Brief No. 12.1

TRANSNATIONAL REPRESSION

The Long Arm of Authoritarianism

Katherine Armstrong

P | I | P | S

Transnational Repression
The Long Arm of Authoritarianism

APRIL 2020

Katherine Armstrong

P | I | P | S
The Project on International Peace and Security
Global Research Institute
College of William & Mary

Transnational Repression
The Long Arm of Authoritarianism

Non-democratic regimes increasingly use the internet to reach across borders to track, hack, blackmail, and harass emigrants. Although often viewed as isolated cybercrimes, these attacks represent an expansion of extraterritorial authoritarian control. Technologically based and facilitated tactics allow non-democratic states to manipulate emigrant communities from afar. Moreover, these capabilities may be used to target actors who are critical to U.S. security, such as politicians and members of the military and intelligence communities.

The targeting of co-ethnic and co-national U.S. citizens and residents threatens U.S. civil society, democracy, sovereignty, and—if left unchallenged—security. The United States should address this threat by taking steps to deter perpetrators and defend targets. For example, the Department of State should support non-governmental organizations in maintaining a comprehensive watch list that publicizes incidents of transnational repression and ranks states' propensity to engage in this behavior. The U.S. government and international community should consider states' rankings when making policy regarding aid, diplomatic relations, and trade.

Introduction

Global audiences were shocked in 2018 by the brutal murder of Jamal Khashoggi, a vocal critic of Saudi Crown Prince Mohammed bin Salman's policies, in the Saudi consulate in Istanbul. Yet emigrants around the world face attacks by their kin states that are unrecognized, unmonitored, and underreported because they occur via information and communication technologies (ICTs). The attack against Khashoggi is part of the growing trend of transnational repression. Saudi Arabia and other Gulf States, China, Russia, Iran, Turkey, Morocco, Egypt, Eritrea, Zimbabwe, Syria, and Tajikistan are some of the countries developing strategies to control extraterritorial populations.[1]

This analysis examines the phenomenon of transnational repression. It explains the circumstances that created a need for extraterritorial control and describes how technology shapes the toolkit used to repress. It explores six tactics that vary in severity, but share a goal of imposing costs and changing a target's behavior through intimidation and manipulation.

The use of transnational repression against co-ethnics and co-nationals has immediate consequences for U.S. democracy, sovereignty, and partnerships with other countries. It is also an emerging threat to national security. Because the toolkit can be used against non-co-ethnics and non-co-nationals—and is, in fact, already being used against these targets to a limited extent—expansion of targets is likely to occur in the coming years.

This paper analyzes which tactics pose the greatest risk and describes three possible scenarios of expanded targeting. The United States can intervene to discourage transnational repression practices by holding non-democratic states accountable and protecting the targets of attacks.

The Phenomenon of Transnational Repression

Transnational repression, a subcategory of transnational authoritarianism, is a systematic effort to prevent political dissent, generally by an authoritarian or non-democratic state, through targeting the members of its emigrant or diaspora communities.[2] Sending or 'kin' states use long-distance strategies to surveil and intimidate emigrant populations.[3] The purpose of extraterritorial repression practices is to deter or encourage a specific activity by imposing a financial, social, psychological, or physical cost on the target.[4]

- *Co-ethnic and co-national targets*. Non-democratic states draw on nationality, ethnicity, religion, and cultural ties to decide who is subject to their rule, increasingly crossing geographic borders. Co-ethnics (individuals of the same ethnicity as the population of the kin state) and co-nationals (individuals with the nationality of the kin state), as well as their close descendants, are often viewed as belonging to countries' extraterritorial populations. As communication and transportation have advanced, non-democratic states have improved their ability to control their populations across geographic boundaries.

  This paper focuses on targets in host or receiving states that are liberal democracies, with the assumption that these cases are most relevant to U.S. interests. Liberal democracies are countries that are labeled as "free" by the *Freedom in the World* 2019 Report and fall between 6 and 10 on the Polity IV scale.[5] Although the targets of transnational repression are co-ethnic and co-national individuals by definition, the development of these capabilities also poses a threat to non-co-ethnics and non-co-nationals.

- *Non-democratic state perpetrators*. Multilateral organizations and non-state actors may participate in transnational repression.[6] This paper, however, focuses on non-democratic states' transnational repression practices. Non-democracies are defined here as countries that are "partly free" or "not free" according to the *Freedom in the World* 2019 Report and fall between -10 and 5 on the Polity IV scale.[7]

- *A set of practices*. This paper conceptualizes authoritarianism as more than a regime type. Authoritarianism is a mode of governance characterized by a distinct set of practices. These authoritarian practices may be observed in a range of political regimes.[8] By using a broader conception of authoritarianism, we can capture how transnational authoritarianism stretches across borders to infiltrate other regime types.[9] Democratic host states sometimes tolerate or even enable transnational repression across borders.[10]

Is Transnational Repression Effective?

Transnational repression alters the cost-benefit calculation individuals make before taking an action. It raises the cost of activities against the kin state, thereby affecting whether and how individuals engage in these activities.[11] The success of these tactics in controlling individuals' behavior depends on the tactic used, the target's political engagement, the presence of proxies in the kin state,[12] and the perceived capacity of the kin state to carry out threats,[13] among other factors.[14] Regardless of whether the tactic succeeds in altering a specific behavior, all tactics

impose financial, social, psychological, or physical costs on the target.[15] For an evaluation of the likelihood of success by tactic, see the Appendices.

Growing in Scope and Frequency

The number of governments practicing transnational repression is increasing, with the practice becoming commonplace in the Middle East, Northern Africa, sub-Saharan Africa, and Central Asia.[16] Freedom House found that 24 countries, including Russia, China, Iran, Saudi Arabia, and Turkey, had recently used such tactics.[17] Case studies reveal the growing pervasiveness of extraterritorial repression, although quantitative measures of transnational repression are rare.[18] The stark increase in INTERPOL alerts since the 2000s is one of the few available indicators of the growing trend. Red Notices increased by 60 percent after technological improvements to the INTERPOL system in 2009. Fair Trials International notes that non-democracies can exploit the new system to rapidly spread false or misleading information about individuals.[19]

Due to the proliferation and improvement of communications and transportation technology in the past two decades, transnational repression has become more common.[20] The tools of repression have shifted to exploit technological changes. Today's relatively widespread technology-based attacks either have no historical equivalent or have historical equivalents that are far inferior in affordability, speed, and immunity to distance and were therefore less frequently used.

The Control of Populations: Exit and Voice[21]

Autocratic states encounter an *illiberal paradox*—a trade-off between political incentives to control their borders and economic incentives to allow emigration.[22] Non-democracies wish to restrict emigration for political and security reasons: to suppress dissent and ensure thorough control over their citizens. They wish to encourage emigration because of the economic benefits tied to cross-border mobility: remittances, skills acquisition, and unemployment relief.[23]

Emigrant populations create a vulnerability for non-democracies. ICTs allow these populations to communicate with friends and family in the kin state. For emigrants living in democratic host states, information relayed to friends and relatives is likely to be critical of the repressive leaders and policies of the kin state. As "bridge figures," emigrants can create external pressure on the sending state, often through transnational advocacy networks.[24]

Controlling Exit in the Past

In the past, autocracies generally securitized emigration at the border. Migration was tightly regulated in the Soviet bloc, as exemplified by East Germany's construction of the Berlin Wall.[25] Transnational repression also occurred—for example, by Turkey, Egypt, Iran, and Russia.[26] Trotsky's 1940 assassination in Mexico on Stalin's orders,[27] the infiltration of student opposition groups in Europe by the Shah's secret service, the 1979 assassination of the deposed Shah's

nephew in Paris by the Islamic Republic of Iran, and the 1992 assassination of Kurdish opposition members in Berlin by the Islamic Republic are early examples of transnational repression.[28] Transnational repression is not a new practice, but its current pervasiveness is unprecedented. The tactics used are also evolving due to the improvement and expansion of ICTs.[29]

Today: Silencing Voice after Exit

Non-democratic governments manage the risks posed by population mobility[30] and an expanded public sphere by designing policies to handle co-ethnic and co-national populations outside their territorial boundaries. Technology and globalization lead non-democracies to resolve the illiberal paradox by silencing "voice" rather than controlling exit.[31] The expansion of transnational authoritarianism does not necessarily indicate enhanced authoritarian power. Rather, this expansion is an adaptation to the contemporary challenges and opportunities posed by ICTs.[32]

Implications of Technology for Extraterritorial Authoritarian Rule

Securitization of exit is now rarer because globalization increases the benefits of allowing emigration.[33] Falling transportation costs and global economic dependence make migration easy and expected. However, technological developments also create vulnerabilities for sending states.

- *Extensity and velocity of communication flows*. Communication is faster and more extensive. The cost of communication is usually unaffected by the distance it travels.[34] ICTs turn exiles and emigrants into a greater threat to non-democratic regimes, yet provide these regimes with cheap options to silence them with deniability. Extraterritorial populations are more capable of exercising voice in sending states, while the government can more efficiently suppress voice from abroad.[35]

- *Growing benefits of emigration*. Opportunities for education abroad, relief of unemployment pressures, and remittances encourage non-democratic states to allow emigration.[36] Transportation and communication technologies make these advantages more accessible to emigrant-sending states. For instance, companies like Western Union facilitate remittance sending online.

- *Increased population mobility*. Migration has increased since World War II. The intensity of international migration is due in part to lower transportation costs and shorter travel times. For the same reason, migration is now often circular (i.e. repeated migration between the kin and host state) and is no longer a definitive break with the sending state.[37]

- *An expanded public sphere*. Because of circular migration and extensive, rapid communication flows, territorial boundaries no longer define the national public sphere. Physical departure from a country may not entail exit from its public sphere.[38]

Non-democratic states benefit economically from emigration. Technological advancements, however, allow emigrants to maintain close ties with the national public sphere, which creates

political vulnerabilities for the sending state. Non-democracies have learned to harness technology and leverage transnational ties to maintain control over emigrants' voice after exit.

The Repertoire of Transnational Repression

> *Today, extraterritorial repression is more pervasive, and authoritarian states have various functional equivalents to physical control at their disposal.*
>
> Marlies Glasius, *Authoritarianism in a Global Age*, 2018[39]

Digital communications technology creates an opportunity for emigrants and exiles to communicate with residents of their kin states and to engage in activism. Simultaneously, ICTs allow non-democratic regimes to control emigrants from afar.[40] Digital media and social networks support the communication that makes transnational repression necessary in the eyes of kin states, while enabling new and facilitating existing mechanisms of transnational repression.[41]

Governments Have the Technological Upper Hand

States are better able to exploit the opportunity afforded by technology than individuals or activist groups.[42] ICTs allow states to monitor quickly and easily the activity of emigrants on a large scale.[43] Limited accountability and oversight by other governments or international bodies allow states to use technological tools of repression against political targets with few consequences.[44]

- *Availability of personal data*. The data revolution makes individuals vulnerable to exploitation by governments. Because non-democratic governments are not held accountable to their publics to the same degree as liberal democracies, they can harness the data and technological revolutions to control their populations domestically and abroad.[45] Personal information, such as phone numbers, facilitates cyberattacks and other tactics.

- *Lowered cost of surveillance technology*. Once available only to elite intelligence agencies, social media surveillance technology is now widely accessible to non-democratic governments.[46] The cost of such surveillance has drastically lowered as the social media surveillance market has grown, China has begun to export the technology, and governments have shifted to automated surveillance.[47] Government purchases of technology to monitor a population's behavior on social media are increasingly common.

Technology Underlies the New Repertoire

The repertoire of transnational repression today is largely consistent with past tactics, which included propaganda campaigns, infiltration of exile groups, property confiscations, citizenship revocation, persecution of relatives, and assassinations.[48] However, the current toolkit is based on and facilitated by new technologies. Digital media and networks are fundamental to modern transnational repression practices.[49] While perpetrators borrow practices used by cybercriminals,[50]

transnational repression is more than just cybercrime—it is politically motivated and state-sponsored. ICTs offer "functional equivalents to physical control" that are cheaper, easier, faster, and more scalable.[51] The modern toolkit is thus different in kind as well as in degree.

The most significant change in kind due to the adoption of technologically based and facilitated techniques is the lack of accountability for attacks. The internet is anonymous compared to physical control and other traditional means.[52] Limited regulation of the internet and difficulty of attribution results in perpetrators often not being held accountable.

The contemporary repertoire includes techniques that vary in severity of effect,[53] including physical, psychological, and symbolic damage (see Figure 1). This typology offers a comprehensive view of the toolkit of transnational repression, but its categories are neither exhaustive nor mutually exclusive. In practice, targeting often involves a combination of tactics.

Figure 1: Transnational Repression Tactics

T.R. Tactic	Definition	Examples
Disinformation	Use of false, misleading information for the purpose of damaging a victim's reputation or causing psychological distress	Social media campaigns, smear campaigns on state media, personalized disinformation messages
Passive Cyberattacks	Hacking into a victim's accounts and/or devices without actively harming the victim	Surveillance, location tracking, monitoring communications
Active Cyberattacks	Hacking into a victim's accounts and/or devices such that the attack has direct consequences for the victim	Posting via victim accounts, commandeering bank or other accounts, censorship, distributed denial-of-service attacks
Institutional Measures	Use of laws or institutions to harass or detain a victim	Abuse of INTERPOL Red Notices and diffusions, arrest, extradition, revocation of citizenship, revocation of scholarships
Threats of Violence	Threatening the victim or individuals close to the victim (proxies) with physical violence	Phone threats, threatening messages, in-person visits
Physical Violence	Use of violence against the victim or proxies	Assault, assassination

Disinformation

Disinformation for transnational repression is the use of false or misleading information to damage a victim's reputation, disorient, or frighten. Disinformation includes misleading personalized

messages and smear campaigns on state-controlled traditional media. In recent years, social media campaigns have emerged as an easily deniable alternative to state-controlled media.

> *Guo Wengui*. The disinformation campaign against exiled Chinese businessman Guo Wengui was the most extensive one recorded in a dataset of coordinated Twitter accounts that conducted information operations against the Hong Kong protestors. The campaign spanned from April 2017 to the end of the dataset in July 2019. Guo Wengui, otherwise known as Miles Kwok, fled to the United States from China in 2017 after the arrest of his associate, the former Vice Minister of State Security. Guo is now a vocal critic of the Chinese government.
>
> Guo's public allegations of corruption against prominent government officials led the Chinese government to accuse him of corruption and issue an INTERPOL Red Notice. Days after issuance of the Red Notice, an onslaught of tweets mostly in Chinese criticizing Guo's character and relationships began—the dataset includes at least 38,732 tweets targeting Guo.
>
> The tweets targeting Guo began to overlap with tweets criticizing the Hong Kong protestors. The tweet volume by day of the week, repetition according to an apparently automated schedule, and the correlation between tweet volume and developments in Guo's deteriorating relationship with the Chinese government imply professional, government-tied use. The disinformation attack likely sought to sway overseas Chinese populations and discourage critical voices in Western media.[54]

Passive Cyberattacks

Passive cyberattacks primarily use surveillance: perpetrators access a victim's accounts, social networks, or devices without actively harming the victim. Passive cyberattacks include location tracking, monitoring of communications, and other online surveillance. Such attacks may serve to gather information before an active cyberattack or other type of attack.

Pegasus software is an example of how governments conduct passive cyberattacks. Governments purportedly use the malware, sold by the Israeli firm NSO Group, to target criminals and terrorists.[55] However, Citizen Lab found that over 100 activists, human rights defenders, and journalists were hacked by governments, such as Saudi Arabia and the United Arab Emirates, using NSO Group's tools.[56] Pegasus exploits weaknesses of the messaging app WhatsApp to spy through users' phones. The malware can gather files from the phone; trace calls, messages, and keystrokes; track location; and turn on the microphone and camera.[57] Before WhatsApp fixed a vulnerability, the malware could embed through a call—even if the target did not pick up the call.[58]

> *Afaf Mahfouz*. Afaf Mahfouz is a civil society activist living in Florida who works with women's groups in Egypt. She was on the list of 33 Egyptian intellectuals, journalists, lawyers, opposition politicians, and activists—some living in the United States, Canada, and Britain—whose phones were embedded with surveillance software beginning in 2016. Server registration and geographic coordinates linked the malware to Egyptian government

authorities. Embedded via mobile phone applications, the malware allowed government officials to track the phone's location, see whom the target contacted, and read emails and files. Without notification from Human Rights Watch, Mahfouz would not have known that her mobile phone was under surveillance.[59]

Active Cyberattacks

Active cyberattacks, like passive ones, involve accessing a victim's accounts, communications, social networks, or devices, but have direct consequences for the victim. Posting via a victim's accounts, commandeering accounts, censorship, and distributed denial-of-service attacks are types of active cyberattacks. WeChat's censoring of political messages and disabling of the accounts of users who voice support for the Hong Kong protestors—including users in the United States—is an example. One WeChat user explained that he no longer discusses politically sensitive topics to keep relatives in China safe and ensure that he can still travel to China.[60] Since active cyberattacks usually include surveillance, they can be difficult to differentiate from passive cyberattacks.

Iranian activists. Iranian activists who went into exile during the Green Movement that arose after the 2009 elections have been the targets of systematic transnational repression, especially active cyberattacks. These activists use digital means to communicate with contacts in Iran. However, their online communications have made them vulnerable. The Iranian government hacked individuals through customized phishing. Agents of the Islamic Republic also sought to infiltrate the Facebook groups and social networks of activists to interfere with their activities. Farsi news media outside of Iran faced distributed denial-of-service attacks. The assaults on exiled Iranian activists are not limited to active cyberattacks, but they demonstrate the use of active cyberattacks to silence dissidence.[61]

Institutional Measures

Non-democracies use domestic and international laws and institutions to harass or detain victims. Arrest, extradition, cancellation of scholarships, and revocation of citizenship may be used to target emigrants.[62]

Non-democracies routinely use international organizations, especially the International Criminal Police Organization (INTERPOL), to silence criticism of their political regimes, leaders, and policies.[63] INTERPOL's system of alerts includes Red Notices and diffusions. Red Notices are alerts that a person is wanted for arrest and extradition. While they are intended to be issued for criminals, Red Notices and diffusions (similar in effect to Red Notices, although less formal and subject to less oversight[64]), are issued against dissidents and civil society activists. Abusing countries include, but are not limited to, Turkey, Russia, China, Kazakhstan, Tajikistan, Uzbekistan, and Venezuela.[65]

The INTERPOL alert system violates the principle of due process because the organization cannot notify individuals of a notice against them without the issuing country's permission.[66] Even when alerts do not lead to extradition, they raise the cost of dissent through travel restrictions, separation

of families, business complications, difficulty opening bank accounts, and revocation of visas.[67] Red Notices are sometimes successful in changing targets' behavior through "gagging."[68]

> *Enes Kanter*. Enes Kanter is a center for the Boston Celtics, an alleged Gülenist, and an outspoken critic of President Erdoğan. Along with harassment encouraged by Turkish ministers, Kanter has faced pressure from Turkish consulates in the United States and harassment by the Turkish government. In 2017, Kanter learned that the Turkish government had revoked his passport and labeled him a terrorist. Turkey issued an INTERPOL Red Notice against Kanter, severely restricting his international travel.[69]

Threats of Physical Violence

Threats of physical violence against the victim or proxies—usually relatives—are often effective silencing mechanisms. Government agents may issue threats in person, but increasingly use phone calls or online messages.

> *Gulhumar Haitiwaji*. Gulhumar Haitiwaji, a resident of France, is one of many Uyghurs in Europe and North America whose relatives have been threatened with physical violence through phone calls and WeChat. Haitiwaji became an outspoken critic of policies in Xinjiang Province, China, when her mother disappeared into a 're-education' camp in 2017. She appeared on television and started a petition for her mother's release with almost 500,000 signatures. In 2019, Haitiwaji began receiving calls from her mother asking her to delete her posts if she "ever wanted to see her [Haitiwaji's mother] alive again." Following these phone calls and threats against her mother from Chinese officials, she cancelled a planned appearance at a human rights summit in Geneva in 2019. Haitiwaji's withdrawal from public activism suggests that the Chinese effort to silence Uyghurs in Europe and North America using proxy threats of violence has found a degree of success.[70]

Physical Violence

Government agents may use physical violence against the victim or proxies. Violence may range from assault to assassination. Physical violence often silences the targeted behavior. Lethal violence, while effective in silencing an individual's voice, can produce a backlash. At the same time, a single assassination can send a potent signal to other dissidents.[71]

> *Sergei Skripal*. Sergei Skripal, a former Russian military intelligence officer, was the victim of an assassination attempt in Salisbury in 2018.[72] Skripal had acted as a double agent for the United Kingdom in the 1990s and 2000s and settled in the United Kingdom in 2010. Skripal and his daughter were poisoned with a nerve agent, the sophistication of which points to a state perpetrator. The poisoning led to the expulsion of Russian diplomats from EU and NATO countries.[73] The international response was atypical: only high-profile, violent incidents typically lead to clear consequences for the perpetrator.[74]

The Consequences of Transnational Repression

Transnational repression has repercussions for civil society, interstate relations, and security. The silencing and intimidation of co-ethnic and co-national intellectuals, activists, and other key players in civil society should be of immediate concern to the United States.

The U.S. government should anticipate an expansion of targets to include strategic individuals, such as politicians, members of the intelligence community, and military service members using the tactics that non-democratic governments are honing to control co-ethnics and co-nationals.

- *Weakens democracy*. The expansion of authoritarian practices into democratic states threatens civil society and democracy. For example, non-democracies use social media surveillance to detect and deter protest in liberal democracies. The stifling effect of surveillance on free expression is well studied. Monitoring leads to self-censorship by dissidents, minorities, activists, and journalists.[75] Transnational repression violates free speech rights by censoring directly (i.e. removing content) and indirectly (i.e. intimidating into silence). Transnational repression prevents residents of liberal democracies from exercising democratic rights, including freedom of speech and freedom of association.

  Institutional tactics weaken democratic institutions. The use of multilateral institutions for repression undermines their legitimacy. Abuse of INTERPOL, for instance, weakens the organization's credibility in combatting real threats to the international community.

- *Jeopardizes U.S. partnerships*. When the perpetrator is a U.S. ally or partner, high-profile acts of transnational repression are likely to cause tension with the perpetrator state, whether the U.S. government responds with condemnation or the U.S. public agitates for a response. The murder of Jamal Khashoggi on the orders of Crown Prince Mohammed bin Salman demonstrates how transnational repression can complicate U.S. alliances and partnerships and create conflict in the U.S. government and civil society.[76]

- *Violates sovereignty*. Transnational repression is a violation of sovereignty because its perpetrators reach over borders to control the behavior of individuals in host states. The transnational nature of tactics used disregards the sovereignty of host states.[77]

- *Threatens homeland security.* The use of force by other countries within U.S. borders is a threat to homeland security. The United States has addressed past high-profile use of transnational force by states as a security threat. For instance, the 2011 plot to murder the Saudi ambassador to the United States on U.S. soil was considered "international terrorism transcending national boundaries" and resulted in criminal charges and sanctions.[78] Washington should similarly view incidents of transnational repression as a homeland security threat and act accordingly.

Conceptualizing Transnational Repression as a Security Threat

> *I heard no one cares about it. I'm not an American citizen yet, and even if you're a citizen, if it's not a national security issue, I heard they will not help.*
>
> Tahir Imin, Uyghur-American interviewed in UHRP report[79]

According to the Authoritarianism in a Global Age project, there is a gap in research—a failure to recognize extraterritorial uses of state power, especially by authoritarian regimes.[80] The few analysts who study extraterritorial repression recognize that states' long-distance coercive power threatens emigrant communities as well as civil society and democracy in host states. Practitioners and scholars, however, have not acknowledged the security threat to host states.

An Unmonitored Arena

Governments and observers dismiss transnational repression as isolated incidents, cybercrime, a civil society issue, or infighting among outsiders. As a result, it occurs in an unmonitored, unpoliced arena where states can perfect capabilities to control actors outside their borders with few to no consequences. Non-democratic regimes are unchallenged as they hone manipulation strategies that can be used against U.S. civil society, political, and security actors.

Expansion of Targets

Neglecting transnational repression will lead to an expansion of targets. The tactics used for transnational repression are not limited to co-ethnic and co-national targets, although some tactics are more transferable. Use of these capabilities against non-co-ethnic and non-co-national targets already occurs and can be expected to increase. For instance, tools of transnational repression are being used against journalists and military service members outside of emigrant communities. Furthermore, the economic influence of regimes like China creates conditions under which non-co-ethnic and non-co-national targets of pressure campaigns are more likely to comply with demands, as in the NBA-China tweet controversy.[81] Due to the likely expansion of targets, transnational repression is a growing as well as a current threat to U.S. national security.

- *Threat to co-ethnics and co-nationals in the United States*. Transnational repression affects co-ethnics and co-nationals who are legal residents and citizens of the United States. These targets include civil society leaders and may include strategic individuals, such as politicians, military service members, and members of the intelligence community.

  The targeting of co-ethnic and co-national security actors from the sending state already occurs. Alexander Litvinenko, a former Russian secret service agent, was poisoned in the United Kingdom in 2006.[82] Sergei Skripal, a former Russian military intelligence officer (and U.K. double agent) was the victim of an assassination attempt in the United Kingdom in 2018.[83] Former Azerbaijani parliament member Huseyn Abdullayev was extradited from Turkey to Azerbaijan in 2018, although he had political asylum in Germany.[84]

- *Expansion to non-co-ethnic/non-co-national targets*. Non-democratic regimes use the tactics they hone within the unmonitored arena of transnational repression against other (non-co-ethnic and non-co-national) targets. They will continue to expand the range of targets until the United States or other state actors credibly challenge this behavior and assert that the cost of practicing transnational repression exceeds its benefits.

  Non-co-ethnic journalists in liberal democracies are hacked, impersonated, and harassed by non-democratic countries, such as Russia, Iran, and Saudi Arabia.[85] The goal of this intimidation—to silence or discredit critical voices—and the tactics used parallel the transnational repression of emigrant communities.

  NATO troops in Eastern Europe are likewise being harassed and intimidated using the tools of transnational repression. "Technological enablers" are fundamental to the intimidation of both emigrant communities and NATO troops, allowing non-democracies to reach distant targets in a manner that is cheaper and more deniable than physical means.[86] U.K. troops in Estonia have been subject to threatening social media and text messages likely sent by Russia.[87] NATO personnel in Poland, Lithuania, and elsewhere in the Baltics have faced personalized disinformation and intimidation from Russia.[88]

  Russia tests its capabilities through these attacks on NATO troops.[89] By some accounts, Russia was emboldened in its attempts to manipulate the 2016 election by the United States' lack of response to earlier interference.[90] Similarly, Russia and other non-democracies test the waters through transnational repression and have not been challenged. Non-democracies' opportunities to develop and test techniques that can be used to intimidate or distress individuals, whether NATO personnel or co-ethnics, enable them to achieve strategic goals using these techniques.

Collaboration between Perpetrators

The tools of transnational repression can not only be used against new targets, but also by new perpetrators. Non-democratic states are learning from each other's methods of managing emigrant communities and projecting power.[91] Autocratic regimes are collaborating to develop practices and repurpose institutions to control populations abroad with minimal accountability.[92]

Cooperation occurs formally and informally.[93] Formal cooperation has occurred, for example, through the Shanghai Cooperation Organization (SCO). The SCO encourages regional security cooperation, including the sharing of data and possibly of surveillance technology, among China, Russia, and Central Asian states.[94] Since political dissidence is viewed as a security risk by non-democratic states, responses often fall into the 'security' realm.

Direct assistance, policy diffusion, and replication of methods are evident.[95] For instance, Russian transnational coercive strategies seem to borrow from Libyan ones.[96] Under Gaddafi's regime, an envoy in London tracked and eliminated political opponents in the United Kingdom—much as Russian emigrants have been attacked and assassinated in the 21st century.[97]

Tactics of Greatest Concern

Figure 2 below uses a novel risk assessment tool (see Appendix A) to determine which tactics of transnational repression should be of the greatest concern to U.S. policymakers. Each tactic is assigned a risk rating for each risk category (cost, immunity to distance, ease of attribution, likelihood of success, and transferability to non-co-ethnic/non-co-national targets) according to the risk assessment tool. The overall risk rating is based on a weighted sum of the five risk categories. The three technology-based tactics are high-risk, while the three technology-facilitated tactics are medium-risk. When designing policy to address transnational repression, U.S. officials should consider the risk rating of each tactic, as well as the feasibility of solutions.

Figure 2: Risk Ratings by Tactic[98]

T.R. Tactic (Overall Risk Rating)	**Cost**	**Immunity to Distance**	**Ease of Attribution**	**Likelihood of Success**	**Transferability to Non-Co-Ethnic Targets**
Disinformation (High risk)	High risk	High risk	High risk	Medium risk	High risk
Passive Cyberattacks (High risk)	High risk	High risk	High risk	Medium risk	High risk
Active Cyberattacks (High risk)	High risk	High risk	High risk	Medium risk	High risk
Institutional Measures (Medium risk)	Medium risk	Medium risk	Low risk	High risk	Medium risk
Threats of Violence (Medium risk)	Medium risk	Medium risk	Medium risk	High risk	Medium risk
Physical Violence (Medium risk)	Low risk	Medium risk	Low risk	High risk	Medium risk

Possible Scenarios: Strategic Individuals

Non-democracies are likely to use capabilities perfected within the 'unmonitored arena' of transnational repression—especially the high-risk, technology-based tactics—against non-co-ethnic and non-co-national targets. The following scenarios explore some of the repercussions that expanded targeting using high-risk tactics will likely have for U.S. civil society, democracy, and security. Foreign governments are already exercising influence on some non-co-ethnics and non-co-nationals within U.S. borders, foreshadowing escalation to situations like those described below. The consequences of these repression strategies will be financial, psychological, and social damage to individuals and potential behavioral change.

- *Active cyberattack against a politician*. A local politician, while not Iranian-American, has many Iranian-American constituents. She works closely with several Iranian-American organizations. In the past, she has publicly criticized the Islamic Republic of Iran's policies. She receives a phishing email that appears to be from a colleague and clicks on a link. She soon realizes that she can no longer access her mobile banking account. Her account has been hacked. She receives a threatening text message from an unknown number that warns her to break off contact with the Iranian-American groups and stop denouncing the Iranian government. Knowing that her constituents facing similar threats have not been able to access government protection, she concedes. In the next election cycle, she chooses not to run for re-election because she can no longer fulfill her duties as an elected official.

- *Disinformation against an economic leader*. The U.S. born Chief Executive Officer (CEO) of a major U.S. company posts on social media and shares with the press her disapproval of Chinese policies regarding censorship and the harassment and detention of Uyghurs. As her criticism garners attention from the public, more newspapers and social media users in the United States and abroad pick up the story. The CEO notices a barrage of negative posts directed at her. The posts accuse her of impropriety, question past business deals, and denounce her character. They are written in English and Mandarin. Hundreds of posts by Chinese government bots repeat these criticisms daily. The company's stock begins to suffer. Overwhelmed by the online harassment, the CEO retracts her statement and issues an apology. Despite living and working in the United States, the CEO no longer feels comfortable exercising freedom of expression due to the disinformation campaign.

- *Passive cyberattack against a social influencer*. A well-known social media influencer in the United States was approached online by unknown accounts that tried to engage him in conversation and encouraged him to post pro-Russian content. He refused. He then received a WhatsApp call from an unfamiliar account, which he declined. Several weeks later, he receives a message from a human rights organization that he has been the target of hacking. All his messages and phone calls are compromised. His phone camera and microphone may have been recording for weeks. Afraid of blackmail, the influencer accedes to the unknown users' demands. He believes that he has no choice but to comply, even though he does not agree with the material he now shares with his followers.

The tactics used to silence and manipulate emigrant communities can be used to target a variety of actors in the public space, as well as members of the military and intelligence communities. Given the current lack of government awareness and protection, U.S. individuals are vulnerable to threats and harassment from non-democratic regimes. If costs are not imposed on perpetrators and protections implemented for victims, these tactics will be used against strategic U.S. individuals.

Recommended Policy Actions

The following policy recommendations work to alter the risk levels described in the above risk ratings. They reduce risk levels by imposing additional costs on perpetrators (increasing *cost*) or by protecting victims (decreasing *likelihood of success*). Reducing the vulnerability of targets

protects victims in the short term and will change perpetrators' cost-benefit analysis over the long term. Raising cost and reducing likelihood of success should reduce non-democratic states' use of transnational repression practices. Because the toolkit is likely to change over time and tactics often overlap in practice, the following recommendations are not tactic-specific, except the recommendation for reducing INTERPOL abuse. Figure 3 below summarizes the effectiveness of each policy, ranked by cost, against each tactic. Policymakers should consider cost and effectiveness when designing a set of policies to combat transnational repression.

The United States should not tighten border controls as a response to this challenge, as border controls cannot protect the multitude of targets and potential targets already in the United States. Instead, Washington should take measures to limit non-democratic states' capacity to target individuals in the United States.

Establishing a Standard of Acceptable Behavior

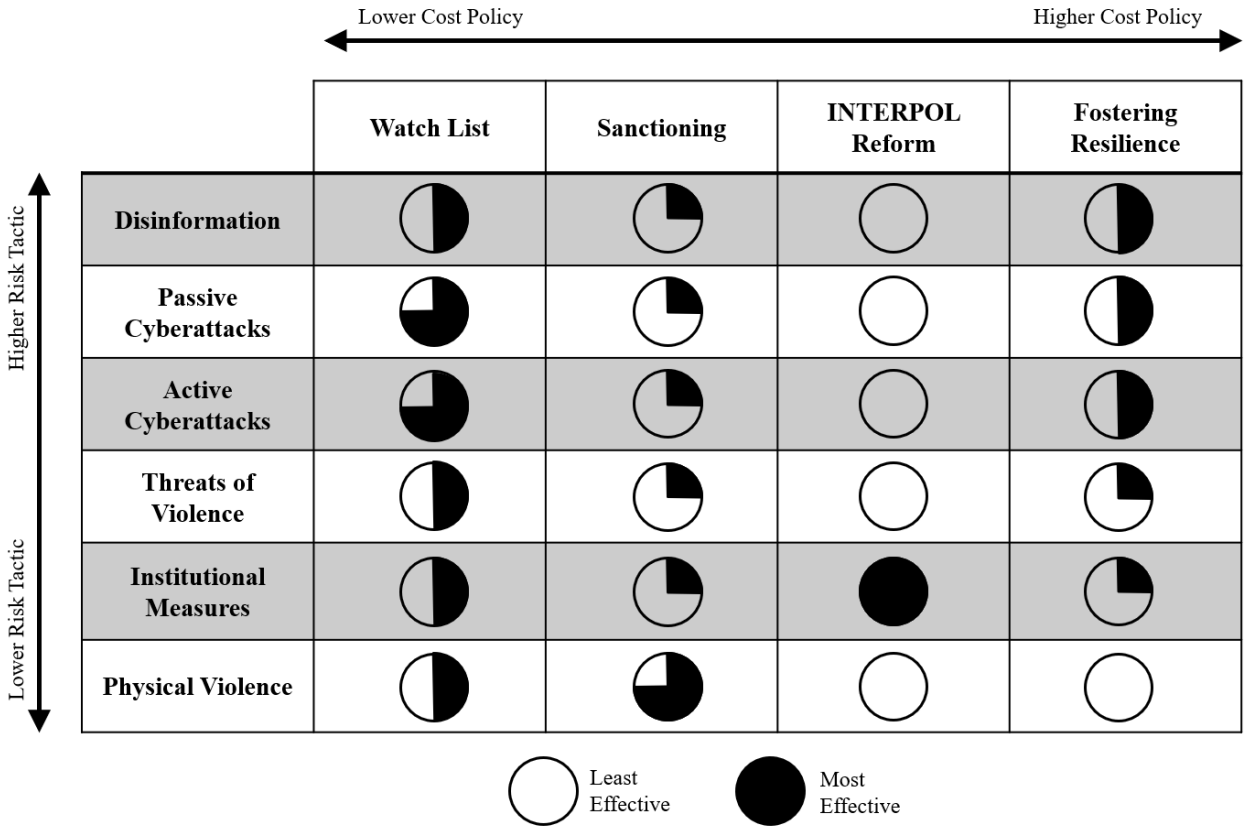
The U.S. government's overarching response should be to establish standards of behavior. Washington, in collaboration with multilateral organizations, can create an ethical framework[99] that outlines the acceptable treatment of emigrants. Currently, part of the problem is the lack of norms and laws governing transnational repression. The phenomenon is treated as if it only damages civic spaces, despite the threat it poses to sovereignty and security. The U.S. government, the international community, and civil society should change the reputational consequences of transnational repression practices. The United States should clearly signal that the perpetrators of transnational repression within its borders will face consequences.

Domestic and international laws and norms can provide the basis for this standard. Legislation, such as the TRAP Act of 2019, the Uyghur Human Rights Policy Act of 2019, and the UIGHUR Act of 2019, can help establish clear codes of conduct, as well as the consequences for violation.[100] Non-governmental organizations (NGOs) and diaspora organizations should support the introduction of additional bills to protect targeted diasporas.[101]

Although international norms in cyberspace are weak, there are rules that can be invoked following serious cyberattacks, such as NATO's Article 5.[102] Similar multilateral rules should be created to explicitly cover the systematic targeting of individuals. Social media platforms should contribute to developing behavioral standards in cyberspace by removing inauthentic content. Detection and removal efforts can dovetail with programs to address extremist content and disinformation, led by the Global Engagement Center at the Department of State.[103]

Efforts to set a standard of acceptable behavior will be complicated by the phenomenon's transnational nature, the failure of governments and publics to view it as systematic and perpetrated by states, and the 'gray area' between acceptable and unacceptable behaviors. Below are specific recommendations to establish and police a standard of behavior and protect victims.

Figure 3: Effectiveness of Policy by Tactic



- *Develop a comprehensive watch list of victims and perpetrators*. NGOs should collaborate to develop a watch list of victims and perpetrators.[104] The Department of State, NGOs, and individual victims should report incidents of transnational repression to a central program, ideally led by Freedom House. The list of victims should be confidential and used to alert targets. NGOs and the Department of State should publicize the index of perpetrators and the U.S. government should consider the index in aid, diplomacy, and trade policymaking decisions via mechanisms such as those discussed below under *Sanctioning*. The State Department can support the maintenance of a watch list through information sharing, e.g. reporting INTERPOL abuse. The watch list would combat underreporting of high-risk tactics. While these tactics are by nature difficult to attribute, a centralized reporting system could improve rates of attribution.

    - *Protect victims*. Protecting victims decreases the likelihood of success of transnational repression tactics, especially cyber-tactics. Some scholars and human rights organizations currently report incidents of transnational repression as part of other programs;[105] some (such as Human Rights Watch) also alert political dissidents who have been hacked or may be targeted.[106] Other organizations (such as Citizen Lab) share information with at-risk groups about how to improve cybersecurity.[107] Notification and educational resources can help cyberattack targets take prompt preventative measures, such as changing passwords, switching

phones, and not sharing confidential information via devices that may be under surveillance. The NGOs working in this space should collaborate through Freedom House to create a more comprehensive list of targets and provide cyberattack targets with educational resources to protect themselves and their information.

- *Label and punish perpetrators*. A publicized ranking of states' propensity to engage in transnational repression raises the cost of transnational repression by creating reputational consequences. This index is a low-cost, efficient way to draw attention to the phenomenon. The index will create negative press, helping to establish and police norms against transnational repression. The U.S. government and international community can subsequently consider states' rankings in aid, diplomacy, and trade policy decisions.

  Negative publicity should help deter future acts of transnational repression by signaling that perpetrators will face reputational costs. Khashoggi's murder, for instance, shocked global audiences and caused business elites to boycott the Saudi Public Investment Fund's 'Davos in the Desert' summit.[108] Most cases, however, remain out of the public eye, or at least out of Western media outlets.[109]

- *Sanction individuals*. Washington should drastically raise the cost of transnational repression tactics for perpetrators through economic, diplomatic, and judicial means. The U.S. Department of the Treasury, Department of State, and judicial system can use existing—thus relatively low-cost—measures to sanction individuals who plan and conduct acts of violent transnational repression, as determined by the watch list.

  In accordance with the Global Magnitsky Human Rights Accountability Act, the Secretary of the Treasury (in consultation with the Secretary of State and the Attorney General) may impose financial sanctions, while the Secretary of State imposes visa restrictions.[110] The Department of State may designate individuals and immediate family as ineligible for entry into the United States under Section 7031(c) of the FY 2019 Department of State, Foreign Operations, and Related Programs Appropriations Act.[111] While these measures currently apply only to the most severe forms of transnational repression,[112] Congress or the president may expand the definition of gross human rights abuses.[113] When U.S. criminal law applies, courts may investigate and prosecute cases of transnational repression.[114]

- *Improve INTERPOL rules and processes*. The United States can decrease the likelihood of success of INTERPOL-based institutional measures, at least within its borders. While institutional measures are a medium-risk tactic, there are efficient ways to reduce this threat. Even without additional funding, INTERPOL abuse can be drastically curtailed.

  The bipartisan Transnational Repression Accountability and Prevention (TRAP) Act of 2019 sets standards for the use of INTERPOL alerts in U.S. legal proceedings.[115] It limits the use of notices in U.S. officials' decision making and requires special approval for notices from countries with records of abuse. It also requires the State Department to report abuses of the alert system and calls for the use of U.S. diplomatic power to help victims of abuse.[116] Increasing funding to INTERPOL, specifically to the Commission for the Control

of INTERPOL's Files (CCF) and the Notices and Diffusions Task Force, will help the organization improve its review process.[117] INTERPOL itself should continue to reform by punishing abusers of its system, for example by suspending the membership of violators or barring them from leadership positions.[118]

- *Foster resilience in emigrant communities*. Resilience against these attacks decreases the likelihood of their success, especially for less severe tactics.[119] Mechanisms that encourage political and civic engagement build resilient societies.[120] Targets who claim they will "not be silenced" are those most passionate about activist commitments and community ties, such as Abdujelil Emet,[121] Omar Abdulaziz,[122] and Enes Kanter.[123] Youth groups, diaspora associations, independent foreign-language media, and other NGOs can increase the engagement of emigrant communities in host states with grants from the Department of Homeland Security.

Conclusion

As transnational repression becomes increasingly commonplace, yet goes largely unchallenged, non-democratic states are perfecting capabilities to exercise force across borders. Co-ethnic and co-national civil society leaders are the current victims of this trend, soon to be joined by a range of economic, social, political, and security actors. Transnational repression capabilities can—and will—be used against individuals outside emigrant communities. The U.S. government should be most concerned about technology-based tactics, which are difficult to attribute and easily transferable to non-co-ethnic and non-co-national targets.

Current U.S. policy does not comprehensively address the toolkit of transnational repression. Washington, U.S. civil society, and multilateral institutions should seek to establish and uphold a standard of acceptable behavior regarding transnational repression. The core of this effort should be a watch list of victims and perpetrators, organized by NGOs and supported by the Department of State. The watch list would warn and help protect targets. When tied to reputational consequences, aid, diplomatic relations, and trade, it would impose costs on perpetrators and deter future acts of transnational repression. The United States should lead the endeavor to curtail the use of extraterritorial repression, lest broad sectors of U.S. society become vulnerable to harassment and manipulation by foreign powers.

Acknowledgements

I want to thank the PIPS community of fellows, interns, former fellows, Professor Amy Oakes, and Professor Dennis Smith for their advice and support throughout this process—especially Zoha Siddiqui for her extensive research, editorial, and logistical assistance. I thank COL Brad Duplessis, USA and an anonymous reviewer for their help from the beginning of this project to the very end. I greatly appreciate the comments from Major General Mark Matthews, USAF (Ret.); Elsa Kania; Clint Watts; and Mike Pregent that helped shape this project. I thank the U.S. Army Mad Scientist Team and the Joint Forces Staff College (JFSC) for opportunities to share my research. I also thank Mitchell Romano for stepping in whenever help was needed.

Appendix A. Risk Assessment Tool

The risk ratings displayed in Figure 2 are determined using the following risk assessment tool, which produces a risk rating for each risk category and an overall risk rating based on a weighted sum of the five risk categories. A higher number indicates a greater degree of risk to the United States and other liberal democratic host states.

Risk Category Rating	Overall Risk Rating
0: Low risk	0-6: Low risk
1: Medium risk	7-13: Medium risk
2: High risk	14-20: High risk

Cost

A. Can this tactic be carried out purely over the internet? (0-no, 1-yes)
B. Does this tactic usually require formal use of government bureaucracy and/or intelligence services? (1-no, 0-yes)

Immunity to Distance

A. Does the cost of this tactic increase as distance from the target increases? (1-no, 0-yes)
B. Does the effectiveness of this tactic decrease as distance from the target increases? (1-no, 0-yes)
    - Does the tactic rely on travel through or physical presence near the kin state?
    - Does the tactic rely on the credibility of a threat that is decreased by the distance of the target and/or proxies from the kin state?

Ease of Attribution

A. How difficult is it to attribute this kind of attack? (0-2, 2-most difficult)

Likelihood of Success

A. Does this tactic, on average, succeed in imposing financial, social, psychological, or physical costs on the target? (0-no, 1-yes)
B. Does this tactic, on average, succeed in changing the target's behavior that the perpetrator intended to stop or alter? (0-no, 1-yes)

Transferability

A. Can this tactic be used on non-co-ethnic/non-co-national targets? (0-no, 1-yes)
B. Does using the tactic on a non-co-ethnic/non-co-national target decrease effectiveness? (1-no, 0-yes)
    - Does the tactic rely on relational ties (proxies) in the kin state?
    - Does the tactic rely on legal privileges granted by the kin state?

Overall Risk Rating

Overall Risk Rating = 1(Cost) + 1(Immunity to distance) + 2(Ease of attribution) + 3(Likelihood of success) + 3(Transferability)

- *Cost* and *immunity to distance* receive the lowest weights because, given states' significant resources, neither costs nor distance are likely to be prohibitive to a state determined to target a political dissident using one of these tactics.

- *Ease of attribution* receives a higher weight because non-attribution, or at least plausible deniability, is valuable to states considering one of these tactics. However, the possibility of attribution has not prevented states from repressing dissidents in the past.

- *Likelihood of success* and transferability to non-co-ethnic/non-co-national targets are weighted highest. Likelihood of success plays the most important role in determining whether a state will use a transnational repression tactic, because the fundamental purpose of these tactics is to impose costs and alter behavior.

- *Transferability* is weighted highest alongside likelihood of success. Transferability to non-co-ethnic and non-co-national targets should be key to host states' assessment of the threat posed by each tactic because, as the foregoing analysis demonstrates, transferability allows a tactic to be used against a broad range of strategic actors.

Appendix B. Risk Rating Calculations by Tactic

T.R. Tactic	Cost		Immunity to Distance		Ease of Attribution	Likelihood of Success		Transfer-ability		Overall Risk Rating (Weighted)
Disinformation	1	1	1	1	2	1	0	1	1	17
Passive Cyberattacks	1	1	1	1	2	1	0	1	1	17
Active Cyberattacks	1	1	1	1	2	1	0	1	1	17
Institutional Measures	1	0	1	0	0	1	1	1	0	11
Threats of Violence	1	0	1	0	1	1	1	1	0	13
Physical Violence	0	0	0	1	0	1	1	1	0	10

[1] Emanuela Dalmasso, Adele Del Sordi, Marlies Glasius, Nicole Hirt, Marcus Michaelsen, Abdulkader S. Mohammad, and Dana Moss, "Intervention: Extraterritorial Authoritarian Power," *Political Geography* 64 (2018): 95-104, https://doi.org/10.1016/j.polgeo.2017.07.003.

[2] This paper uses the term *transnational repression* to mean a specific type of transnational authoritarianism that aims to silence dissent through coercion. Transnational authoritarianism, as described by Glasius (2017) in "Extraterritorial Authoritarian Practices: A Framework" (187), includes practices of repression, legitimation, and cooptation. Repression, or coercion, is one of Gerschewski's three pillars of authoritarian stability and is closely intertwined with the other pillars, legitimation and cooptation (Gerschewski 2013, as cited in Dalmasso et al., "Intervention: Extraterritorial Authoritarian Power," 100). The strategies discussed in the typology are used by non-democratic states attempting to stabilize their rule primarily (but not exclusively) through repression. The definition of transnational repression is based on Gerasimos Tsourapas, "A Tightening Grip Abroad: Authoritarian Regimes Target Their Emigrant and Diaspora Communities," *The Online Journal of the Migration Policy Institute*, August 22, 2019, https://www.migrationpolicy.org/article/authoritarian-regimes-target-their-emigrant-and-diaspora-communities.

[3] Kin states are states that can make a historical or cultural claim to represent dispersed ethnic groups. Fiona B. Adamson, "Non-State Authoritarianism and Diaspora Politics," *Global Networks* 20, no. 1 (January 2020): 150-169, https://doi.org/10.1111/glob.12246, 1; Charles King and Neil J. Melvin, "Diaspora Politics: Ethnic Linkages, Foreign Policy, and Security in Eurasia," *International Security* 24, no. 3 (Winter 1999-2000): 108-138, www.jstor.org/stable/2539307.

[4] Marlies Glasius, "Extraterritorial Authoritarian Practices: A Framework," *Globalizations* 15, no. 2 (December 2017): https://doi.org/10.1080/14747731.2017.1403781, 187.

[5] This paper uses the Polity IV scale ranging from -10 to 10. Polity scores convert to regime categories as follows: autocracies (-10 to -6), anocracies (-5 to 5), and democracies (6 to 10). For more information on *Freedom in the World*'s ratings and status characteristics, consult the methodology. "Freedom in the World 2019 Map," *Freedom House*, 2019, https://freedomhouse.org/report/freedom-world/freedom-world-2019/map; "Political Regime, 2015," *Our World in Data*, 2015, https://ourworldindata.org/grapher/political-regime-updated2016?time=1816..2015; "Methodology 2019: Introduction," *Freedom House*, 2019, https://freedomhouse.org/report/methodology-freedom-world-2019.

[6] Tsourapas, "A Tightening Grip Abroad."

[7] "Freedom in the World 2019 Map," *Freedom House*; "Political Regime, 2015," *Our World in Data*.

[8] Glasius, "Extraterritorial Authoritarian Practices," 183.

[9] Adamson, "Non-State Authoritarianism," 6.

[10] Glasius, "Extraterritorial Authoritarian Practices," 195. For instance, the United States has been complicit in the repression practices of other countries, such as the Philippines and Bangladesh. U.S. authorities assisted authorities in the Philippines and Bangladesh in improving social media monitoring capacity, despite these authorities' poor human rights records. Note: The Philippines does not meet this paper's definition of a non-democracy due to its score of 8 on the Polity IV scale, but it is classified as partly free by the Freedom in the World 2019 Report. Allie Funk and Adrian Shahbaz, "Social Media Surveillance," *Freedom House*, 2019, https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance?fbclid=IwAR2BobNRoWyQ2ODdXLiFttAsp4kLnYxV3fpv8ycWvWuJTkoWESlNheuzkFQ.

[11] Nate Schenkkan, "Global Purge: Understanding and Responding to Transnational Repression," testimony before the *Commission on Security and Cooperation in Europe*, September 12, 2019, https://www.csce.gov/sites/helsinkicommission.house.gov/files/SCHENKKAN%20Nate%20-%20Testimony.pdf.

[12] Threatening emigrants' connections in the kin state appears to be the most effective tactic for changing behavior: it forces targets to relinquish either voice or ties to friends and family, which in many cases enable voice. Glasius, "Extraterritorial Authoritarian Practices," 190.

[13] Dana M. Moss, "Transnational Repression, Diaspora Mobilization, and the Case of The Arab Spring," *Social Problems* 63, no. 4 (November 2016): 480-498, https://doi.org/10.1093/socpro/spw019, 480.

[14] Moss' study of Syrian activists in the United States and Great Britain and Michaelsen's study of exiled Iranian activists found that newcomers to protest were more likely to be deterred than experienced activists. Ibid., 480-498; Marcus Michaelsen, "Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State," *Globalizations* 15, no. 2 (December 2016): 248-264, https://doi.org/10.1080/14747731.2016.1263078.

[15] A Chinese-American who stopped sharing political articles on WeChat and created a new account because he was blocked from using the chat function stated, "this censorship has just affected me psychologically and my behavior." Emily Feng, "China Intercepts WeChat Texts From U.S. And Abroad, Researchers Say," *NPR*, *All Things*

Considered, August 29, 2019, https://www.npr.org/2019/08/29/751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says.
[16] Tsourapas, "A Tightening Grip Abroad."
[17] "Freedom in the World 2019," *Freedom House*, 2019, https://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf, 6.
[18] Dalmasso et al., "Intervention: Extraterritorial Authoritarian Power."
[19] INTERPOL issued 1,277 Red Notices in 2002, compared to 13,048 in 2017. While some of the increase in diffusions and Red Notices may be due to foreign fighters traveling to Syria and Iraq, experts say a significant part of the increase is attributable to the misuse of alerts by non-democracies. Edward Lemon, "Weaponizing Interpol," *Journal of Democracy* 30, no. 2 (April 2019): 15-29, https://muse.jhu.edu/article/721640/pdf, 20.
[20] The collapse of the Soviet Union also contributed to the growing phenomenon of transnational repression—as new states emerged whose nations stretched past the newly established state boundaries—and as emigrants left the former Soviet states for new destinations. King and Melvin, "Diaspora Politics," 138.
[21] Hirschman's work on exit, voice, and loyalty (1970, 1978, 1993) and O'Donnell's extension of this framework (1986) inform the modest body of extraterritorial authoritarianism literature. Glasius, "Extraterritorial Authoritarian Practices," 185.
[22] Tsourapas, "A Tightening Grip Abroad."
[23] Tsourapas' illiberal paradox framework builds on James F. Hollifield's liberal paradox. Ibid.
[24] Michaelsen, "Exit and Voice," 251.
[25] Dalmasso et al., "Intervention: Extraterritorial Authoritarian Power," 98; Gerasimos Tsourapas, "The Peculiar Practices of 'Authoritarian Emigration States'," *British Academy Review*, no. 32 (Spring 2018): 22-24, https://www.thebritishacademy.ac.uk/sites/default/files/BritishAcademyReview32-Spring2018.pdf.
[26] Dalmasso et al., "Intervention: Extraterritorial Authoritarian Power," 95.
[27] Mexico does not meet the definition of a democracy used in this paper because it is classified as partly free by the Freedom in the World 2019 Report.
[28] Dalmasso et al., "Intervention: Extraterritorial Authoritarian Power," 96; Michaelsen, "Exit and Voice," 249.
[29] Dalmasso et al., "Intervention: Extraterritorial Authoritarian Power," 96.
[30] "Authoritarianism and mobility," *Authoritarianism in a Global Age*, University of Amsterdam, accessed February 3, 2020, http://www.authoritarianism-global.uva.nl/about/beyond-exit-and-voice-authoritarianism-and-mobility/.
[31] Tsourapas, "A Tightening Grip Abroad."
[32] Michaelsen, "Exit and Voice," 261.
[33] Gerasimos Tsourapas, "The Long Arm of the Arab State," *Ethnic and Racial Studies* 43, no. 2 (2020): 351-370, https://doi.org/10.1080/01419870.2019.1585558.
[34] Glasius, "Extraterritorial Authoritarian Practices," 181.
[35] Ibid., 181.
[36] Tsourapas, "The Peculiar Practices."
[37] Glasius, "Extraterritorial Authoritarian Practices," 181.
[38] Ibid., 181.
[39] Dalmasso et al., "Intervention: Extraterritorial Authoritarian Power," 96.
[40] Michaelsen, "Exit and Voice," 248.
[41] Ibid., 248.
[42] Ibid., 252.
[43] Ibid., 248.
[44] Funk and Shahbaz, "Social Media Surveillance," *Freedom House*.
[45] Lindsey Gorman, "A Silicon Curtain is Descending: Technological Perils of the Next 30 Years," *German Marshall Fund of the United States*, September 12, 2019, http://www.gmfus.org/publications/silicon-curtain-descending-technological-perils-next-30-years?fbclid=IwAR3ItMaA_MmDcCUEe3XJx7nLm1DdXByyoQZ3UVTozwrlBHp3e2UW3rcGSO0.
[46] Funk and Shahbaz, "Social Media Surveillance," *Freedom House*.
[47] For 1.5 to 2.5 million dollars, the Chinese firm Semptian will monitor the online behavior of a population of five million. Ibid.
[48] Shain (1989), as cited in Michaelsen, "Exit and Voice," 252.
[49] Ibid., 255.
[50] John Scott-Railton and Katie Kleemola, "London Calling: Two-Factor Authentication Phishing From Iran," *the Citizen Lab*, August 27, 2015, https://citizenlab.ca/2015/08/iran_two_factor_phishing/.
[51] Dalmasso et al., "Intervention: Extraterritorial Authoritarian Power," 96.

[52] Ibid., 98.
[53] Severity is defined as the level of costs (financial, social, psychological, and physical) imposed on the target. Lethal violence is the most *severe* form of transnational repression. Within the framework of this paper, severity and risk (calculated with the Risk Assessment Tool) are different measures of the threat posed by various tactics.
[54] Elise Thomas, Tom Uren, and Jake Wallis, "Tweeting through the Great Firewall," *Australian Strategic Policy Institute*, September 3, 2019, https://www.aspi.org.au/report/tweeting-through-great-firewall.
[55] Robert McMillan and Rajesh Roy, "Indian Activists Targeted in Alleged WhatsApp Attack Demand Answers," *Wall Street Journal*, November 2, 2019, https://www.wsj.com/articles/alleged-spy-attack-via-whatsapp-sparks-concern-in-india-11572640154?fbclid=IwAR0BRc0oYoZD7JZcYRrBapP9wtpNgqhDd4C11UtmTxz13swOL8tB0vrd9Lc.
[56] Abusers of the software included the governments of Saudi Arabia, the United Arab Emirates, Mexico, India, and Panama. "NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases," *the Citizen Lab*, October 29, 2019, https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/?fbclid=IwAR0kTRuQAPiujouYCb6FdprAf_6oZDuyHQBwj75Hp5UOrMqcbv9AujLJFzE%22; Ron Deibert, Yahya Assiri, Shubhranshu Choudhary, and Silkie Carlo, "Pegasus: Surveilling Journalists From Inside Their Phones," *Al Jazeera* video, December 1, 2019, https://www.aljazeera.com/programmes/listeningpost/2019/11/pegasus-surveilling-journalists-phones-191130124609237.html?fbclid=IwAR3jOExzW1X-9E3LEqt-j_UsWJI4XVi9q6N7umO7J7oR-JRcNnjRTr0GGHU; Bill Marczak, John Scott-Railton, and Ron Deibert, "NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident," *the Citizen Lab*, July 31, 2018, https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/.
[57] "NSO Group / Q Cyber Technologies," *the Citizen Lab*; Deibert, et al., "Pegasus: Surveilling Journalists," *Al Jazeera*.
[58] "NSO Group / Q Cyber Technologies," *the Citizen Lab*.
[59] Ronen Bergman and Declan Walsh, "Egypt Is Using Apps to Track and Target Its Citizens, Report Says," *New York Times*, October 3, 2019, https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html.
[60] Zoe Schiffer, "WeChat Keeps Banning Chinese Americans for Talking About Hong Kong," *The Verge*, November 25, 2019, https://www.theverge.com/2019/11/25/20976964/chinese-americans-censorship-wechat-hong-kong-elections-tiktok?fbclid=IwAR3STesfTG3dL8VbjIj4STBFhKRgawCiPpK1pj2YQ7WLGOcFNBuW2dTILYI.
[61] Michaelsen, "Exit and Voice," 256-257.
[62] Gulf states, especially Bahrain, Kuwait, Oman, Qatar, and the United Arab Emirates, regularly revoke dissidents' citizenship. Glasius, "Extraterritorial Authoritarian Practices," 188.
[63] Theodore R. Bromund, Tom Firestone, Sandra A. Grossman, Thomas K. Ragland, and Roger Wicker, "Assessing the Potential of the TRAP Act to Prevent Interpol Abuse," *The Heritage Foundation*, October 29, 2019, https://www.heritage.org/crime-and-justice/event/assessing-the-potential-the-trap-act-prevent-interpol-abuse?fbclid=IwAR3nZ6jpwT2_1CdYGkW-8ddJqaSkAhy-79Nj7vo7LGpUU37ZRXJopk6CJAM.
[64] "'Tools of Transnational Repression – How Autocrats Punish Dissent Overseas': Briefing Note to the Commission," *Fair Trials*, September 12, 2019, https://www.csce.gov/sites/helsinkicommission.house.gov/files/MIN%20Bruno%20-%20Testimony.pdf.
[65] Masood Farivar, "How Authoritarian Governments Are Exploiting Interpol to Harass Political Enemies," *Voice of America News*, October 3, 2019, https://www.voanews.com/usa/how-authoritarian-governments-are-exploiting-interpol-harass-political-enemies; Bromund et al., "Assessing the Potential of the TRAP Act," *The Heritage Foundation*.
[66] Bromund et al., "Assessing the Potential of the TRAP Act," *The Heritage Foundation*.
[67] Lemon, "Weaponizing Interpol"; Bromund et al., "Assessing the Potential of the TRAP Act," *The Heritage Foundation*.
[68] Sandra A. Grossman, "How Abusive Red Notices Affect People in the U.S. Immigration System and Steps That Can Be Taken Within the U.S. and at INTERPOL to Protect Victims," testimony before the *Commission on Security and Cooperation in Europe*, September 12, 2019, https://www.csce.gov/sites/helsinkicommission.house.gov/files/GROSSMAN%20Sandra%20-%20Testimony.pdf.
[69] The Turkish government's harassment has imposed costs on Kanter but has thus far not stifled his protest. Enes Kanter, "I Will Not Be Silenced Over Turkey," *Boston Globe*, October 10, 2019, https://www.bostonglobe.com/opinion/2019/10/10/enes-kanter-will-not-silenced-over-turkey/J8RsHZo2qlu7zzOw6OcYSJ/story.html; Chris Forsberg, "Why Enes Kanter's Safety is in Danger Traveling

Outside the United States," *NBC Sports Boston*, December 24, 2019, https://www.nbcsports.com/boston/celtics/why-enes-kanters-safety-danger-traveling-outside-united-states.
[70] Benjamin Haas, "'Think of Your Family': China Threatens European Citizens Over Xinjiang Protests," *The Guardian*, October 16, 2019, https://www.theguardian.com/world/2019/oct/17/think-of-your-family-china-threatens-european-citizens-over-xinjiang-protests; Michael Barbaro, Jessica Cheung, Rachel Quester, Lisa Tobin, and Lisa Chow, "Is China Really Freeing Uighurs?," *The Daily*, August 15, 2019, https://www.nytimes.com/2019/08/15/podcasts/the-daily/china-xinjiang-uighur-detention.html; "Gulbahar Haitiwaji," *Xinjiang Victims Database*, August 25, 2019, https://shahit.biz/eng/#view.
[71] Moss, "Transnational Repression, Diaspora Mobilization," 482.
[72] Tsourapas, "The Peculiar Practices."
[73] Bellingcat Investigation Team, "Identifying The Berlin Bicycle Assassin: From Moscow to Berlin (Part 1)," *Bellingcat*, December 3, 2019, https://www.bellingcat.com/news/uk-and-europe/2019/12/03/identifying-the-berlin-bicycle-assassin-part-1-from-moscow-to-berlin/.
[74] Vikram Dodd, Luka Harding, and Ewen MacAskill, "Sergei Skripal: Former Russian Spy Poisoned With Nerve Agent, Say Police," *The Guardian*, March 8, 2018, https://www.theguardian.com/uk-news/2018/mar/07/russian-spy-police-appeal-for-witnesses-as-cobra-meeting-takes-place.
[75] Funk and Shahbaz, "Social Media Surveillance," *Freedom House*.
[76] Julian Borger, "Jamal Khashoggi: US Spy Chief Given Deadline to Name Saudi Writer's Killers," *The Guardian*, December 13, 2019, https://www.theguardian.com/world/2019/dec/12/jamal-khashoggi-congress-dni-mohammed-bin-salman.
[77] "Repression Across Borders: The CCP's Illegal Harassment and Coercion of Uyghur Americans," *Uyghur Human Rights Project*, August 28, 2019, https://uhrp.org/press-release/new-uyghur-human-rights-project-uhrp-report-details-how-chinese-government-engaged?fbclid=IwAR3ieH0-qJHSuFLgoI640kLySNa2-sUOMmpV95454LgJFnNdNcD-O6-MFYw.
[78] "Two Men Charged in Alleged Plot to Assassinate Saudi Arabian Ambassador to the United States," *The United States Department of Justice, Office of Public Affairs*, October 11, 2011, https://www.justice.gov/opa/pr/two-men-charged-alleged-plot-assassinate-saudi-arabian-ambassador-united-states.
[79] "Repression Across Borders," *Uyghur Human Rights Project*.
[80] Dalmasso et al., "Intervention: Extraterritorial Authoritarian Power," 95.
[81] After Daryl Morey, general manager of the Houston Rockets basketball team, tweeted in support of the Hong Kong protestors, he faced backlash from Chinese state and social media. The team's management considered firing him and pushed players to post positively about China. The NBA issued an apology. James Palmer, "The NBA Is China's Willing Tool," *Foreign Policy*, October 7, 2019, https://foreignpolicy.com/2019/10/07/us-businesses-like-the-nba-are-chinas-willing-tools/.
[82] Tsourapas, "The Peculiar Practices."
[83] Ibid.
[84] Tsourapas, "A Tightening Grip Abroad."
[85] Bradley Hanlon, "Are Journalists Ready for Foreign Interference in 2020?," *Alliance for Securing Democracy*, November 7, 2019, https://securingdemocracy.gmfus.org/are-journalists-ready-for-foreign-interference-in-2020/?fbclid=IwAR1QjfQ3OsJR4trhorJv-2nn0d6j4Jh-KW9wa3gUNkkBxxeN4k0z9L9TKKA.
[86] Joseph V. Micallef, "Russian Harassment of NATO Personnel, Families: The Next Chapter in Information Warfare?" *Military.com*, September 3, 2019, https://www.military.com/daily-news/2019/09/03/russian-harassment-nato-personnel-families-next-chapter-information-warfare.html.
[87] Bill Gardner, "'We Are Watching You': Russia Accused of Sending Threatening Texts to British Troops," *The Telegraph*, October 15, 2019, https://www.telegraph.co.uk/news/2019/10/15/watching-russia-accused-sending-threatening-texts-british-troops/.
[88] Christopher Woody, "The US and NATO Are Preparing for Russia to Go After Troops Both in the Field and at Home," *Task & Purpose*, December 16, 2019, https://taskandpurpose.com/us-nato-russian-disinformation-europe?fbclid=IwAR2uSYZsezvJvDj5sF19LQHkYkkc9VeQDuHrJWSwq0XAORIREDfqOLP8UpU.
[89] According to Keir Giles, a senior consulting fellow at Chatham House's Russia and Eurasia Program. Micallef, "Russian Harassment of NATO Personnel," *Military.com*.
[90] Ibid.
[91] Tsourapas, "The Peculiar Practices."
[92] Alexander Cooley, "The International Dimensions of the New Transnational Repression," written testimony before the *Commission on Security and Cooperation in Europe*, September 12, 2019, https://www.csce.gov/sites/helsinkicommission.house.gov/files/COOLEY%20Alex%20-%20Testimony.pdf, 3.

[93] Ibid., 1-7.
[94] Daniel Calingaert, "Exporting Repression," *Freedom House*, March 26, 2013, https://freedomhouse.org/blog/exporting-repression; Alexander Cooley and John Heathershaw, *Dictators without Borders: Power and Money in Central Asia* (New Haven, CT: Yale University Press, 2017), 193-94.
[95] Calingaert, "Exporting Repression," *Freedom House*.
[96] Additionally, Chinese transnational soft power strategies of legitimation or cooptation (two other forms of transnational authoritarianism) are similar to Egyptian and Cuban practices. See endnote 2. Tsourapas, "The Peculiar Practices."
[97] Ibid., 24.
[98] For the calculation of these risk ratings, see Appendix B. For the risk assessment tool used to derive these ratings, see Appendix A.
[99] Chris Meserole and Alina Polyakova, "Exporting Digital Authoritarianism: The Russian and Chinese Models," *The Brookings Institution*, August 17, 2019, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.
[100] "Repression Across Borders," *Uyghur Human Rights Project*.
[101] Schenkkan, "Global Purge."
[102] Jill Aitoro, "In Cyber, the US Can't 'Enforce Standards That Don't Exist,'" *Fifth Domain*, December 7, 2019, https://www.fifthdomain.com/smr/reagan-defense-forum/2019/12/07/in-cyber-the-us-cant-enforce-standards-that-dont-exist/?fbclid=IwAR1yvbMpQI5dTpZcE6o__v9iH1q_DNqubAPkQvhFmVbxqIkLlSTlE-s7Sq4.
[103] Expanding detection and removal efforts will be challenging, but past successes in the field of countering violent extremism suggest that they are possible. The differing stances on political advertising taken by companies (e.g. Twitter and Facebook) show that these platforms have control over the content they allow. While social media platforms have the capacity to remove content, they are unlikely to do so without incentives (such as tax breaks) or threats of government regulation. Marie-Helen Maras, "Social Media Platforms: Targeting the 'Found Space' of Terrorists," *Journal of Internet Law* 21, no. 2 (August 2017): 3-9, 7.
[104] This initiative may be modeled after indices such as the Nuclear Threat Initiative's "Nuclear Security Index" and "Global Health Security Index." The publicly accessible watch list of perpetrators should include visuals of the overall rankings, a breakdown of each state's rankings, and an explanation of how the rankings were developed.
[105] Freedom House, Citizen Lab, and Human Rights Watch report some incidents of transnational repression as part of other programs. They do not report comprehensively on incidents, gather the information in a single location, or necessarily label the incidents as transnational repression. In late 2020, however, Freedom House is slated to release a study of transnational repression around the world since 2014. Cooley and Heathershaw constructed the Central Asian Political Exiles (CAPE) database, which describes the pursuit of exiles by Central Asian states. As of 2016, it included 163 individuals who had been subject to extraterritorial repression, although the scholars recognize that the database is far from exhaustive. Cooley and Heathershaw, *Dictators without Borders*, 188.
[106] Bergman and Walsh, "Egypt Is Using Apps to Track," *New York Times*.
[107] "Net Alert," *the Citizen Lab*, accessed February 3, 2020, https://citizenlab.ca/category/research/tools-resources/net-alert/; "Security Planner," *the Citizen Lab*, last updated February 20, 2020, https://securityplanner.org/#/.
[108] Patricia Sabga, "Khashoggi to Aramco Attacks: Saudi 'Vision 2030' Clouded by Risks," *Al Jazeera*, October 1, 2019, https://www.aljazeera.com/ajimpact/khashoggi-aramco-attacks-saudi-vision-2030-clouded-risks-191001024541062.html.
[109] Tsourapas, "A Tightening Grip Abroad."
[110] "FAQ: Global Magnitsky Sanctions," *U.S. Department of the Treasury*, December 21, 2017, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/12212017_glomag_faqs.pdf.
[111] "Report to Congress on Anti-Kleptocracy and Human Rights Visa Restrictions," *Bureau of International Narcotics and Law Enforcement Affairs, U.S. Department of State*, December 10, 2018, https://www.state.gov/report-to-congress-on-anti-kleptocracy-and-human-rights-visa-restrictions/.
[112] See endnote 53.
[113] "S.284 – Global Magnitsky Human Rights Accountability Act," *Congress.gov*, January 28, 2015, https://congress.gov/bill/114th-congress/senate-bill/284/text; "7031c – Transmittal Letter," *U.S. Department of State*, accessed February 27, 2020, https://www.state.gov/7031c-transmittal-letter/.
[114] Schenkkan, "Global Purge."
[115] In September 2019, Helsinki Commission Chairman Rep. Alcee Hastings and Ranking Member Rep. Joe Wilson introduced the TRAP Act in the House of Representatives and Helsinki Commission Co-Chairman Sen. Roger Wicker and Ranking Member Sen. Ben Cardin introduced the Act in the Senate. As of February 2020, the TRAP

Act had not passed in either house of Congress. "Helsinki Commission Leaders Introduce Transnational Repression Accountability and Prevention (TRAP) Act," *Commission on Security and Cooperation in Europe*, September 12, 2019, https://www.csce.gov/international-impact/press-and-media/press-releases/helsinki-commission-leaders-introduce; "H.R.4330 – TRAP Act of 2019," *Congress.gov*, accessed March 5, 2020, https://www.congress.gov/bill/116th-congress/house-bill/4330.

[116] Bromund et al., "Assessing the Potential of the TRAP Act," *The Heritage Foundation*.

[117] "'Tools of Transnational Repression," *Fair Trials*.

[118] Grossman, "How Abusive Red Notices Affect People."

[119] See endnote 53.

[120] Allison D. Miller, "Community Cohesion and Countering Violent Extremism: Interfaith Activism and Policing Methods in Metro Detroit," *Journal for Deradicalization*, no. 15 (Summer 2018): 197-232, http://journals.sfu.ca/jd/index.php/jd/article/view/153/122; Rohan Gunaratna, Jolene Jerard, and Salim Mohamed Nasir, *Countering Extremism: Building Social Resilience Through Community Engagement* (London: Imperial College Press, 2013), 1-18.

[121] Abdujelil Emet is a Uyghur living in Germany, who stated that he would increase his activism against the Chinese government if the threat to his family were carried out. Haas, "Think of Your Family," *The Guardian*.

[122] Omar Abdulaziz published an article titled, "Saudi spies hacked my phone and tried to stop my activism. I won't stop fighting." Omar Abdulaziz, "Saudi Spies Hacked My Phone and Tried to Stop My Activism. I Won't Stop Fighting," *The Washington Post*, November 14, 2019, https://www.washingtonpost.com/opinions/2019/11/14/saudi-spies-hacked-my-phone-tried-stop-my-activism-i-wont-stop-fighting/?fbclid=IwAR3LRmy2vjSES-3mRwYOHbDULw2VAHZ2fO0jG69_XqIOKX_NuRs593QV6IY.

[123] Enes Kanter published a piece titled "I will not be silenced over Turkey" in response to harassment by Turkish officials. Kanter, "I Will Not Be Silenced," *Boston Globe*.