelligence problem," *Intelligence and National Security*, vol. 36, pp. 260–278, 2020, doi: 10.1080/02684527.2020.1840746.

[10] A. Brantly, "Defining the role of intelligence in cyber," in *Understanding the intelligence cycle*, M. Pythian, Ed. London: Routledge, 2013, pp. 77-98.

[11] L. Maschmeyer, R.J. Deibert, J.R. Lindsay, "A tale of two cybers – how threat reporting by cybersecurity firms systematically underrepresents threats to civil society," *Journal of Information Technology & Politics* vol. 18, no. 1, pp. 1–20, 2020, doi: 10.1080/19331681.2020.1776658.

[12] D. Ronald, *Access contested: Security, identity, and resistance in Asian cyberspace information revolution and global politics*. Cambridge, MA: MIT Press, 2012.

[13] R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain, *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press, 2010.

[14] R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain, *Access denied: The practice and policy of global internet filtering*. Cambridge, MA: MIT Press, 2008.

[15] R.J. Deibert, R. Rohozinski, M. Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war," *Security Dialogue*, vol. 43, pp. 3–24, 2012, doi: 10.1177/0967010611431079.

[16] D. Ronald, *Reset: Reclaiming the internet for civil society*. Toronto, ON: Anansi, 2020.

[17] R. Horvath, *The legacy of Soviet dissent: Dissidents, democratisation and radical nationalism in Russia*. London: Routledge, 2005.

[18] H. Harding, "Neither friend nor foe: A China policy for the nineties," *Brookings Review*, vol. 10, p. 6–11, 1992, doi: 10.2307/20080288.

[19] F.B. Adamson, "The growing importance of diaspora politics," *Current History*, vol. 115, no. 784, pp. 291–297, 2016.

[20] J.M. Brinkerhoff, "Diasporas and conflict societies: Conflict entrepreneurs, competing interests or contributors to stability and development?," *Conflict, Security & Development,* vol. 11, pp. 115–143, 2011, doi: 10.1080/14678802.2011.572453.

[21] Y. Shain, "Ethnic diasporas and U.S. foreign policy," *Political Science Quarterly*, vol. 109, p. 811–841, 1994, doi: 10.2307/2152533.

[22] B. Bueno de Mesquita, *The logic of political survival*. Cambridge, MA: MIT Press, 2003, doi: 10.7551/mitpress/4292.001.0001?locatt=mode:legacy.

[23] B. Bueno de Mesquita, A. Smith, *The dictator's handbook: Why bad behavior is almost always good politics*. New York, NY: PublicAffairs, 2011. https://public.ebookcentral.proquest.com/choice/PublicFullRecord.aspx?p=5375849.

[24] W. Zimmerman, *Ruling Russia: Authoritarianism from the revolution to Putin*. Princeton, NJ: Princeton University Press, 2016, doi: 10.1515/9781400880836.

[25] J.M. Brinkerhoff, "Digital diasporas and conflict prevention : The case of Somalinet.com," *Review of International Studies*, vol. 32, no. 10, pp. 25–47, 2014.

[26] P. Chung, "On the behavior of a totalitarian regime toward dissidents: An economic analysis," *Public Choice*, vol. 33, pp. 75–84, 1978, doi: 10.1007/BF00123945.

[27] Y. Shain, "The war of governments against their opposition in exile," *Government and Opposition*, vol. 24, pp. 341–356, 1989, doi: 10.1111/j.1477-7053.1989.tb00727.x.

[28] A. Dowty, *Closed borders: The contemporary assault on freedom of movement*. New Haven, CT: Yale University Press, 1987.

[29] G. Cain, *The perfect police state*. New York, NY: Public Affairs, 2021.

[30] T. Heath. (2018). Beijing's influence operations target Chinese diaspora. [Online]. Available: https://warontherocks.com/2018/03/beijings-influence-operations-target-chinese-diaspora/ [Accessed: Oct. 24, 2022].

[31] B. Rolfe, "Building an electronic repertoire of contention," *Social Movement* Studies, vol. 4, pp. 65–74, 2005, doi: 10.1080/14742830500051945.

[32] C. Tilly, *From mobilization to revolution*. New York, NY: Random House, 1978.

[33] M.M. Hussain, P.N. Howard, "What best explains successful protest cascades? ICTs and the fuzzy causes of the Arab Spring," *International Studies* Review, vol. 15, pp. 48–66, 2013, doi: 10.1111/misr.12020.

[34] A.A Khan, "The role social of media and modern technology in Arabs Spring," *Far East Journal of Psychology and Business*, vol. 7, no. 4, pp. 56–63, 2012.

[35] P.N. Howard, M.M. Hussain, "The role of digital media," *Journal of Democracy*, vol. 22, pp. 35–48, 2011, doi: 10.1353/jod.2011.0041.

[36] D.M. Moss, "Transnational repression, diaspora mobilization, and the case of the Arab Spring," *Social Problems*, vol. 63, pp. 480–498, 2016, doi: 10.1093/socpro/spw019.

[37] A.F. Brantly, "From cyberspace to independence square: Understanding the impact of social media on physical protest mobilization during Ukraine's Euromaidan Revolution," *Journal of Information Technology & Politics,* vol. 16, no. 4, pp. 360–378, 2019, doi: 10.1080/19331681.2019.1657047.

[38] G. King, J. Pan, M.E. Roberts, "How censorship in China allows government criticism but silences collective expression," *American Political Science Review*, vol. 107, pp. 326–343, 2012, doi: 10.1017/s0003055413000014.

[39] P.N. Howard, S.D. Agarwal, M.M. Hussain, "The dictators' digital dilemma: When do states disconnect their digital networks?," *Social Science Research Network*, vol. 13, 2011, doi: 10.2139/ssrn.2568619.

[40] S. Feldstein, *The rise of digital repression: How technology is reshaping power, politics, and resistance*. New York, NY: Oxford University Press, 2021, doi: 10.1093/oso/9780190057497.001.0001.

[41] S. Feldstein. (2021). Governments are using spyware on citizens. Can they be stopped? [Online]. Carnegie Endowment for International Peace. Available: https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019 [Accessed: Oct. 18, 2022].

[42] A. Brantly, "The cyber losers," *Democracy and Security*, vol. 10, pp. 132–155, 2014, doi: 10.1080/17419166.2014.890520.

[43] J.P. Barlow. (1996). A declaration of the independence of cyberspace. [Online]. Electronic Frontier Foundation. Available: https://www.eff.org/cyberspace-independence [Accessed: Aug. 30, 2021].

[44] C. Shirky, *Here comes everybody: The power of organizing without organizations*. New York, NY: Penguin Press, 2008. http://digitool.hbz-nrw.de:1801/webclient/DeliveryManager?pid=2469081&custom_att_2=simple_viewer.

[45] C. Shirky. (2010). The political power of social media. [Online]. *Foreign Affairs*. Available: https://www.foreignaffairs.com/articles/2010-12-20/political-power-social-media. [Accessed: Oct. 24, 2022]

[46] R. MacKinnon, *Consent of the networked: The worldwide struggle for Internet freedom*. New York, NY: Basic Books, 2012.

[47] S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, 1st ed. New York: NY: PublicAffairs Press, 2019.

[48] J.R. Lindsay, "Cyber espionage," in *The Oxford handbook of cyber security*, P. Cornish, Ed. Oxford: Oxford University Press, 2021, pp. 223–238, doi: 10.1093/oxfordhb/9780198800682.013.12.

[49] M.E. Roberts, *Censored: Distraction and diversion inside China's great firewall*. Princeton, NJ: Princeton University Press, 2018, doi: 10.23943/9781400890057.

[50] E. Politou, E. Alepis, C. Patsakis, "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions," *Journal of Cyber Security*, vol. 4, pp. 1–20, 2018, doi: 10.1093/cybsec/tyy001.

[51] J. van Hoboken, "The privacy disconnect," in *Human rights in the age of platforms*, R.F. Jorgensen, Ed. Cambridge, MA: MIT Press, 2019, pp. 255–284.

[52] A. Brantly, "Utopia Lost – Human Rights in a Digital World," *Applied Cybersecurity & Internet Governance*, vol. 1, no. 1, pp. 1–19, 2022, doi: 10.5604/01.3001.0016.1238.

[53] B. Schneier, *Data and Goliath: The hidden battles to collect your data and control your world*. New York, NY: W.W. Norton & Company, 2015. http://www.worldcat.org/title/data-and-goliath-the-hidden-battles-to-collect-your-data-and-control-your-world/oclc/904399710.

[54] K. Levy, B. Schneier, "Privacy threats in intimate relationships," *Journal of Cyber Security*, vol. 6, pp. 1-13, 2020, doi: 10.1093/cybsec/tyaa006.

[55] W. Diffie, S.E. Landau, *Privacy on the line: The politics of wiretapping and encryption*. Cambridge, MA: MIT Press, 1999.

[56] K. O'Hara, W. Hall, *Four internets: Data, geopolitics, and the governance of cyberspace*. New York, NY: Oxford University Press, 2021.

[57] S. Nagaraia, R. Anderson. (2009). The snooping dragon: Social-malware surveillance of the Tibetan Movement. [Online]. Cambridge: University of Cambridge Computer Laboratory. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf [Accessed: Oct. 24, 2022].

[58] R. Deibert, R. Rohozinski. (2009). Tracking GhostNet: Investigating a cyber espionage network. [Online]. Toronto, CA: The Citizen Lab and The SecDev Group.

Available: https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf [Accessed: Oct. 24, 2022].

[59] T. Zeynep, *Twitter and tear gas*: *The power and fragility of networked protest*. New Haven, CT: Yale University Press, 2017.

[60] K. Zetter. (2021). The NSO "surveillance list": What it is and isn't, zero day. [Online]. Available: https://zetter.substack.com/p/the-nso-surveillance-list-what-it [Accessed: Aug. 30, 2021].

[61] Amnesty International. (2021). Forensic methodology report: How to catch NSO Group's Pegasus. [Online]. London: Amnesty International. Available: https://www.amnesty.org/en/documents/doc10/4487/2021/en/ [Accessed: Jul. 27, 2023].

[62] B. Marczak, A. Abdulemam, N. Al-Jizawi, S.A. Berdan, J. Scott-Railton, and R. Deibert. (2021). From Pearl to Pegasus Bahraini Government hacks activists with NSO Group Zero-Click iPhone exploits. [Online]. The Citizen Lab. Available: https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/ [Accessed: Aug. 30, 2021].

[63] D. Priest. (2021). A UAE agency put Pegasus spyware on phone of Jamal Khashoggi's wife months before his murder, new forensics show. [Online]. *The Washington Post*. Available: https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/ [Accessed: Oct. 25, 2022].

[64] P. Rueckert. (2021). Pegasus: The new global weapon for silencing journalists. [Online]. Forbidden Stories. Available: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/ [Accessed: Aug. 9, 2023].

[65] W.P. Staff. (2021). Takeaways from the Pegasus project. [Online]. *The Washington Post*. Available: https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/ [Accessed: Aug. 2, 2023].

[66] C. Edwards and E. Fernández. *Reframing health and health policy in Ireland: A governmental analysis*, 4th Edn. Cambridge: Manchester University Press, 2017. http://www.jstor.org/stable/j.ctv18b5nmg.

[67] Y. Gorokhovskaia, N. Schenkkan, G. Vaughan. (2023). *S*till not safe: Transnational repression in 2022. [Online]. Washington, DC: Freedom House. Available: https://freedomhouse.org/sites/default/files/2023-04/FH_TransnationalRepression2023_0.pdf [Accessed: Aug. 10, 2023].

[68] M. Michaelsen. (2020). The digital transnational repression toolkit, and its silencing effects. [Online]. Washington, DC: Freedom House. Available: https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects [Accessed: Oct. 25, 2022].

[69] Y. Gorokhovskaia, I. Linzer. (2020). Defending democracy in exile. [Online]. Washington, DC: Freedom House. Available: https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf [Accessed: Oct. 25, 2022].

[70] M. Michaelsen, "Far away, so close: Transnational activism, digital surveillance and authoritarian control in Iran," *Surveillance Society*, vol. 15, pp. 465–470, 2017, doi: 10.24908/ss.v15i3/4.6635.

[71] M. Fatafta, "Transnational digital repression in the MENA Region," in *Digital activism and authoritarian adaptation in the Middle East*. Project on Middle East

Political Science. Stanford, CA: Stanford Cyber Policy Center, 2021. Available: https://pomeps.org/wp-content/uploads/2021/08/POMEPS_Studies_43_Draft3-1.pdf#page=42.

[72] J. Earl, T.V. Maher, J. Pan, "The digital repression of social movements, protest, and activism: A synthetic review," *Science Advances*, vol. 8, eabl8198, 2022, doi: 10.1126/sciadv.abl8198.

[73] A. Dukalskis, S. Furstenberg, Y. Gorokhovskaia, J. Heathershaw, E. Lemon, N. Schenkkan, "Transnational repression: Data advances, comparisons, and challenges," *Political Research Exchange*, vol. 4, no. 1, 2104651, 2022, doi: 10.1080/2474736x.2022.2104651.

[74] B. Jardine, E. Lemon, N. Hall. (2021). No space left to run: China's transnational repression of Uyghurs. [Online]. Washington, DC: Oxus Society for Central Asian Affairs. Available: https://oxussociety.org/wp-content/uploads/2021/06/transnational-repression_final_2021-06-24-1.pdf [Accessed: Aug. 9, 2023].

[75] D. Silverberg. (2022). Digital repression across borders is on the rise [Online]. *MIT Technology Review*. Available: https://www.technologyreview.com/2022/07/08/1055582/digital-repression-across-borders-is-on-the-rise/ [Accessed: Oct. 25, 2022].

[76] A. Hern. (2015). Hacking Team Hack casts spotlight on murky world of state surveillance. [Online]. *The Guardian*. Available: https://www.theguardian.com/technology/2015/jul/11/hacking-team-hack-state-surveillance-human-rights [Accessed: Oct. 25, 2022].

[77] L.H. Newman. (2018). DC's Stingray mess won't get cleaned up. [Online]. *Wired*. Available: https://www.wired.com/story/dcs-stingray-dhs-surveillance/ [Accessed: Oct. 25, 2022].

[78] A. Brantly, N. Cal, D. Winkelstein, *Defending the borderland: Ukrainian military experiences with IO, cyber, and EW*. West Point, NY: United States Army Cyber Institute, 2017. http://www.dtic.mil/dtic/tr/fulltext/u2/1046052.pdf.

[79] C. Doctorow, *Little brother*. New York, NY: Tom Doherty Associates, 2008.

[80] K. Kertysova, "Artificial intelligence and disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered," *Security and Human Rights*, vol. 29, pp. 55–81, 2018, doi: 10.1163/18750230-02901005.

[81] A. Zervopoulos, A.G. Alvanou, K. Bezas, A. Papamichail, M. Maragoudakis, K. Kermanidis, "Deep learning for fake news detection on Twitter regarding the 2019 Hong Kong protests," *Neural Computing & Applications*, vol. 34, pp. 969–982, 2022, doi: 10.1007/s00521-021-06230-0.

[82] M.N. Schmitt, L. Vihul (Eds.), *Tallinn Manual 2.0 on the international applicable to cyber operations*. Cambridge: Cambridge University Press, 2017.

[83] K. Tai, Y.Y. Zhu, "A historical explanation of Chinese cyber sovereignty," *International Relations of the Asia-Pacific*, vol. 22, no. 3, pp. 469–499, 2022, doi: 10.1093/irap/lcab009.

[84] M.L. Mueller, *Networks and states: The global politics of internet governance*. Cambridge, MA: MIT Press, 2013, doi: 10.7551/mitpress/9780262014595.001.0001.

[85] R. Shandler, M.L. Gross, D. Canetti, "A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United

Kingdom, and Israel," *Contemporary Security Policy*, vol. 42, pp. 1–28, 2021, doi: 10.1080/13523260.2020.1868836.

[86] E.D. Borghard, S.W. Lonergan, "Cyber operations as imperfect tools of escalation," *Strategic Studies Quarterly*, vol. 13. no. 3, pp.122–145, 2019.

[87] S. Kreps, J. Schneider, "Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics," *Journal of Cybersecurity*, vol. 5, no. 1, pp. 1–11, 2019, doi: 10.1093/cybsec/tyz007.

[88] M. Abromwitz, N. Schenkkan. (2021). The long arm of the authoritarian state. [Online]. *The Washington Post*. Available: https://www.washingtonpost.com/opinions/2021/02/03/freedom-house-transnational-repression-authoritarian-dissidents/ [Accessed: Oct 25, 2022].

[89] M. Michaelsen. (2020). Silencing across borders: Transnational repression and digital threats against exiled activists from Egypt, Syria, and Iran. [Online]. The Hague: Hivos. Available: https://hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf [Accessed: Oct. 25, 2022].

[90] Coda Media. (2021). Putin's playbook: Strongmen around the world are using Russian tactics to quell dissent. [Online]. Available: https://www.codastory.com/disinformation/russias-foreign-agents-law-reverberates-around-the-world/ [Accessed: Oct. 25, 2022].

[91] Human Rights Watch. (2021). Spyware used to hack Palestinian rights defenders. [Online]. Available: https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders [Accessed: Oct. 25, 2022].

[92] Y. Gorokovskaia, A. Datt. (2022). How to resist China's campaign of transnational repression. [Online]. Washington DC: Freedom House. Available: https://freedomhouse.org/article/how-resist-chinas-campaign-transnational-repression [Accessed: Oct. 25, 2022].

[93] N. Al-Jizawi, S. Anstis, S. Barnett, S. Chan, N. Leonard, A. Senft, R. Deibert. (2022). Psychological and emotional war: Digital transnational repression in Canada. [Online]. Toronto, CA: Citizen Lab. Available: http://tld-documents.llnassets.com.s3.amazonaws.com/0034000/34289/citizen%20lab%20report.pdf [Accessed: Oct. 25, 2022].

[94] Human Rights Watch. (2021). They don't understand the fear we have: How China's long reach of repression undermines academic freedom at Australia's universities. [Online]. Available: https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines [Accessed: Oct. 25, 2022].

[95] S. Rotella. (2021). Even on U.S. campuses, China cracks down on students who speak out. [Online]. ProPublica. Available: https://www.propublica.org/article/even-on-us-campuses-china-cracks-down-on-students-who-speak-out [Accessed: Oct. 25, 2022].

[96] M. Russell. (2022). "Foreign agents" and "undesirables": Russian civil society in danger of extinction. [Online]. Brussels: European Parliamentary Research Service. Available: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729297/EPRS_BRI(2022)729297_EN.pdf [Accessed: Oct. 25, 2022].