P | I | P | S

Transnational Repression

The Long Arm of Authoritarianism

PIPS White Paper 12.1: *Executive Summary*

Katherine Armstrong, Research Fellow
Zoha Siddiqui, Research Intern

Non-democratic regimes—such as China, Iran, Russia, and Saudi Arabia—increasingly use the internet to track, hack, blackmail, and harass emigrants across borders, a phenomenon known as transnational repression (TR). The use of transnational repression against co-ethnics and co-nationals threatens U.S. citizens, democracy, and sovereignty. It also is a harbinger of future attacks against U.S. government officials, members of the national security community, and key players in civil society.

To counter this emerging threat, the United States should: (1) develop a comprehensive TR watch list of perpetrators and victims; (2) sanction perpetrators using existing laws; and (3) work to reform the International Criminal Police Organization (INTERPOL) rules and processes to lessen the likelihood that they can be used as tools of transnational repression.

The Phenomenon of Transnational Repression

Transnational repression 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. Due to the proliferation and improvement of communications and transportation technology, transnational repression has become more common. The tools of repression also have shifted to exploit technological changes. States now have the ability to reach electronically across borders to threaten and punish political dissidents.

The Toolkit of Transnational Repression

Digital media and social networks allow emigrant populations to communicate with friends and family in kin states, creating a political vulnerability for these states. Non-democratic states, however, use these same information and communication technologies (ICTs) to develop new and enhance existing tools of repression. ICTs allow states to monitor quickly, cheaply, and anonymously emigrants' activity on a large scale.

This paper classifies tactics of transnational repression as high, medium, or low risk. Risk refers to the likelihood that a tactic will be used and proliferate. Risk ratings are determined by each

tactic's cost, immunity to distance, ease of attribution, likelihood of success, and transferability to non-co-ethnic/non-co-national targets. High and medium-risk tactics should be of greatest concern to U.S. policymakers.

- *High-risk tactics*. Disinformation, passive cyberattacks, and active cyberattacks are all high-risk tactics because they are affordable, easy to use over large distances, difficult to attribute, and transferable to non-co-ethnic targets. Disinformation uses false or misleading information to damage a victim's reputation, disorient, or frighten. Passive cyberattacks involve remote surveillance of the target. Active cyberattacks include posting via a victim's social media accounts, commandeering a victim's accounts, censorship, and distributed denial-of-service attacks.

- *Medium-risk tactics.* Institutional measures, threats of violence, and physical violence are medium-risk tactics. Non-democracies routinely use laws and institutions, such as INTERPOL, to silence journalists, businesspeople, and political opponents they consider threats. INTERPOL allows states to issue alerts for an individual's arrest and extradition. 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. Governments increasingly threaten physical violence against victims or their relatives using phone calls or online messages.

Conceptualizing Transnational Repression as a Security Threat

Transnational repression threatens democracy, violates national sovereignty, jeopardizes U.S. partnerships with other countries, and compromises homeland security. Furthermore, the United States should expect to see an expansion of TR tactics to non-co-ethnics and non-co-nationals, including security actors, such as politicians, members of the intelligence community, and military servicemembers. Russia, Iran, and Saudi Arabia currently conduct disinformation, passive cyberattacks, and active cyberattacks against non-co-ethnic journalists. Russia similarly uses online social media to harass NATO troops in Eastern Europe.

Recommended Policy Actions

To protect victims of transnational repression, the United States should propose an ethical framework that conveys the acceptable behavior of sending states regarding their emigrants. To enforce this ethical framework, the United States should monitor victims and perpetrators of transnational repression, sanction perpetrators, and reduce the ability of non-democratic states to use multilateral institutions for repressive purposes.

- *Develop a comprehensive watch list of victims and perpetrators.* Non-governmental organizations (NGOs), the Department of State, and individual victims should report incidents of transnational repression to Freedom House, which is currently documenting past incidents. A centralized reporting system would improve rates of attribution for TR attacks and streamline the processes for protecting current and potential targets through

cybersecurity education. The negative press created by the watch list would punish and deter perpetrators—as would tying states' rankings to aid, diplomacy, and trade.

- *Sanction individuals*. In accordance with the Global Magnitsky Human Rights Accountability Act, the Secretary of the Treasury and Secretary of State may impose financial sanctions and visa restrictions, respectively, on perpetrators of violent transnational repression. The Department of State can 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. While these measures apply only to the most severe forms of transnational repression, Congress or the president may expand the definition to cover other TR tactics.

- *Improve INTERPOL rules and processes.* The review practice used by INTERPOL needs reform. Setting standards for the use of INTERPOL alerts within the United States and increasing funding to the Commission for the Control of INTERPOL's Files (CCF) and the Notices and Diffusions Task Force are necessary steps.

Conclusion

Non-democratic states are perfecting capabilities to exercise force over borders, posing a threat to U.S. security actors and civil society. The U.S. government, NGOs, and multilateral institutions should establish a standard of acceptable behavior towards emigrant communities and monitor violations of this standard through a watch list of victims and perpetrators. The watch list would help protect targets and impose costs on perpetrators, thereby deterring future acts of transnational repression.