“Your Family Will Suffer”

How China is Hacking, Surveilling, and Intimidating Uyghurs in Liberal Democracies

UHRP
Uyghur Human Rights Project
ئۇيغۇر كىشىلىك ھوقۇق قۇرۇلۇشى

THE OXUS SOCIETY
FOR CENTRAL ASIAN AFFAIRS

About the Uyghur Human Rights Project

The Uyghur Human Rights Project (UHRP) promotes the rights of the Uyghur people through research-based advocacy. We publish reports and analysis in English and Chinese to defend Uyghurs' civil, political, social, cultural, and economic rights according to international human rights standards.

About the Oxus Society for Central Asian Affairs

The Oxus Society for Central Asian Affairs is a DC-based non-profit organization dedicated to fostering academic exchange between Central Asia and the rest of the world.

Authors

Natalie Hall is a researcher at the Oxus Society for Central Asian Affairs and former program coordinator at the Carnegie Endowment for International Peace.

Bradley Jardine is a global fellow at the Wilson Center's Kissinger Institute on China and the United States and director of research at the Oxus Society for Central Asian Affairs.

Acknowledgements

The authors would like to express their appreciation for the expert review and editing of this report by Dr. Elise Anderson, UHRP Senior Program Officer for Research and Advocacy; Reece Thompson, UHRP Development, Outreach, and Research Officer; and Henryk Szadziewski, UHRP Director of Research. They also extend their sincerest thanks to all the Uyghur diaspora members who offered to share their stories of cross-border repression for this report. Finally, the authors would also like to acknowledge Eliza Campbell for her advice regarding human rights and digital security policy.

Cover Design by YetteSu.

1602 L Street NW | Washington, DC 20036
www.uhrp.org | info@uhrp.org

www.oxussociety.org | info@oxussociety.com

Table of Contents

I. Executive Summary

Since 2002, the People's Republic of China (PRC) has engaged in an unparalleled campaign of transnational repression as part of its efforts to coerce and control Uyghurs living abroad. As a result, members of the Uyghur diaspora have experienced the long reach of China's authoritarian state in the form of relentless harassment, intimidation, and coercion. This campaign of fear expanded dramatically in 2017 as China embarked on a policy course of mass repression and internment in the Uyghur Region.

This report expands on previous work on the China's Transnational Repression of Uyghurs dataset, collected in partnership with the Uyghur Human Rights Project and the Oxus Society for Central Asian Affairs, adding 5,530 instances of stage 1 transnational repression spanning 19 years and 22 countries to the dataset. Cases of intimidation and harassment often go unreported, suggesting that the number of cases and number of Uyghurs facing this harassment may be much higher. The broad reach of China's stage 1 transnational repression of Uyghurs, in tandem with instances of stage 2 and stage 3 repression, shows how the Chinese government has pursued, coerced, and intimidated Uyghurs living abroad, resulting in anxiety, fear, and depression.

We surveyed 72 Uyghurs living in diaspora communities in liberal democracies across North America, the Asia Pacific, and Europe, 95.8 % of whom reported feeling threatened and 73.5% of whom noted that they had experienced digital risks, threats, or other forms of online harassment. Members of Uyghur communities worldwide are interested in protecting themselves, with 89.7% of respondents expressing interest in increasing their security knowledge. However, many respondents did not feel that this protection would necessarily come from their home governments—44.1% felt that their host governments take the intimidation they face seriously, with only 20.5% feeling that the host governments would fix these issues.

Our report analyzes the survey data with a primary focus on how Uyghurs living in the democratic world continue to have their rights—guaranteed to them by democratic governments—violated

by the Chinese government, and how state-aligned actors curtail the freedoms of Uyghurs, and potentially many others, through data collection, surveillance, intimidation, and harassment. China's authoritarianism extends well beyond its borders. The party-state co-opts other countries and their corporations into its campaign of violence and intimidation against Uyghurs; no state or other actor has yet taken responsibility for their protection. Further, our findings suggest that non-Uyghurs are increasingly targeted by this campaign that threatens their freedoms and individual rights. We have also expanded the existing dataset on China's Transnational Repression of Uyghurs by conducting a comprehensive review of open-source news reporting on the intimidation and harassment of Uyghurs living abroad. We further supplement this publicly available data with ten original interviews we conducted with Uyghurs around the world. Together, the information we have gathered and analyzed represents one of the most comprehensive examinations of Uyghur digital insecurity to date.

The response to this global reach must also be global. The Oxus Society and UHRP urge swift action on 13 recommendations to civil society and the private sector, national governments, and inter-governmental bodies, including:

- Governments should **strengthen safe havens** for Uyghur refugee resettlement programs by increasing refugee admissions quotas, streamlining bureaucratic obstacles, streamlining procedures, and providing assistance in mitigating the impacts of digital harassment, including digital hygiene education programs;
- Governments should **increase accountability** by raising the cost to Chinese state agents of engaging in this transnational repression;
- All actors should **incorporate digital rights in action** to protect discussions of human rights privacy and the protection of individuals' identities.
- The private sector should **monitor digital threats** on online platforms in all relevant languages, including Uyghur, Chinese, Turkish, and others, develop tools to identify state-

actor harassment, and make secure communication platforms available in appropriate languages.

II. Introduction

In 2019, Nurgul Sawut, a Uyghur living in Australia, discovered that a botnet had targeted her Facebook account. This swarm of fake accounts, one of which mimicked her own sister's profile, attacked her with a public smear campaign and infected her computer with malware. This malware—software that provides malicious actors with access to and control over a target's electronic devices—has made its way onto Ms. Sawut's phone twice. In one case, she could reset the device; in another, she had to discard her phone altogether. She has since begun to use encrypted email, avoided downloading WeChat onto her phone, and disconnected her Facebook account from any outside apps.

In retribution for her defiance, Ms. Sawut believes Chinese security services arrested and detained members of her family who were living in the Xinjiang Uyghur Autonomous Region (XUAR).[1] Then, in 2021, she learned that she was one of 10,000 people whose names appeared on a Chinese state list of "suspected terrorists," a charge she claims doesn't surprise her based on her activism.[2] However, for many Uyghurs, such a charge comes as a warning—an indication that they are subject to additional Chinese surveillance abroad. Ms. Sawut, like many members of the Uyghur diaspora, has felt the reach of China's coercive practices across sovereign borders.[3]

Today, an estimated 500,000 Uyghurs live in diaspora communities worldwide, with significant population centers in

[1] We refer to this region interchangeably as "the Uyghur Region" and "the XUAR" (short for "Xinjiang Uyghur Autonomous Region"). Uyghurs around the world see "Xinjiang," the shortened form of "Xinjiang Uyghur Autonomous Region" preferred by the authorities in the PRC, as an offensive colonial term. In addition to "Uyghur Region," many Uyghurs also refer to their homeland as "East Turkistan."

[2] Josh Taylor, "I Can't Be That Careless': Australian Uyghur Activist Targeted Online," *Guardian,* May 15, 2021, https://www.theguardian.com/world/2021/ may/16/i-cant-be-that-careless-australian-uyghur-activist-targeted-online.

[3] "Repression across Borders: The CCP's Illegal Harassment and Coercion of Uyghur Americans," Uyghur Human Rights Project, August 28, 2019, https://docs.uhrp.org/pdf/UHRP_RepressionAcrossBorders.pdf.

Central Asia, Turkey, Europe, the Asia Pacific, and North America. Our previous reporting has shown that these communities, particularly in authoritarian settings, are increasingly embattled as China pressures and cooperates with local security services to arrest Uyghurs and demand their deportations.[4] Since 1997, 1,149 Uyghurs living abroad have been detained by their host governments at the request of Chinese security services, while a confirmed 427 Uyghurs have been deported or rendered back to China during that same period, with cases concentrated in Southeast Asia and the Middle East.[5] Together, these individuals represent 1,548 separate cases of transnational repression.[6]

While these forms of repression, which we have classified as stage 2 and stage 3, are occurring primarily in the Muslim world, Western democracies are also under siege with a spike in stage 1 repression—forms of intimidation that have not reached the level of arrest or deportation.[7] Altogether, our data suggest that 7,078 cases of transnational repression of Uyghurs have occurred worldwide. As Uyghurs become more frequent targets for state-backed intimidation, a two-tier model of citizenship is emerging in which a hostile foreign power is undermining the constitutional and political rights of Uyghur citizens in democratic countries. Of concern to policymakers and observers alike is how emerging technologies are accelerating Beijing's capacity for transnational repression, with state actors and their proxies operating with impunity to surveil, harass, and intimidate using malware, botnets, and even tracking devices. Digital technology, in particular, has given the Chinese Communist Party (CCP) new tools to monitor the activities of

As Uyghurs become more frequent targets for state-backed intimidation, a two-tier model of citizenship is emerging in which a hostile foreign power is undermining the constitutional and political rights of Uyghur citizens in democratic countries.

[4] Bradley Jardine, Edward Lemon, and Natalie Hall, "No Space Left to Run: China's Transnational Repression of Uyghurs," Oxus Society for Central Asian Affairs and the Uyghur Human Rights Project, June 24, 2021, https://uhrp.org/report/no-space-left-to-run-chinas-transnational-repression-of-uyghurs/.

[5] Bradley Jardine and Robert Evans, "Nets Cast From the Earth to the Sky: China's Hunt for Pakistan's Uyghurs," Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, August 18, 2021, https://oxussociety.org/nets-cast-from-the-earth-to-the-sky-chinas-hunt-for-pakistans-uyghurs/.

[6] "China's Transnational Repression of Uyghurs Dataset," Oxus Society for Central Asian Affairs, accessed on August 8, 2021, https://oxussociety.org/viz/transnational-repression/.

[7] Bradley Jardine, Edward Lemon, and Natalie Hall, "No Space Left to Run: China's Transnational Repression of Uyghurs," Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, June 24, 2021, https://uhrp.org/report/no-space-left-to-run-chinas-transnational-repression-of-uyghurs/.

diaspora communities and reduce the costs of extraterritorial political control, extending the reach of the Chinese state well beyond its borders.

This report explores the methods and extent to which China and its international proxies are engaged in a systematic campaign of surveillance and harassment of the Uyghur diaspora. Our work focuses primarily, though not exclusively, on democracies, which have long been seen as a haven beyond the reach of the Chinese government. However, as this report reveals, democracies are not the haven against the Chinese government's intimidation and harassment that many observers have thought them to be. China's efforts to control Uyghurs extend far beyond its borders. Its actions infringe on the rights of Uyghurs otherwise guaranteed by their democratic host states, including their rights to freedom of speech, freedom of assembly, and sometimes, even their freedom of travel and movement.[8]

Unlike "counter-exiles" studies, which assess how autocracies repress political activism beyond their borders, our study finds that most targeted Uyghurs were not politically active before they were targeted. Some Uyghurs have remained apolitical after experiencing transnational repression, while others have been galvanized into action by China's intimidation and harassment. For our analysis, we define "politically active" as giving testimony, being actively involved in a human rights organization, or speaking to media or going public—all before an instance of transnational repression. We note people who do not meet these criteria—or who became politically active after the Chinese government harassed or intimidated—as such. Our data indicate that Chinese transnational repression may be one driving factor pushing the Uyghur diaspora toward political activism.

Our data indicate that Chinese transnational repression may be one driving factor pushing the Uyghur diaspora toward political activism.

Mass targeting based on ethnicity and culture has become the norm for Chinese security services. The extensive sweep of this campaign has instilled fear and uncertainty in the broader international Uyghur community, effectively disrupting the

[8] "China upset as Interpol removes wanted alert for exiled Uyghur leader," *Reuters,* February 24, 2018, https://www.reuters.com/article/us-china-xinjiang/china-upset-as-interpol-removes-wanted-alert-for-exiled-uighur-leader-idUSKCN1G80FK.

activities of more vocal and politically engaged individuals as well as those less politically inclined. This report seeks to assess the vulnerability of Uyghur diaspora communities in democratic states and to propose policy options to help mitigate the risks they face so as to guarantee Uyghur citizens and residents the same rights and freedoms as other diaspora communities.

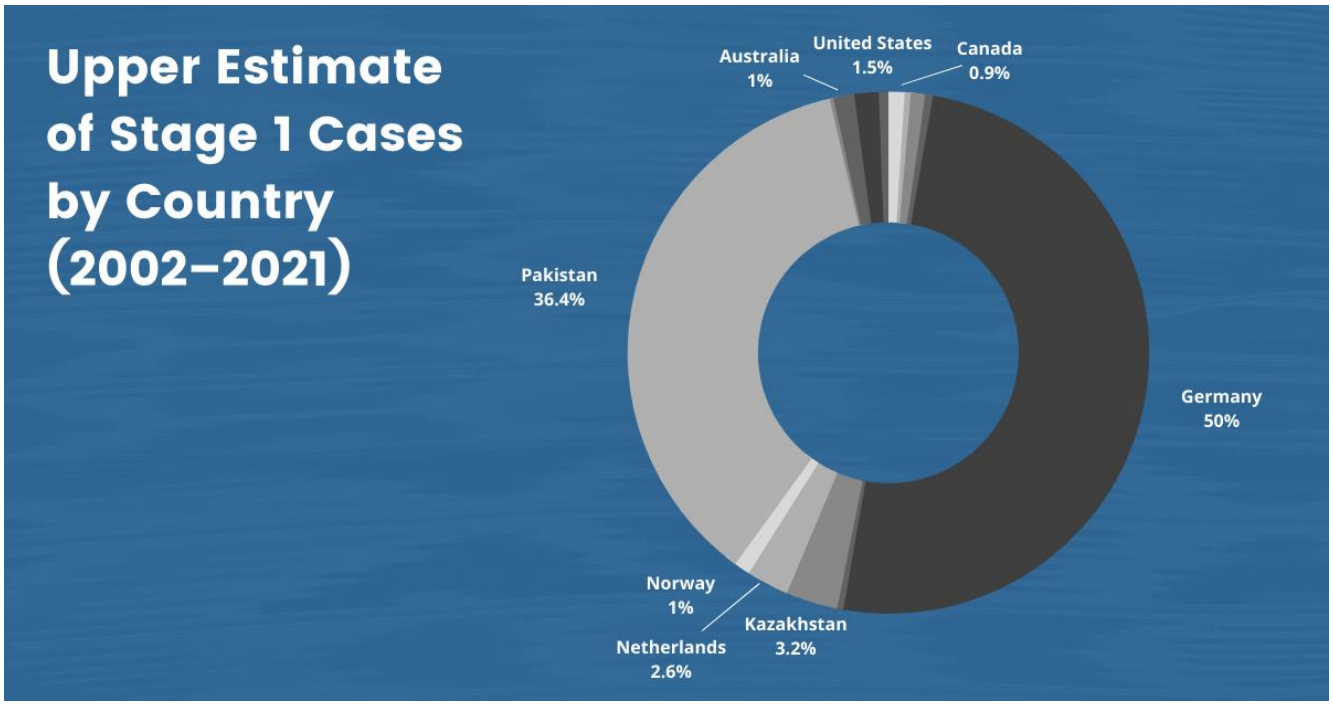

Image 1. This chart shows the geographic distribution of the 5,530 cases of stage 1 transnational repression we recorded based on publicly available reporting and original interviews. It represents all cases collected worldwide 2001–2021. A large number of cases appear in Germany, the location of the World Uyghur Congress. Source: Oxus Society for Central Asian Affairs.

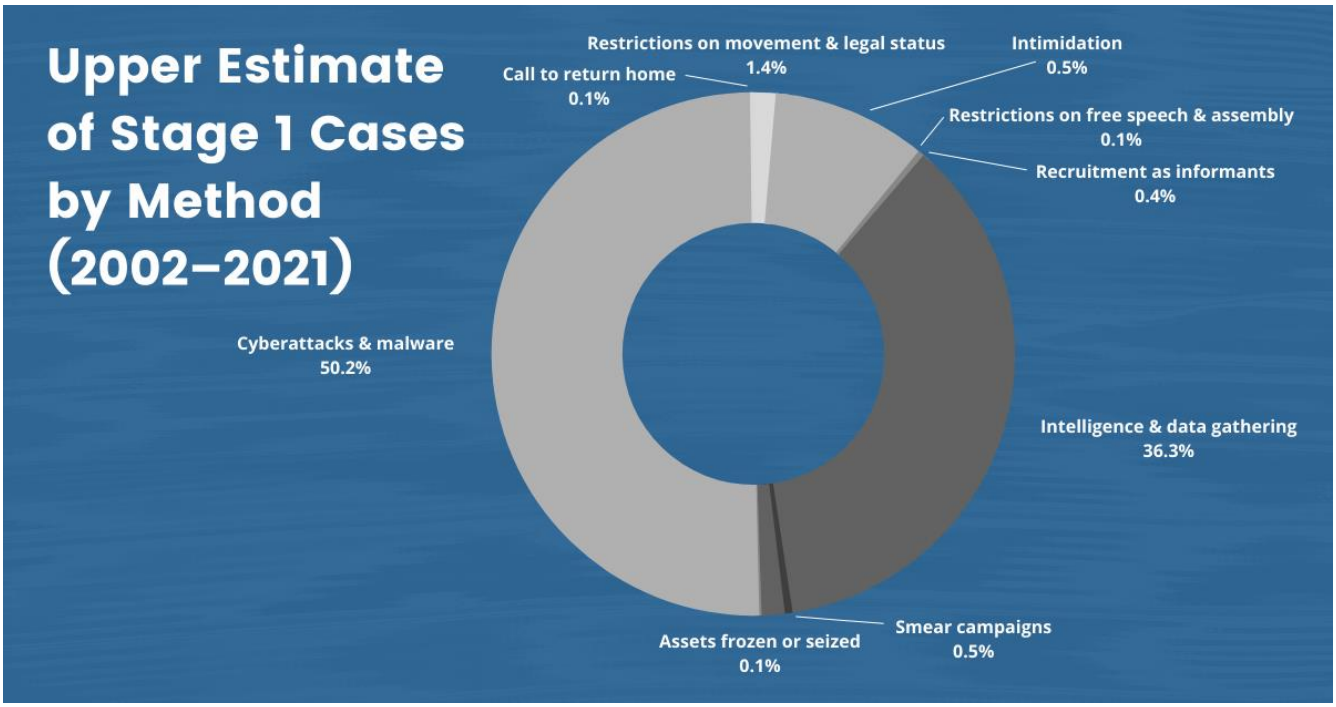

Image 2. This chart shows the methodological distribution of the 5,530 cases of stage 1 transnational repression we recorded. It represents all cases collected worldwide 2001–2021. Just over 50% of all recorded cases are cyberattacks. Source: Oxus Society for Central Asian Affairs.

III. Methodology

China's transnational repression tactics have proven highly effective in causing Uyghurs around the world to self-censor and be more cautious in their approach to anything that may be perceived as political activism. As China's surveillance dragnet expands overseas, it is becoming more difficult to conduct interviews with people willing to identify themselves by name for fear of repercussions and retaliation. In addition, tangible threats to family members back home make public testimony a high-risk endeavor that individuals in the Uyghur diaspora must contemplate before making media statements.

This report builds on the China's Transnational Repression of Uyghurs Dataset created by the authors for the Oxus Society for Central Asian Affairs (Oxus) in collaboration with the Uyghur Human Rights Project (UHRP). The China's Transnational Repression of Uyghurs Dataset contains incidents of transnational repression conducted by the People's Republic of China to target

Uyghur citizens from the XUAR since 1997, when the first cases of detention and rendition were recorded.[9] We use a three-stage model of transnational repression adopted by the Central Asia Political Exiles (CAPE) database in order to evaluate the different cases recorded in our full dataset:

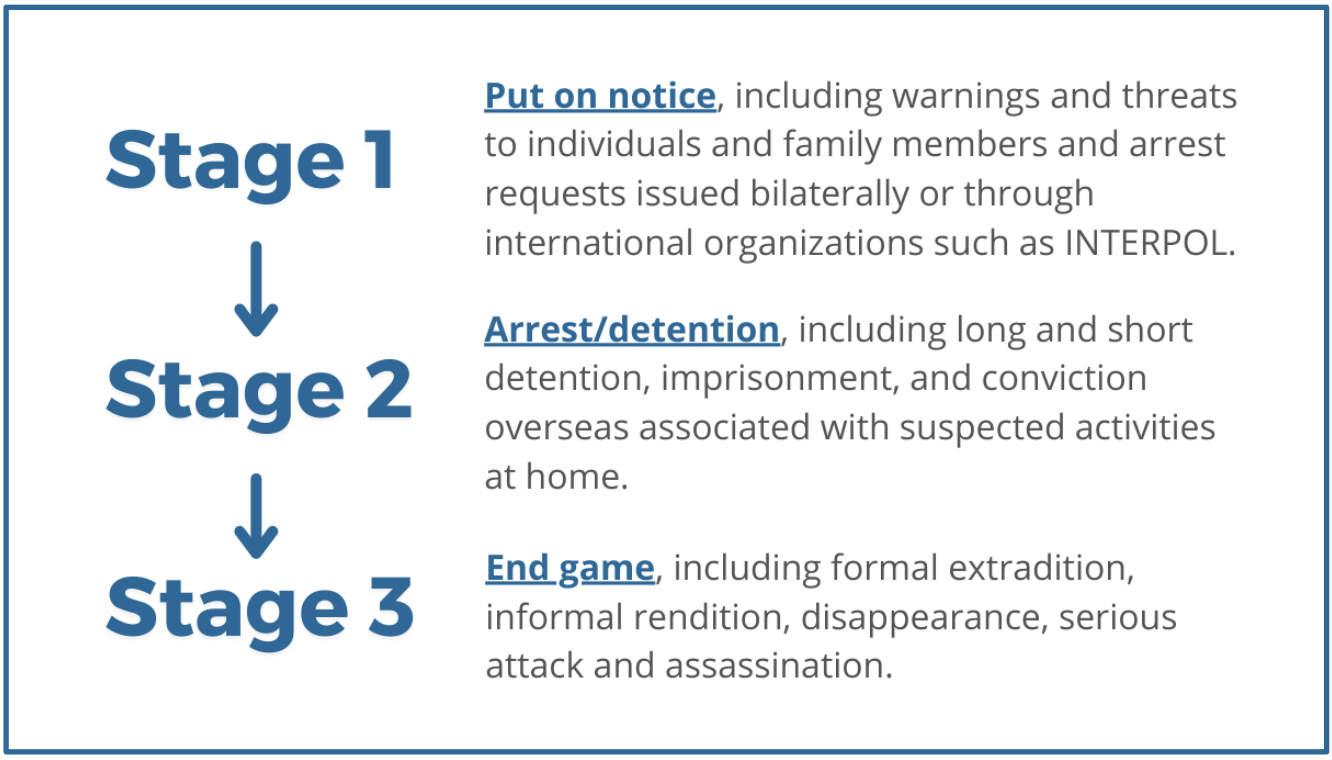

Image 3. CAPE methodology for evaluating transnational repression as outlined by Saipira Furstenberg, John Heathershaw, Edward Lemon, David Lewis, and Alexander Cooley. Source: Central Asia Political Exiles database.

Following CAPE, we measured the degree of transnational repression on a 3-point ordinal scale according to these three stages. We then assigned each case a score between 1 and 3, with 3 representing the most severe form of transnational repression: deportation to China. Our June 2021 report focused on stages 2 and 3 of this ordinal scale,[10] and we found that many individual cases include forms of repression across different stages. Therefore, the

[9] The forms of transnational repression discussed in this report have largely targeted Uyghur former citizens of the XUAR. While we do not believe that only Uyghurs have been the targets of this repression, the cases in our dataset overwhelmingly show that Uyghurs living abroad are a special target of the Chinese state.

[10] Bradley Jardine, Edward Lemon, Natalie Hall, "No Space Left to Run: China's Transnational Repression of Uyghurs," Oxus Society for Central Asian Affairs and Uyghur Human Rights Project, June 24, 2021, https://uhrp.org/report/no-space-left-to-run-chinas-transnational-repression-of-uyghurs/.

current report focuses exclusively on stage 1 to offer a complete record of the ongoing nature of this phenomenon.

We have coded each case according to a particular typology of attack (outlined below). We then logged each instance, separated by time and/or geography, even of a previously targeted individual, separately. For example, in 2019 Mehmet Tohti experienced a variety of harassment and intimidation, including unknown vehicles parked outside his house and people knocking on his door asking for information about his activities, both of which fit into a category of *Intimidation* outlined below.[11] In 2016, Mehmet had called a distant relative who was then detained immediately after the phone call.[12] The time separating these events and different strategies deployed by the Chinese government led us to enter them as two separate instances in the dataset.

We have divided the dataset into two broad categories. The first category consists of Full Entries, which document the cases of individuals with known identities and histories. We have called the second category Anonymous Cases, which refers to individuals or groups of Uyghurs whose names are not publicly available. Anonymous cases may have been part of larger public attacks on Uyghurs where we can only account for the number of affected individuals but cannot independently identify them or add further context beyond the available reporting. Our upper estimate of cases is a combination of Full Entries and Anonymous cases.

The stage 1 data, like the data for stages 2 and 3 from our July 2020 report, represents cases worldwide. However, our analysis in the current report focuses on Europe, the Asia Pacific region, and North America. Traditionally perceived as refugee havens and bulwarks of liberal values on the international stage, these regions have long been thought to be beyond the reach of authoritarianism. However, our findings suggest otherwise: Uyghurs living in these

[11] Rachel Gilmore, "'We're coming to get you': China's critics facing threats, retaliation for activism in Canada," *Global News*, April 2, 2021, https://globalnews.ca/news/7734158/china-pressure-activists-canada-uyghur-hong-kong-tibet-spying/.

[12] Tom Blackwell, "'Don't step out of line': Confidential report reveals how Chinese officials harass activists in Canada," *National Post*, January 5, 2018, https://nationalpost.com/news/world/confidential-report-reveals-how-chinese-officials-harass-activists-in-canada-there-is-a-consistent-pattern/wcm/2de0402f-5d1c-4a0a-b4bb-8dcfd56b3788.

regions of the world remain targets of China's ongoing campaign of intimidation, coercion, and harassment.

We conducted ten interviews with Uyghurs in Washington, D.C., USA; Adelaide, Australia; Toronto, Canada; Tokyo, Japan; Oslo, Norway; and Munich, Germany, to gain more background into the particular situation of Uyghurs residing in key target cities with significant diaspora populations. We also conducted three interviews with cybersecurity experts and engineers working with Uyghur NGOs around the world.

Additionally, we ran two surveys to assess the degree of vulnerability for Uyghur diaspora members regarding cyber-attacks. We sent out our first survey in English to Uyghur diaspora communities in North America. We then translated our second survey into Uyghur to ensure that only those identifying as Uyghurs could respond. We distributed this survey among several Uyghur communities in Japan, Australia, and Europe. While not exhaustive, the data we gathered from these surveys offer critical insight into the vulnerabilities of Uyghur diaspora communities.

IV. Assessing Threat Vulnerability in the Uyghur Diaspora: Survey Results

The threat of targeted surveillance and other intrusions puts activists under pressure to effectively protect their contacts and communications. Not only do activists have to stay up to date with the rapidly evolving methods of attack and deception, but they also make daily security decisions knowing they are up against resourceful state actors. Moreover, the complexity of today's digital tools and platforms further complicates their understanding of the technical underpinnings of the threats they might be facing. As a result, activists often feel uncertain in choosing the right tools and layers of protection.

As a case study of these more significant trends, we requested that members of Uyghur diaspora communities in the United States,

Australia, Europe, and Japan participate in a small survey focused on their digital safety and security practices to assess Uyghur communities' vulnerabilities. Of the 72 people we surveyed:

- 95.8% of respondents felt that they faced unique digital threats; and
- 73.5% of those respondents reported experiencing "digital risks, threats, or forms of surveillance."

Uyghurs in the diaspora have sought to protect themselves in response to these threats:

- 51.5% of respondents felt that they knew where to access internet resources to help them make good security decisions; and
- 73.2% of respondents felt that they could implement new tools and techniques for information security into their lives.

However, respondents felt that the Uyghur community is underprepared with regards to their digital security and hygiene:

- Only 33.8% thought that they knew who to contact when asking for advice from a security expert;
- 50% felt that they had not been sufficiently trained in digital security; and
- 89.7% expressed interest in increasing their security knowledge and skills.

Some governments have made it easier for people living inside their borders to report such incidents. For example, a U.S. Federal Bureau of Investigation counterintelligence bulletin noted that Uyghurs facing harassment could call the FBI tip line and report about what had taken place.[13] However, there is clearly still work to be done:

[13] "Chinese Government Transnational Repression Violates US Laws and US-based Uyghurs' Rights" (counterintelligence bulletin), U.S. Federal Bureau of Investigation, August 11, 2021, https://s.ipvm.com/uploads/embedded_file/07b033ce06e5a7a52f4591f49b3feb19be3a558d132df949f515d3107fa4da87/20bad084-f6b4-4d5f-980a-7e04ca90158c.pdf.

- 41.2% of respondents surveyed felt that they did not know how to report a security incident, while 29.5% felt that they did (the other 29.4% did not reply either way);
- 30.9% do not feel comfortable reporting security issues, even if they are unsure about them, while 39.7% do (an additional 29.4% of respondents did not indicate either way); and
- only 44.1% of respondents felt that their host government or police would take their case seriously, while 20.5% felt that the security problems they faced would be fixed.

Watering hole attack: When attackers make a fake website that looks like a website their target audience might visit but contains malware

Phishing attack: Counterfeit communications (email, message, etc.) that appear to come from a reliable source but can compromise an individual or organization's accounts or personal data (e.g., by coaxing targets into giving an attacker their username and password), give an outsider access to compromise networks or systems, or hold computer networks ransom (i.e., ransomware). Phishing attacks can also be used to download malware onto a target's devices.

Spear phishing attack: A subset of phishing that targets specific individuals rather than a group. Attackers often tailor these emails and messages to their specific targets, using content and linguistic cues to encourage their target to compromise their account, or to click on a link or download a file containing malware.

Chinese hackers are targeting Uyghurs abroad beyond the organizational level. Increasingly, individual Uyghurs, even those who are not politically active, are being attacked worldwide. Critically, the Chinese government has targeted Uyghurs online through social media and cyber campaigns and through malware and backdoors in smartphone software to collect data and spy on them. These efforts are part of an encompassing campaign. Since 2017, China has expanded its surveillance and information collection, both domestically and abroad, in lockstep with the so-called People's War on Terror. Using hackers rather than the more

"traditional" spies and informants reduces the cost of this data collection. Although it is difficult to implicate the Chinese state in such attacks directly, the fact that the attacks target Uyghurs suggests they are at the very least serving government interests.

Targeting the communications of dissidents and human rights groups can put their contacts in China at risk. After a number of Yahoo accounts were hacked in 2010, World Uyghur Congress spokesperson Dilshat Raxit reported that he was unable to reach some of his contacts inside China with whom he had communicated via email in the past. In some cases, private companies double down by failing to inform their customers, as in 2015 when former Microsoft employees revealed that the company had decided not to tell the hackers' targets, many of them Uyghurs, that their email accounts had been compromised.[14]

Starting in 2012, the Chinese government could trigger access to a backdoor in Android operating systems through hidden malware that allowed an outside user to record calls, turn on a phone's microphone, export photos, share phone location, and download conversations on chat apps. Websites commonly used by Uyghurs were corrupted with malware that could siphon data from an iPhone. These efforts, as noted above, would become part of China's dragnet that collects big data on its citizens—both domestically and abroad. In 2015, the Chinese government began seizing the phones of Uyghurs living in the XUAR, only to return them with spyware installed or return an entirely different phone. The unique serial number of each phone was noted and paired with the increasingly ubiquitous cameras and hardware on the streets of the Uyghur Region, ensuring near-constant state surveillance. Uyghurs were arrested and detained for owning more than one phone, not having a phone, disposing of a phone, or having a phone that was "too old."[15]

---

[14] Joseph Menn, "Microsoft failed to warn victims of Chinese email hack: former employees," *Reuters*, December 30, 2015, https://www.reuters.com/article/us-microsoft-china-insight/microsoft-failed-to-warn-victims-of-chinese-email-hack-former-employees-idUSKBN0UE01Z20151231.

[15] Paul Mozur and Nicole Perlroth, "China's Software Stalked Uighurs Earlier and More Widely, Researchers Learn," *New York Times*, January 19, 2021, https://www.nytimes.com/2020/07/01/technology/china-uighurs-hackers-malware-hackers-smartphones.html.

In July 2019, the *Guardian* revealed that Chinese border guards at the Irkeshtam border crossing were downloading spyware onto travelers' phones and taking data from them, including emails, texts, contacts, and information about the smartphones themselves, as well as scanning for banned content, including material on fasting during Ramadan and the Dalai Lama.[16] The Chinese government's efforts to surveil and track people—even foreign travelers—in the XUAR begins at the border, irrespective of nationality. The information they obtain aids police efforts to construct a database of Uyghurs residing beyond China's borders.

These efforts were coupled with four types of surveillance ware distributed via app and news site starting in 2013 with shared command and control (C2) infrastructure as well as root malware, suggesting a shared point of origin. Lookout analysts note that the shared naming conventions, coding techniques, infrastructure, and shared targets among these tools indicate that this surveillance ware is Chinese in origin. For example, DoubleAgent and GoldenEagle were also used to target Tibetans; logging statements of at least one in the family of malware are in Chinese. Furthermore, researchers at the tech firm Lookout were able to peer inside these codes and analyze their IP origins to understand where they had originated: Beijing. This array of surveillance ware was used in hundreds of fake apps tailored to a Uyghur audience. These apps mimicked VPNs and other sites, including Radio Free Asia, and were introduced to sites already frequented by Uyghurs and Tibetans. Analysts have since sorted the malware into four major groups: SilkBean, Double Agent, CarbonSteal, and GoldenEagle. All were designed to collect data from smartphones and exfiltrate it to a single external command and control center. Hackers used these four types of malware to target Uyghur populations in the Uyghur Region as well as in Afghanistan, Egypt, France, Indonesia, Iran, Kazakhstan, Kuwait, Malaysia, Pakistan, Saudi Arabia, Syria, Turkey, and Uzbekistan—countries on the IJOP list.[17]

---

[16] Hilary Osborne and Sam Cutler, "Chinese border guards put secret surveillance app on tourists' phones," *Guardian*, July 2, 2019, https://www.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones.

[17] "Mobile APT Surveillance Campaigns Targeting Uyghurs," *Lookout*, June 2020, https://www.lookout.com/documents/threat-reports/us/lookout-uyghur-malware-tr-us.pdf, 18.

Name of Malware	**Capabilities**
SilkBean	Allowed an external actor to execute over 70 commands remotely once an app was downloaded, often from a third-party Android app store. Two application package names—com.uyghur.hunter.islamapk and com.islamapk.uy—speak to how this malware was used to target Uyghurs explicitly.
DoubleAgent	Copied data unencrypted from a variety of apps, including WhatsApp, Skype, and Telegram. Additionally, DoubleAgent had a direct command and control center overlap with SilkBean.
CarbonSteal	Allowed an external actor to record phone calls and sounds around the infected device, as well as copy SMS and MMS messages, call logs, installed apps, and data about their installation; track location; log when the device was turned on and off; and upload additional apps and capabilities. Analysts believe CarbonSteal is still active and evolving.
GoldenEagle	Allowed an external actor to copy contact information, information about installed apps, caller history, documents found in external storage, and text messages. An external actor could also take screenshots and photos, record calls, record audio in the environment of the phone, track the phone's location, and possibly gain further access to the phone's software, allowing that actor to install further malware.

Table 1: Types of malware used in cyberattacks against Uyghurs. Most have been attributed to users in China. Source: Lookout.

Chinese government-adjacent hackers' use of websites to host and disseminate malware has had other notable cases: in 2019 Lookout uncovered that Chinese hackers had created a site called

Syrian News to target Uyghurs in Syria. They also created similar apps explicitly targeting Uyghurs living in Afghanistan, Kuwait, Indonesia, Malaysia, Pakistan, and Turkey, in an effort to collect data on them. Apps were available in Uyghur, English, Arabic, Chinese, Turkish, Pashto, Farsi, Malay, Indonesian, Uzbek, Urdu, and Hindi.[18]

In 2018, a Chinese group of hackers "discovered" a backdoor hack into the iPhone at the Tianfu Cup in China. This hack, called "Chaos," allowed an iPhone to be taken over remotely after visiting a webpage embedded with malware. In January 2019, Apple offered a fix. However, research into the hack later in 2019 revealed that the backdoor hack—and similar hacks to the Android operating system—had been in use since at least 2018, meaning that the personal iPhones of Uyghurs were vulnerable to government exploitation for more than a year.[19] In August 2019, Google revealed five "exploit chains" for iPhones, one of which replicated Chaos and was initiated by government-adjacent hackers.[20] In September 2019, *Reuters* reported that Chinese government-affiliated hackers had exploited weaknesses in Central and South Asian telecommunications companies in Kazakhstan, Turkey, India, Thailand, and Malaysia. These hackers analyzed the user data and call records they collected to search for "high-value individuals," including Uyghurs abroad. These data points allowed these hackers to gain insight into who Uyghurs living abroad contact and where they are connecting from—potentially dangerous information for both Uyghurs living abroad and their families in the Uyghur Region.[21]

In 2019, cybersecurity firm Volexity discovered 11 compromised websites providing news, resources, and other content in Uyghur.

[18] Mozur and Perlroth, "China's Software Stalked Uighurs Earlier and More Widely."

[19] Ian Beer, "A very deep dive into iOS exploit chains found in the wild," Project Zero (blog), August 29, 2019, https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html; Thomas Brewster, "iPhone Hackers Caught by Google Targeted Android and Microsoft Windows, Say Sources," *Forbes*, September 1, 2019, https://www.forbes.com/sites/thomasbrewster/2019/09/01/iphone-hackers-caught-by-google-also-targeted-android-and-microsoft-windows-say-sources/.

[20] O'Neill, "How China turned a prize-winning iPhone hack against the Uyghurs."

[21] Jack Stubbs, "China hacked Asian telecoms to spy on Uighur travelers: sources," *Reuters,* September 5, 2019, https://www.reuters.com/article/us-china-cyber-uighurs/china-hacked-asian-telcos-to-spy-on-uighur-travelers-sources-idUSKCN1VQ1A5.

All of these websites were behind the Great Firewall, leaving only Uyghurs living abroad to access them. These websites included Uyghur Academy, *Turkistan Times*, *Uighur Times* (in English, Mandarin, and Uyghur), and East Turkistan Education and Solidarity Association, among others. Volexity also revealed that hackers used fake Google applications and plug-ins to steal emails and contact information and that they had created a series of "doppelganger domains" for real websites, including Google.[22]

In May 2021, cybersecurity experts uncovered a plot targeting Uyghurs in Pakistan. The activities involved sending malicious documents by email falsely using the names and logos of the United Nations and United Nations High Commissioner for Refugees. They also set up a fake human rights foundation website called the "Turkic Culture and Heritage Foundation," which tricked people into installing a backdoor to the Windows software running on their computers and gave hackers access to their data.[23] Evidence suggests that Uyghurs living in Pakistan and the Uyghur Region were the primary targets; additional details point to the same operations directed at Uyghurs living in Turkey and Malaysia. According to researchers, these phishing attempts continue as of their reporting.[24]

[22] Andrew Case, Matthew Meltzer, and Stephen Adair, "Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs," *Volexity*, September 2, 2019, https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/.

[23] Shoshanna Solomon, "Israel-Based Cybersecurity Experts Expose Ongoing Hack Attack on Uyghurs," *Times of Israel*, May 27, 2021, https://www.timesofisrael.com/israel-based-cybersecurity-experts-expose-ongoing-hack-attacks-on-uighurs/.

[24] Tim Starks, "Possible Chinese hackers pose as UN, human rights group to eavesdrop on beleaguered Uyghur population," *CyberScoop*, May 27, 2021, https://www.cyberscoop.com/uighur-chinese-hackers-pakistan-check-point-kaspersky/; "Uyghurs, a Turkic ethnic minority in China, targeted via fake foundations," CheckPoint Research, May 27, 2017, https://research.checkpoint.com/2021/uyghurs-a-Turkic-ethnic-minority-in-china-targeted-via-fake-foundations/.

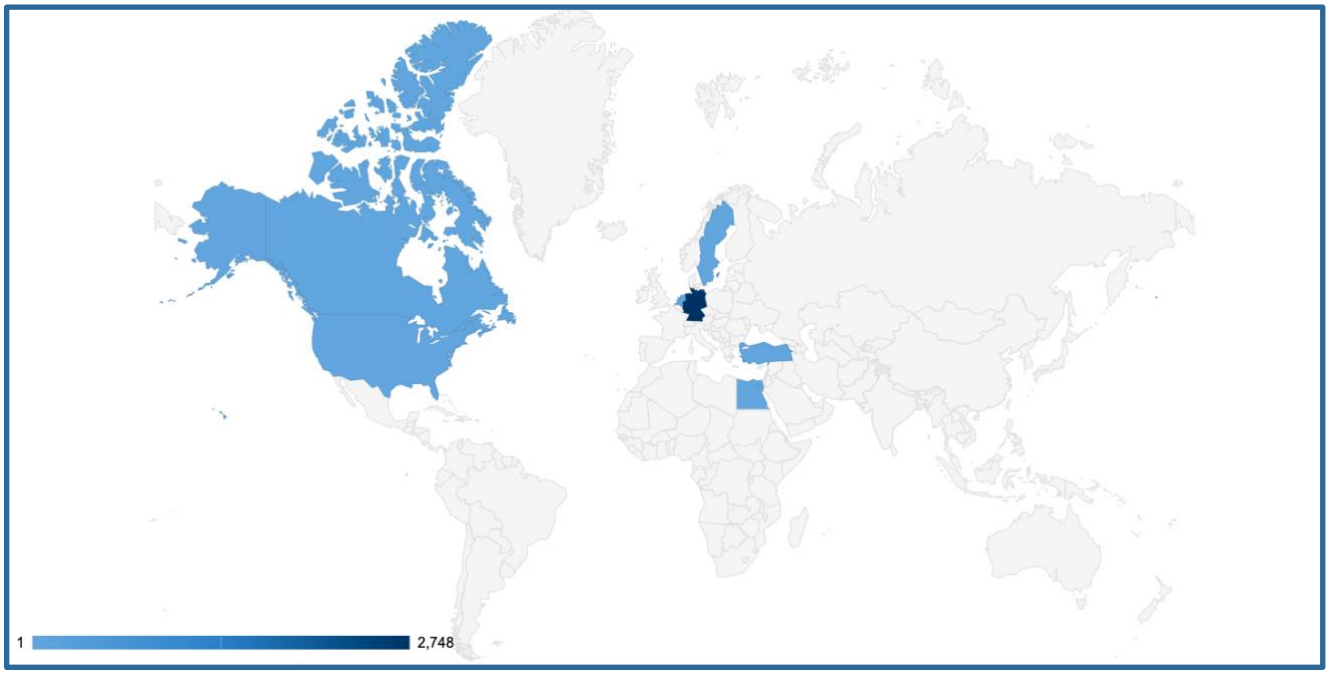

Image 4. Map of cyberattacks on Uyghurs worldwide (2002-2021). This map shows the geographic distribution of the 2,774 cases of cyberattacks in the dataset. Please note that the map does not include the telecoms hacking incidents in Kazakhstan and Pakistan, as there were no detailed numbers of incidents reported in international media. Source: Oxus Society for Central Asian Affairs.

V. Chinese Government Methods of Stage 1 Transnational Repression

China's government has worked to coerce and control Uyghur diaspora communities through a variety of methods. We have identified a total of ten forms of China's stage 1 repression of diaspora Uyghurs:

Typology	Definition
Assets frozen or seized	Instances of an individual or group of individuals whose assets have been seized by the Chinese government either in the Uyghur Region or by a host state acting on behalf of the Chinese government.

Call to return home	Instances of an individual or group of individuals summoned directly by Chinese government representatives or by their family who Chinese government representatives are coercing to demand their return.
Cyberattacks and malware	Instances of an individual or group of individuals targeted online using botnets, malware, spyware, email phishing attempts, DDoS, or other forms of cyberattack.
Intelligence and data gathering	Instances of an individual or group of individuals asked to pass personal information about themselves to the Chinese government.
Intimidation, including active surveillance and threats	Instances of an individual or group of individuals facing repeated contact from Chinese officials in the XUAR or the local embassy/consulate or from family members coerced by Chinese officials via WeChat; having unsolicited packages sent from the Uyghur Region to their home address in their host country; being followed in their host countries by unknown individuals or unmarked vehicles; being photographed at protests; etc.
Recruitment as informants	Instances of individuals being asked to pass information about others to the Chinese government over an extended period.
Restrictions on movement and legal status via passport control	Instances of an individual or group of individuals being given illegal one-way travel documents, instead of having their passports or other government documentation renewed, that restrict their right to free movement or denying passport renewals.[25]

[25] "Weaponized Passports: the Crisis of Uyghur Statelessness," Uyghur Human Rights Project, April 1, 2020, https://uhrp.org/report/weaponized-passports-the-crisis-of-uyghur-statelessness/.

Restrictions on free speech and assembly, including attacks on journalists or public speakers	Instances of an individual or group of individuals subjected to harassment, intimidation, and surveillance such that they are unable to exercise their right to free speech and freedom of assembly.
Smear campaigns	Instances of an individual or group of individuals subjected to Chinese government smear campaigns meant to discredit them as individuals and cast doubt on their claims of human rights violations in the Uyghur Region. These forms of attacks increasingly overlap with state-media production and dissemination of "proof-of-life" videos.[26]
Use of proxies and threats	Instances of an individual's family members, friends, colleagues, or other close associates being threatened with or are arrested or detained in the Uyghur Region.

Table 2: Descriptions of the ten types of attack we have observed across the cases in our dataset. Source: Oxus Society for Central Asian Affairs.

VI. Regional Cases of Transnational Repression

Transnational repression is on the rise globally as a strategy for authoritarian rulers to control the information space and silence external activists.[27] China has emerged as the world's most

[26] "'The Government Never Oppresses Us': Proof-of-Life Videos as Intimidation and a Violation of Uyghur Family Unity," *UHRP*, February 2, 2021, https://uhrp.org/report/the-government-never-oppresses-us-chinas-proof-of-life-videos-as-intimidation-and-a-violation-of-uyghur-family-unity/.

[27] Alex Dukalskis, *Making the World Safe for Dictatorship*, (Oxford: Oxford University Press, 2021), 5.

egregious perpetrator of the practice.[28] According to the combined stage 1, stage 2, and stage 3 data from previous datasets produced by the Oxus Society for Central Asian Affairs and UHRP, the Chinese state and state-adjacent actors have perpetrated at least 7,078 separate instances of transnational repression across 46 separate countries in 6 regions. Democracies are also struggling with transnational repression within their borders, albeit with the less extreme form of repression we have characterized as stage 1. The Chinese government's methods of transnational repression erode legal norms and defy the constitutional rights of many Uyghurs living in liberal democracies, who are guaranteed the right to freedom of speech and the right to peacefully protest. Uyghurs have had those rights repressed by the heavy hand of a foreign power seeking to control and silence them.

Europe

Europe has for over three decades been home to Uyghur diaspora communities and is a sanctuary for Uyghurs fleeing from repression in the XUAR. In March 2021, the EU placed sanctions on CCP officials for the first time since the Tiananmen Square protest in 1989.[29] However, despite these sanctions, only Germany (2018)[30] and Sweden (2019) have made explicit assurances that they will not deport Uyghurs back to China.[31] Further, Sweden has declared Uyghurs to be part of a "persecuted group," a term that makes the

[28] "Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression," Freedom House, January 2021, https://freedomhouse.org/sites/default/files/2021-01/FH_TransnationalRepressionReport2021_rev012521_web.pdf, 15.

[29] Eyck Freymann and Elettra Ardissino, "China and Europe Are Breaking Over Human Rights," *Foreign Policy*, March 29, 2021, https://foreignpolicy.com/2021/03/29/europe-cai-china-human-rights-uyghurs-sanctions/.

[30] In 2018, Germany deported a 23 year-old Uyghur student due to an administrative error. He disappeared in China, and has not been heard from since. After this incident, Germany halted the deportation of Uyghurs to China. For more information. see Adam Taylor, "Germany accidentally deported a Uyghur man to China. His lawyer hasn't heard from him since," *Washington Post*, August 6, 2018, https://www.washingtonpost.com/world/2018/08/06/germany-accidentally-deported-uighur-man-china-his-lawyer-hasnt-heard-him-since/; "Germany halts Uighur deportations to China," *Deutsche Welle*, August 23, 2018, https://www.dw.com/en/germany-halts-uighur-deportations-to-china/a-45190309.

[31] Ellen Halliday, "Uighurs Can't Escape Chinese Repression, Even in Europe," *Atlantic,* August 20, 2019, https://www.theatlantic.com/international/archive/2019/08/china-threatens-uighurs-europe/596347/.

process of claiming asylum status much more straightforward.[32] Germany, one of the most prominent havens for Uyghur refugees fleeing to Europe, reported a two-fold increase in the number of Chinese citizens claiming refugee status in 2020—the most recent peak in an upward trend spanning the last three years.[33] Further details regarding the exact number of Uyghur refugees throughout Europe are unavailable, as governments do not generally disaggregate their immigration data based on ethnicity.

But Uyghurs in Europe still face the long arm of China's ongoing campaign of transnational repression. Many report facing harassment and intimidation, coercion to commit espionage, and social media surveillance campaigns. Our dataset includes 50 cases of Uyghurs who have come forward about their harassment and a higher estimate of 3,040 cases of China's efforts to coerce and silence them across national borders.

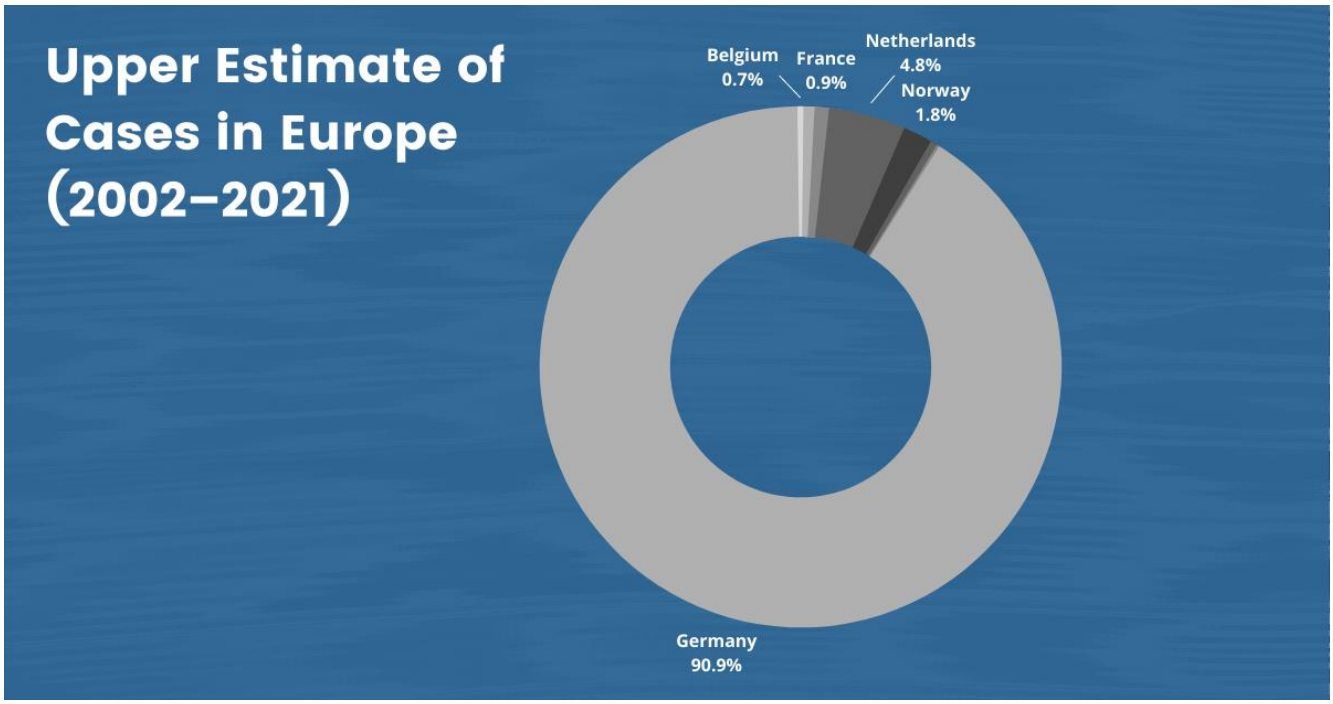

Image 5. This chart shows the geographic distribution of the 3,040 cases of stage 1 transnational repression recorded in Europe. As previously noted, a preponderance of cases occurred in Germany due to continued cyberattacks against the World Uyghur Congress. Source: Oxus Society for Central Asian Affairs.

[32] Anna Hayes, "Sweden Leads the Way on Uyghur Rights," *Fair Observer*, June 16, 2020, https://www.fairobserver.com/region/asia_pacific/anna-hayes-uighur-rights-china-persecution-surveillance-concentration-camps-asylum-news-18221/.

[33] "China Asylum Claims to Germany More Than Double," *Deutsche Welle*, February 16, 2020, https://www.dw.com/en/china-asylum-claims-to-germany-more-than-double/a-52396720.

While Chinese-state intimidation within Europe's borders has increased in recent years, it has occurred since 2007. According to public reporting, Germany's Office for the Protection of the Constitution (BfV) was aware of Chinese efforts to monitor Uyghur activities on German soil starting in that year. For example, a Chinese diplomat in Munich, Ji Wumin, left the country before he could be expelled after people reportedly observed him meeting on numerous occasions with individuals who passed him information about the city's Uyghur community.[34] Later, in 2011, German federal prosecutors also announced espionage charges against a 64-year-old identified only as "L" (in accordance with local privacy laws).[35] Federal prosecutors were pressing similar charges against a Chinese national of Uyghur origin. Prosecutors alleged that the men had passed the information on Munich's Uyghur community to Chinese intelligence between April 2008 and October 2009. Another Uyghur, who chose to remain anonymous at the time of the *Guardian*'s reporting, was asked to take photos of Uyghurs celebrating Eid in Germany, and to hand over the names of any recent arrivals.[36]

Germany has been a prime target for Chinese intimidation, intelligence collection, and cyberattacks abroad due to the size of the Uyghur emigré population there. The country is also home to Uyghur advocacy organizations, including the World Uyghur Congress. The WUC, long associated with now-former President Rebiya Kadeer, has been advocating for the rights and freedoms of those in the Uyghur Region. In response, Beijing has labeled the NGO a "terrorist organization" and has committed acts of transnational repression against the organization's staff for decades.[37]

---

[34] "The Fifth Poison: The Harassment of Uyghurs Overseas," Uyghur Human Rights Project, November 28, 2017, https://uhrp.org/docs/The-Fifth-Poison-The-Harrassment-of-Uyghurs-Overseas.pdf, 11.

[35] "German Man Charged With Spying on Exiles for China," *Associated Press* via *Fox News*, April 8, 2011, https://www.foxnews.com/world/german-man-charged-with-spying-on-exiles-for-china.

[36] Benjamin Haas, "'Think of Your Family': China Threatens European Citizens over Xinjiang Protests," *Guardian*, October 16, 2019, https://www.theguardian.com/world/2019/oct/17/think-of-your-family-china-threatens-european-citizens-over-xinjiang-protests.

[37] "China Smears Former Xinjiang Residents Who Testified About Abuses in the Region," *Radio Free Asia*, April 13, 2021, https://www.rfa.org/english/news/uyghur/smear-04132021191322.html.

In 2009, a case involving a Uyghur in Sweden showed the Chinese Party-state's growing confidence in its ability to build intelligence networks abroad. Naturalized Swedish citizen Barbur Mehsut was arrested on charges relating to "unlawful acquisition and distribution of information relating to individuals for the benefit of a foreign power," for which he had received monetary compensation as well as a visa for his daughter and a job for his wife. He was eventually sentenced to sixteen months' imprisonment. Mehsut had attended meetings of the World Uyghur Congress in the United States in May 2009. He reportedly passed the information on Uyghur activists' activities, health, and finances in Sweden, Norway, Germany, and the United States to Zhou Lulu, a press officer at the Chinese Embassy in Stockholm, and *People's Daily Sweden* correspondent Lei Da. Chinese agents charged Babur Mehsut with gathering information on Adil Hakim,[38] one of the "Guantanamo 22" Uyghurs who had been held as a "non-enemy combatant" at Guantanamo Bay and was applying for asylum in Sweden at the time.[39] Mr. Barbur told police that the Chinese state was concerned that were it to be approved, Mr. Adil's case would set a precedent for more Uyghurs to settle in Sweden as asylum seekers. The Uyghur spy had contacted Hakim and passed details of his case to Chinese authorities, and they even met him at the airport on his arrival from Albania.

As China has escalated its surveillance of Uyghurs in the XUAR and abroad, instances of transnational repression in Europe have been on the rise. Halmurat Harri, a Uyghur activist and Finnish citizen, has said that authorities detained his father in 2018 in response to Mr. Halmurat's protest against his mother's 2017 arrest and his continued activism in Europe. Both of his parents were later released and put under house arrest.[40] Other Uyghurs living in Finland have further reported being surveilled and photographed at protests, information the Chinese government then uses to target

But Uyghurs in Europe still face the long arm of China's ongoing campaign of transnational repression. Many report facing harassment and intimidation, coercion to commit espionage, and social media surveillance campaigns.

[38] His name also appears as "Adil Hakimjan" in some sources.

[39] Ritt Goldstein, "Is China spying on Uighurs abroad?" *Christian Science Monitor,* July 14, 2009, https://www.csmonitor.com/World/Asia-Pacific/2009/0714/p06s12-woap.html.

[40] Xinrou Shu, "Heretic, separatist, traitor: Uyghur Halmurat Harri's Inbetween Life," *Supchina*, April 22, 2021, https://supchina.com/2021/04/22/heretic-separatist-traitor-uyghur-activist-halmurat-harris-in-between-life/.

their relatives at home.[41] France has also seen its Uyghur community targeted and threatened in recent years. Police officers from local stations in the XUAR have been writing to Uyghurs in France over WeChat requesting home, school, work addresses, photos, scans of their ID cards, and those of their spouse, as well as their marriage certificate, if the couple got married in France.[42] Family members back home in the XUAR have also been used as a form of coercion; four such cases occurred in France between 2017 and 2018 alone. In 2019, Gulnahar (pseudonym) and Adili (pseudonym) reported they were contacted by Chinese government officials seeking information about members of the Uyghur diaspora.[43] A year earlier, in 2018, two other French Uyghurs, Mariem (pseudonym) and Nijat (pseudonym), had reported similar instances of harassment.[44]

Since 2019, Netherlands-based activist Abdurehim Gheni has been the regular target of surveillance and intimidation by unknown individuals he believes to be Chinese. He was photographed and threatened during protests in Amsterdam and smeared and discredited by people trying to shout over him. He has also faced harassment and received death threats over the phone. Gheni reported this to the Dutch police, who have taken more proactive steps for his protection by establishing police presence at his protests, and giving him a direct line to contact the police as needed.[45] Uyghurs living in Belgium have reported receiving distressing phone calls from family members and Chinese authorities seeking information about themselves and the Uyghur diaspora community and being followed from protests by a

[41] Halliday, "Uighurs Can't Escape Chinese Repression."

[42] Bethany Allen-Ebrahimian, "Chinese Police are Demanding Personal Information From Uyghurs in France," *Foreign Policy*, March 2, 2018, https://foreignpolicy.com/2018/03/02/chinese-police-are-secretly-demanding-personal-information-from-french-citizens-uighurs-xinjiang/.

[43] Baptiste Fallevoz, Jonathan Walsh, and Georges Yazbeck, "How China Keeps a Close Eye on the Uyghur Diaspora in France," *France 24*, December 16, 2019, https://www.france24.com/en/asia-pacific/20191216-focus-how-china-keeps-a-grip-on-uighur-diaspora-in-france-surveillance-threats.

[44] Joëlle Garrus, "No Place to Hide: Exiled Chinese Uyghurs Feel State's Long Reach," *Agence France-Presse* via Hong Kong Free Press, August 17, 2018, https://hongkongfp.com/2018/08/19/no-place-hide-exiled-chinese-uighur-muslims-feel-states-long-reach/.

[45] "Nowhere Feels Safe," *Amnesty International*, February 21, 2020, updated September 10, 2021, https://www.amnesty.org/en/latest/research/2020/02/china-uyghurs-abroad-living-in-fear/.

consular car with blacked-out windows.[46] Belgian security services have worked to inform Uyghurs of the dangers of following through with the claims made by the local Chinese Embassy concerning the need to pick up documents or packages at the Embassy. However, the Belgian government has not been able to prevent Uyghurs living there from being harassed.

Norway has also seen an increase in fear among its small Uyghur community of 2,500 people. In October 2019, at least 30 Uyghurs in the country alerted Uyghur advocacy groups that they had been receiving automated calls from the Chinese Embassy despite being Norwegian citizens.[47] In an interview with us, Norway-based activist Abduweli Ayup noted that he has been the direct target of China's security services since his 2019 move there from Turkey, saying, "In [January 2020], I received a call over Facebook Messenger warning me to stop discussing the leaked Qaraqash List." He went on: "Later that year, I received another call over Messenger requesting my cell phone number, along with information about the Uyghur community in Bergen, which I refused to provide." The activist told us he has also received death threats.[48]

China's transnational repression in Europe has also targeted municipal and national governments in at least several cases. The German city of Weimar announced in June 2017 that it had awarded its annual human rights prize to imprisoned Uyghur professor Ilham Tohti. The city's web pages for the award were repeatedly attacked following the announcement, and content related to the award was deleted. France has also been a target in China's campaign to control the narrative about the human rights abuses in the Uyghur Region: in February 2019, an academic conference on the XUAR in Strasbourg, France, was interrupted by two individuals, later determined to be Chinese consular officials in

[46] Ellen Halliday, "Uighurs Can't Escape Chinese Repression, Even in Europe," *Atlantic,* August 20, 2019, https://www.theatlantic.com/international/archive/2019/08/china-threatens-uighurs-europe/596347/.

[47] Kiyya Baloch, "Norway: Automated Calls From Chinese Embassy Spook Uyghur Diaspora," *Al Jazeera*, November 14, 2019, https://www.aljazeera.com/features/2019/11/14/norway-automated-calls-from-china-embassy-spook-uighur-diaspora.

[48] Abduweli Ayup (Uyghur diaspora member), online interview by Bradley Jardine, October 5, 2021.

plainclothes. The officials sought to discredit the panelists and disseminate propaganda to spread doubt about the veracity of the claims made.[49]

Abdujelil Emet, a Uyghur activist, World Uyghur Congress volunteer, and imam living in Germany, has faced harassment from Chinese officials first-hand. In 2019, he received a surprise phone call from his sister in the Uyghur Region two days after sitting in on the Bundestag hearing on human rights. Mr. Abdujelil had never given his German phone number to family in the Uyghur Region out of a sense of caution. When he answered his phone, his sister praised the Communist Party and her quality of life in the XUAR. She then shared the news that their brother had died. Throughout the conversation, Abdujelil heard whispers growing in the background. When he demanded to know their source, a Chinese official took the phone and suggested that Abdujelil cease his activism in Germany. The official added that Abdujelil needed to "think of his family" in the XUAR. This was a thinly veiled threat: Abdujelil should cease his activism in Germany lest his family face the consequences. In response, Abdujelil told the officer that should anything happen to his family, he would only become a more vocal advocate for the human rights of Uyghurs, and therefore a more significant problem for the Chinese government.[50]

In June 2021, *Politico Europe* revealed that the Lisbon City Hall had shared the personal information of dissidents and activists with repressive regimes worldwide as part of its "standard operating procedure." To hold a protest, activists and dissidents had to register with the city and hand over their personal information, which was then shared. Since 2011, this practice included sharing Uyghurs' information with the Chinese government that then allowed the Chinese government to go after the families of those who had arranged protests in Lisbon, according to the local branch of Amnesty International. In a country that has long prided itself as a refugee haven, this news throws the substance of that protection into question. Further, it undermines the rights these Uyghurs have to free speech and assembly, as well as to protection from

[49] Halliday, "Uighurs Can't Escape Chinese Repression, Even in Europe."

[50] Haas, "Think of Your Family.'"

intimidation and harassment, as Portuguese and EU refugees and citizens.[51]

Asia Pacific

Australia and New Zealand, like many other liberal democracies, have been destinations for Uyghurs seeking to escape the reach of the Chinese government and its campaign of harassment and intimidation. However, our data reveal that the safe havens offered by Australia and New Zealand are under threat. Our dataset includes 18 confirmed cases of named individuals and an upper estimate of 60 cases of Uyghurs living in Australia and New Zealand who the Chinese government has targeted. Likewise, Japan provides only limited security to Uyghurs living on its soil, some of whom face continued harassment by the Chinese state. Our dataset contains four such named cases and an upper estimate of 21 cases.

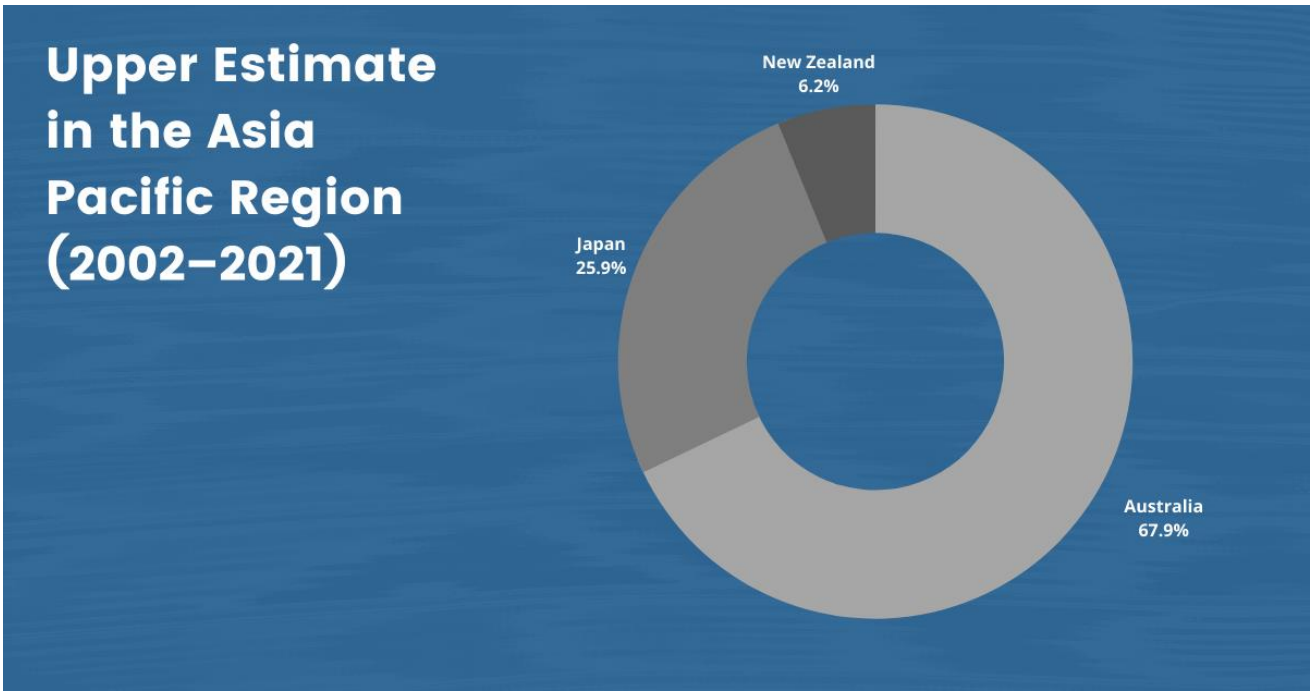

Image 6. This chart shows the geographic distribution of the 81 stage 1 transnational repression cases recorded in the Asia Pacific region. Source: Oxus Society for Central Asian Affairs.

[51] Aitor Hernández-Morales, "Lisbon Has Shared Dissident Info with Repressive Regimes for Years," *Politico*, June 11, 2021 https://www.politico.eu/article/lisbon-portugal-dissidents-personal-data-repressive-regimes/.

Australia is currently home to an estimated 3,000 Uyghurs. The Australian government has expressed concern over the Chinese monitoring of Uyghurs on Australian soil for over a decade. In 2006, the Australian Department of Foreign Affairs and Trade stated: "It is likely that Chinese authorities seek to monitor Uyghur groups in Australia and obtain information on their membership and supporters […]. In pursuing information, Chinese authorities would not necessarily exclude sources who do not have a political profile."[52] Several Uyghurs in the country have spoken with a parliamentary commission about the intimidation and harassment that they have faced, with many citing safety concerns.[53] Community members report forms of pressure such as WeChat calls from their families with government officials present and calls from family members urging them not to become politically active. Uyghurs in Australia also report that they were asked to hand over their information. Some complied to protect their families back home, but after providing initial information, they were asked to provide more.[54]

Chinese state security officials first reached out to Dawud (pseudonym) in September 2017, demanding that he either return or explain why he had not already done so. Dawud sent them proof of employment in Australia, where he had settled with his family, but state security officials emailed back to demand more: they wanted photographs of his life in Australia, including photos of his family and their passports.[55] Eldana Abbas, a Uyghur activist and interpreter living in Australia, reported receiving calls from the Chinese Embassy in Canberra and being photographed by individuals and groups of people during their activities.[56] An Australian Chinese embassy defector named Chen Yonglin claimed

[52]Australia Refugee Review Tribunal - Country Research Section for China, CH31854 China, May 29, 2007, https://www.refworld.org/pdfid/4b6fe1862.pdf, 5.

[53] Daniel Hurst, "Uyghurs Tell Australian Inquiry of 'Intimidation and Harassment' from Chinese Government," *Guardian,* October 8, 2020, https://www.theguardian.com/australia-news/2020/oct/09/uighurs-to-tell-australian-inquiry-of-intimidation-and-harassment-from-chinese-government.

[54] Ibid.

[55] Joshua Boscaini, "Chinese Authorities Accused of Intimidating Uyghurs in Australia," *ABC News* (Australia), March 30 2019, https://www.abc.net.au/news/2019-03-31/chinese-government-accused-of-intimidating-australian-uyghurs/10945090.

[56] "Nowhere Feels Safe," Amnesty International.

in 2005 that the embassy had cultivated 1,000 informants and agents in Australia.[57] Such pressure is still routinely applied.

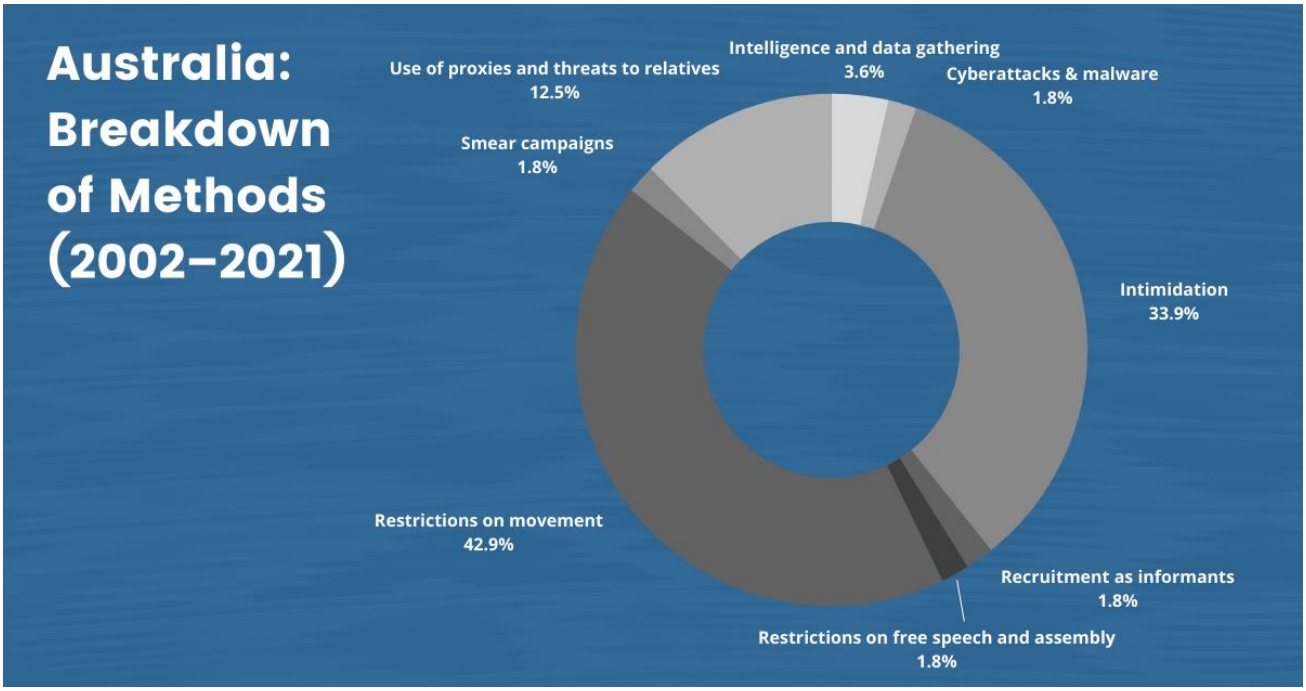

Image 7. This chart shows the methods of stage 1 transnational repression deployed by the Chinese government against Uyghurs living on Australian soil. Source: Oxus Society for Central Asian Affairs.

Uyghurs in New Zealand have also found themselves subject to monitoring from Beijing. Shawdun Abul-Gopur left the XUAR in 2010 for New Zealand, leaving his family behind.[58] Later that year, the Chinese government demanded his return before the calls eventually stopped—but only briefly. Five years later, in 2016, his mother called him, pressing him for information about his life in New Zealand. Mr. Shawdun refused to provide her with any. He then began to receive calls from representatives of the Chinese Embassy, who threatened his family in the Uyghur Region and requested that he come to pick up a package at the Embassy. "We can find you. We are in New Zealand," the caller reminded him.[59]

[57] "Second defector backs spy claims," *CNN*, June 7, 2005, http://www.cnn.com/2005/WORLD/asiapcf/06/07/australia.china.diplomat/; Andrew Greene, "Chinese spies in Australia on the rise, former diplomat Chen Yonglin says," *ABC News* (Australia), November 20, 2016, https://www.abc.net.au/news/2016-11-20/how-many-spies-does-china-have-in-australia/8041004.

[58] Also spelled as "Shawudun Abduguphur" in some sources.

[59] "Migrant receives chilling warning: We can find you. We are in New Zealand,'" *New Zealand Herald*, July 29, 2019, https://www.nzherald.co.nz/nz/migrant-receives-chilling-warning-we-can-find-you-we-are-in-new-zealand/GY4DPLW4EXXA35LRQYLT3YLXAY/.

Due to a subsequent lack of response, he believes his 78-year-old mother and three brothers were detained. They have since been released, but he hasn't been able to contact them since 2016.[60]

As in other parts of the world, a dramatic spike in the targeting of Uyghurs in the Asia Pacific coincided with the start of the mass internment campaign in the Uyghur Region in 2017. In 2018, Halmat Rozi's family members in the XUAR were detained for traveling abroad to visit him in Japan. Mr. Halmat, who had moved to Japan for graduate school and stayed there after graduation, reached out to his family, who told him not to be in touch again. The 47-year-old Uyghur began to attend demonstrations raising awareness of the plight of his and others' families and joined the local Japan Uyghur Association.[61] In May 2020, Halmat received a phone call from his brother and another unidentified individual asking for details about protests, whether Halmat had been in contact with Rebiya Kadeer, and whether Halmat could provide information on the Japan Uyghur Association.[62] His brother encouraged him to cooperate. A few weeks later, he received another call from a member of the state security services again demanding information about protests in Japan. This time Halmat contacted a local TV station, which decided to report his story.[63] To cut off representatives of the state security services, Halmat deleted the app they used to call him, which also cut all contact with his family—a reality that weighs heavily on him.[64] Halmat's story has played a critical role in raising awareness and political visibility of the human rights abuses in the XUAR and the long reach of the Chinese government.

An Australian Chinese embassy defector named Chen Yonglin claimed in 2005 that the embassy had cultivated 1,000 informers among overseas Chinese students. Such pressure is still routinely applied.

[60] Ashley Westerman, "New Zealand condemns China's treatment of Uyghurs but won't call it genocide," *Public Radio International - The World,* May 11, 2021, https://www.pri.org/stories/2021-05-11/new-zealand-condemns-china-s-treatment-uyghurs-wont-call-it-genocide; Mike Wesley-Smith, "Kiwi Uyghur man claims harassment and threats by Chinese embassy," Newshub, July 27, 2019, https://www.newshub.co.nz/home/shows/2019/07/kiwi-uyghur-man-claims-harassment-and-threats-by-chinese-embassy.html.

[61] Takamura Keiichi, "Backstories: Uighurs abroad still feel pressure," *NHK*, July 28, 2020, https://www3.nhk.or.jp/nhkworld/en/news/backstories/1222/.

[62] Takao Harakawa and Sakei Shimbun, "Chinese Abuse of Uyghurs Reaches Japan, Blackmails Migrant into Spying on Tokyo," *JapanForward*, October 1, 2020, https://japan-forward.com/chinese-abuse-of-uyghur-reaches-japan-blackmails-migrant-into-spying-on-tokyo/.

[63] Takamura Keiichi, "Backstories: Uighurs abroad still feel pressure."

[64] Harakawa and Shimbun, "Chinese Abuse of Uyghurs Reaches Japan."

Halmat's case is not unique. In an interview with us, another Japanese Uyghur who requested anonymity to protect his identity revealed some of the methods by which China's security services obtain information from informants. In May 2019, Yusup (pseudonym) began receiving WeChat messages from a man who claimed to know one of his relatives in Xinjiang and claimed to be looking for advice on study abroad programs in Japan. Within a few weeks, however, the man revealed himself to be an agent of the Xinjiang Public Security Bureau. "If you can provide me with information on Uyghur activists, I can help [your relative]," he wrote. Yusup was instructed to attend an annual Uyghur gathering in Tokyo and provide photographs of Erkin Sidick, a Uyghur engineer at NASA and international activist who planned to visit the event. When Yusup declined, the agent changed his tone in his response, reportedly saying, "Your family will suffer. Remember that I am your friend, and I want to help you and your family."[65]

The following months caused great strain on Yusup and his wife. "We didn't want our families to suffer, but we also didn't want to betray our people," he told us. "My wife blamed me for all of it and said that I had placed our families in great danger. It all weighed heavily on me." Throughout 2020, the agent asked Yusup to transcribe posts from Japanese social media concerning Uyghur activism in Tokyo. After fulfilling his requests initially, Yusup attempted to reject the work. Still, the agent instructed him to quit his job and said he would receive a monthly salary for his services to "national security." When Yusup refused to accept payment for his transcription, the officer insisted that his family be paid on his behalf instead. Yusup again refused but later received a message over WeChat of a family member receiving payment from a Chinese security officer: "Remember that I am your friend. I am protecting your family." After that, the agent began sending increasingly sensitive information regarding professionals in Japan whom they wanted him to monitor. Most of the work involved translating blog posts by these individuals and noting their participation at protests and who was sponsoring their activism. The listed professionals also included a Japanese national. Yusup informed Japan's intelligence

[65] Yusup (Uyghur diaspora member), online interview by Bradley Jardine, September 15, 2021.

community after China began monitoring the Japanese citizen, fearing that he was being coerced into committing a criminal offense. In response, one of Yusup's relatives sent a message denouncing him, which Yusup believes was obtained by security services using force.[66] Finally, after over two years of contact with the intelligence officer, Yusup shut down his WeChat account in February 2021, making the agonizing decision not to contact his own family again.[67]

Japan, home to a Uyghur diaspora of approximately 3,000 people, has yet to take any concrete action condemning the actions of the Chinese government or to protect the Uyghurs living on its soil, even as Japanese public opinion turns against the PRC. However, Halmat's demands for political and legislative action similar to those taken by Western countries have not gone unheard: as of early 2021, the Japanese government began debating sanctions similar to the Global Magnitsky Act.[68]

In the past, the Chinese government has also attempted to block Uyghur activism in the Asia Pacific by protesting events held by Uyghur activists and allies and by harassing Uyghurs in the diaspora community. The Australian Jewish Association, a staunch advocate of Uyghur rights and freedoms in Australia, hosted an event on December 2, 2020, with Ramila Chanisheff, the President of the Australia Uyghur Tangritagh Women's Association. During the event, unknown hackers entered the event and disseminated "obscene, abusive messages" on screen, working to discredit Chanisheff and her statement.[69]

In March 2018, thousands of Uyghurs staged a protest in Canberra against Chinese government discrimination; it was the

[66] XUAR authorities have filmed and publicly released many such "denouncements," all of which appear to be produced under coercion and duress. For more on the phenomenon, see "'The Government Never Oppresses Us': China's Proof-of-Life Videos as Intimidation and a Violation of Uyghur Family Unity," Uyghur Human Rights Project, February 2, 2021, https://uhrp.org/report/the-government-never-oppresses-us-chinas-proof-of-life-videos-as-intimidation-and-a-violation-of-uyghur-family-unity/.

[67] Yusup, interview by Bradley Jardine.

[68] Ben Dooley and Hisako Ueno, "Japan Is Finding It Harder to Stay Quiet on Abuse of China's Uyghurs," *New York Times,* April 1, 2021, https://www.nytimes.com/2021/04/01/world/asia/japan-uyghurs-xinjiang.html.

[69] David Adler, "CCP's persecution of the Uyghurs," *Spectator*, January 16, 2021, https://www.spectator.com.au/2021/01/ccps-persecution-of-the-uyghurs/.

largest ever Uyghur-led demonstration in Australia. The rally was held in tandem with others around the world, including in Sydney, Adelaide, New York, and Istanbul.[70] Hours after the protest ended, Uyghurs in the diaspora community, including teenagers who had been born in Australia, started to receive harassing calls, video chats, and messages.[71] Uyghurs in Australia have nevertheless continued to protest despite the Chinese government's alleged attempts to intimidate them into silence. Uyghurs in Adelaide, home to one of the largest Uyghur diaspora communities in Australia at approximately 170 families, have raised concerns over the construction of a new Chinese consulate in their neighborhood. While the Chinese consulate has always had a presence in Adelaide, this new building—considered by the local community to be a potential surveillance outpost—suggests a more permanent and substantial presence. This consulate is the fifth consulate set up by the Chinese government and the fourth largest in Australia.

Uyghurs in the Adelaide diaspora community note that they have received several calls from the Chinese embassy and consulates in Australia and have expressed their concerns about an additional outpost so close to them. As a result, Uyghurs, Tibetans, and other groups who have felt the long reach of the Chinese government first-hand have staged multiple protests outside the Adelaide consulate.[72] In an interview with us, Uyghur Australian citizen Zulfiya Abdulla said many members of the Adelaide community have received calls from relatives in the Uyghur Region telling them to cease their protests, suggesting they are being monitored: "Neighbors have told me that family members [in the XUAR] have said 'stop going to the mosque [in Adelaide],' showing that we are being watched here." She says that she does not feel

[70] Gerry Shih, "Ethnic Uighurs Protest Chinese security crackdown," *Associated Press*, March 15, 2018, https://apnews.com/article/7817b44ef57641d8a36cd1fe17a1e379.

[71] Rick Noack, "Uighurs fled persecution in China. Now Beijing's harassment has followed them to Australia," *Washington Post*, February 10, 2019, https://www.washingtonpost.com/world/2019/02/07/uighurs-australia/.

[72] Peta Doherty, "Adelaide's Uighur community fears new Chinese consulate building will lead to monitoring," *SBS,* April 6, 2021, https://www.sbs.com.au/news/adelaide-s-uighur-community-fears-new-chinese-consulate-building-will-lead-to-monitoring; Rebecca Brice and Rhett Burnie, "New Adelaide Consulate attracts angry protest after complaints about size, human rights abuses," *ABC News* (Australia), March 29, 2021, https://www.abc.net.au/news/2021-03-30/protest-at-opening-of-new-adelaide-chinese-consulate/100037766.

worried about herself because of her Australian citizenship but fears for her family. "My daughter is running for a seat in parliament, and I worry that she will become a target for harassment," she said, giving an indicator of the potential chill on political activity provoked by China's transnational repression.[73]

New Zealand, like Japan and Australia, has yet to take any explicit actions to protect Uyghurs living in its territory, beyond denouncing the "severe human rights abuses in the Xinjiang Uyghur Autonomous Region."[74] The country's immigration system also leaves Uyghurs vulnerable. Similar to the system in the United States, New Zealand's asylum system operates on a three-year cycle of refugee quotas. Would-be asylees must be recognized internationally as refugees and "referred to [the] New Zealand [government] by UNHCR." Further, these refugees are examined based on: "[Immigration New Zealand] policy, credibility, settlement, security, immigration risk, and health." After a five-week "reception program," these refugees become permanent residents of New Zealand.[75] Others may apply for asylum in New Zealand—a process that takes six months as of writing. This immigration process in New Zealand has left some Uyghurs who reside in the country on temporary visas until their asylum claims are processed—a state of legal limbo in which they are unable to get long-term employment or government documentation.[76]

North America

On January 19, 2021, the United States declared the human rights violations in the Uyghur Region to be genocide. Canada soon

[73] Zulfiya Abdulla (Uyghur diaspora member), online interview by Bradley Jardine, October 1, 2021.

[74] "New Zealand parliament says Uighur rights abuses taking place in China," *Reuters*, May 4, 2021, https://www.reuters.com/world/asia-pacific/new-zealand-parliament-says-uyghur-rights-abuses-taking-place-china-2021-05-05/.

[75] New Zealand Refugee and Protection Office website, last updated 2021, accessed July 13, 2021, https://www.immigration.govt.nz/about-us/what-we-do/our-strategies-and-projects/supporting-refugees-and-asylum-seekers/refugee-and-protection-unit/new-zealand-refugee-quota-programme.

[76] Gill Bonnett, "Uighur refugee who fled China left jobless while awaiting NZ residence," *RNZ*, January 30, 2020, https://www.rnz.co.nz/news/national/408464/uighur-refugee-who-fled-china-left-jobless-while-awaiting-nz-residence.

followed suit with its declaration on February 22, 2021. These declarations have drawn greater attention to the issue and galvanized further calls to action among liberal democracies that have followed suit, including the Netherlands (declared March 1, 2021) and the UK (announced April 22, 2021), among others. However, Uyghurs living in Canada and the United States must still confront the Chinese government's efforts to control and silence them across sovereign borders daily. Our dataset contains 64 named cases and an upper estimate of 130 cases of individuals who have experienced Chinese transnational repression while living in the United States and Canada.

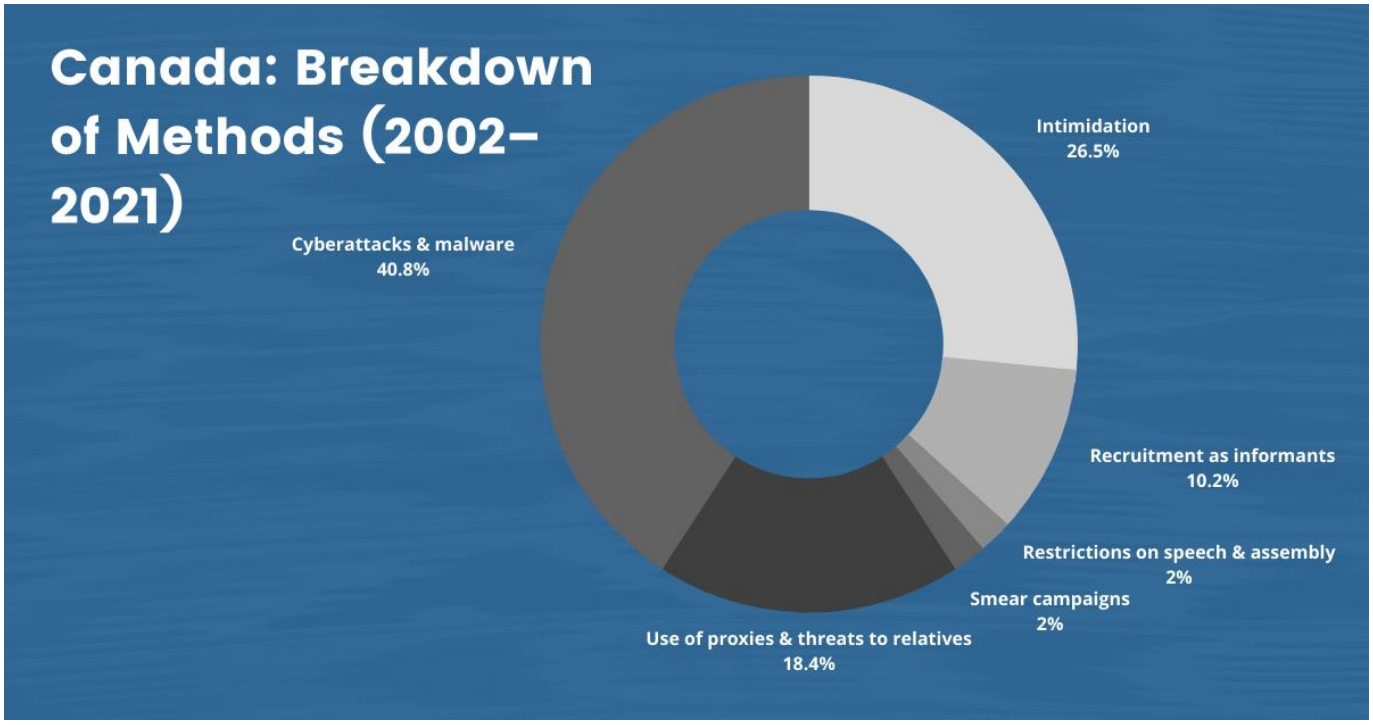

Image 8. This chart shows the methods of stage 1 transnational repression deployed by the Chinese government against Uyghurs living on Canadian soil. Source: Oxus Society for Central Asian Affairs.

According to a confidential report submitted to the Canadian government in 2018, the Chinese government's intimidation and harassment of diaspora communities has become commonplace. This intimidation seems to be working, with many dissidents ceasing their activities on Canadian soil—to the concern of the Canadian government.[77] Dilnur Enwer arrived in Canada in January

[77] Tom Blackwell, "'Don't Step Out of Line': Confidential report reveals how Chinese officials harass activists in China," *National Post*, January 5, 2018, https://nationalpost.com/news/world/confidential-report-reveals-how-chinese-officials-harass-activists-in-canada-there-is-a-consistent-

2019 and applied for asylum. A resident of Montreal, she reported receiving calls from unidentified people and the Chinese embassy repeatedly since her arrival, requesting that she go to the Chinese Embassy to pick up an "important document." Before she lost communication with family in the Uyghur Region, one of her relatives warned her that she would be caught by the Embassy and sent back to the XUAR.[78]

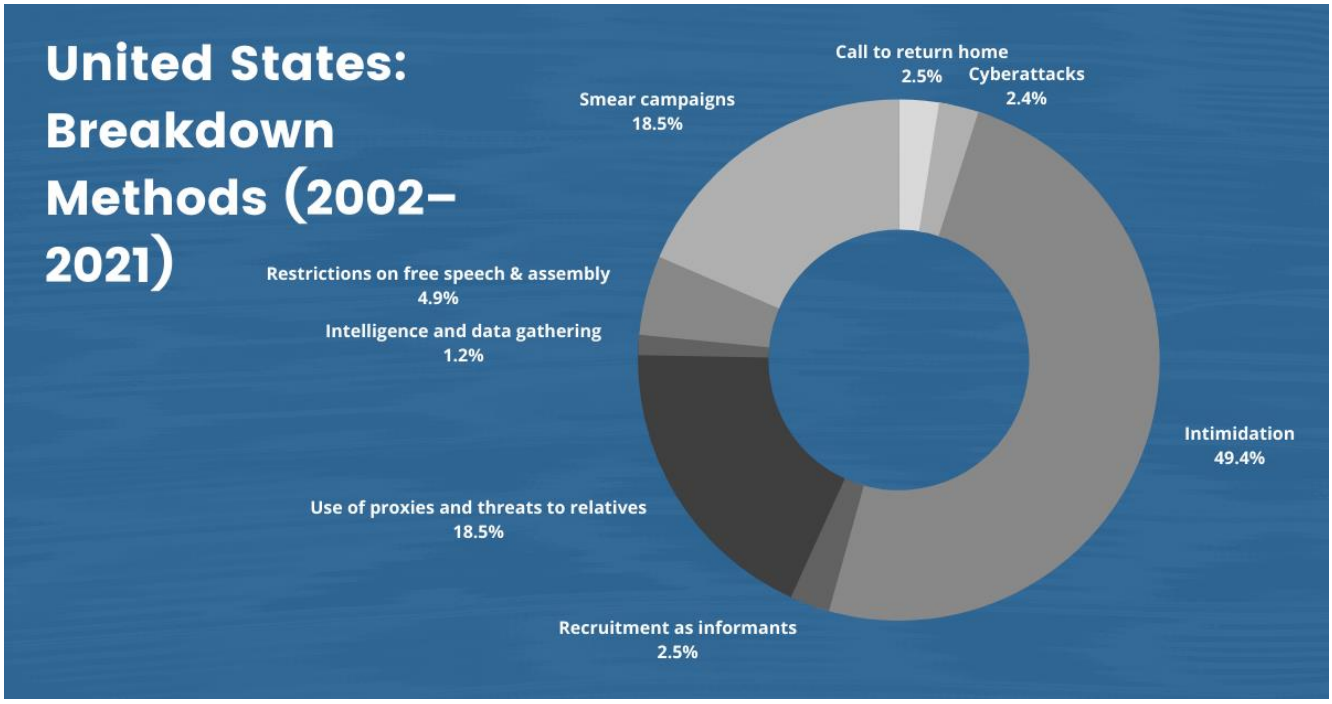

Image 9. This chart shows the methods of stage 1 transnational repression deployed by the Chinese government against Uyghurs living on U.S. soil. Source: Oxus Society for Central Asian Affairs.

The Uyghur American community, primarily centered in the Northern Virginia suburbs of Washington, D.C., numbers around 10,000 people total. Many D.C.-area Uyghurs say that they undergo harassment and intimidation daily, including receiving threats by text, chat apps including WeChat, voicemail, calls, email, or third-

pattern/wcm/2de0402f-5d1c-4a0a-b4bb-8dcfd56b3788/; Jeremy Nuttall, "Putting the Spotlight on Genocide; Canada's Small Uyghur Community Struggles to Make People Understand," *Toronto Star*, November 21, 2020, https://www.thestar.com/news/canada/2020/11/21/putting-the-spotlight-on-a-genocide-canadas-small-uighur-community-struggles-to-make-people-understand.html.

[78] "Nowhere Feels Safe."

party messages.[79] During some of these interactions, Chinese officials have reportedly requested passport information and other details and information on future protests and organizing activity from Uyghurs living in the United States. Many Uyghur community members in and around D.C. often wear masks and sunglasses to obscure their faces and hide their identities from people taking photos when they attend protests in the United States.[80]

Uyghurs in other parts of the United States have faced pressure, as well. In 2018, Gulruy Asqar began to receive calls from the Chinese consulate in Houston. These phone calls started with a recorded message concerning a vital document she supposedly needed to submit to the consulate. A Chinese person would then answer and ask for her details. Asqar refused each time until finally, she told embassy staff that she was a U.S. citizen and "did not care about their document." The calls stopped. Then calls from a Chinese mail delivery company began—another attempt, she suspects, to collect her personal information.[81]

Uyghurs living in Canada and the United States must still confront the Chinese government's efforts to control and silence them across sovereign borders daily.

Chinese state agents increasingly use family members in the Uyghur Region as proxies to pressure Uyghur communities. Kuzzat Altay, the President of the Uyghur American Association, started an entrepreneurship network in 2018 for the Uyghur diaspora community in Fairfax, Virginia.[82] However, most of the 25 members left the network after they received calls from their family members in the Uyghur Region urging them to leave the group.[83] Sometimes repression occurs in response to political activity. In September 2018, Rushan Abbas spoke about the human rights abuses in the Uyghur Region at a think-tank event in Washington. Days later, her

[79] Omer Kanat, "China's Cross Border Campaign to Terrorize Uyghur Americans," *The Diplomat*, August 29, 2019, https://thediplomat.com/2019/08/chinas-cross-border-campaign-to-terrorize-uyghur-americans/.

[80] Colm Quinn, "'We're a People That Are Grieving': Local Uyghurs Have Escaped China, But Still Fear Repression," *DCist*, March 14, 2019, https://dcist.com/story/19/03/14/were-a-people-that-are-grieving-local-uighurs-have-escaped-china-but-still-fear-repression/.

[81] "Nowhere Feels Safe," Amnesty International.

[82] "Kuzzat Altay" (bio), Uyghur American Association, June 10, 2021, accessed via archived version of the website on October 25, 2021, https://web.archive.org/web/20210610190710/https://www.uyghuraa.org/kuzzat.

[83] "Targets of Crackdown in China Fear Government's Reach in U.S.," *Associated Press*, March 8, 2020, https://apnews.com/article/religion-immigration-ap-top-news-international-news-politics-7dc7c0df54fc0d270a15186ac9e5ba84.

sister Gulshan was detained in the XUAR. Rushan sees this as a retaliatory act meant to silence her.[84] She went on to found Campaign for Uyghurs, a D.C.-based advocacy organization where she currently serves as executive director.

The Covid-19 pandemic necessitated that many events about the Uyghur crisis be moved to an online format. Some of these events were "zoom-bombed" by unknown entrants who worked to disrupt the event by attempting to discredit speakers and even prevent them from speaking further. In November 2020, students at Brandeis organized an event on the oppression of Uyghurs in XUAR with activist Rayhan Asat and several scholars. Ms. Asat told us that university offices received threatening template emails from Chinese Students and Scholars Association members before the event. During the event itself, some participants selected pictures of Xi Jinping and other prominent CCP leaders to use in place of their live video. One user played the national anthem during one speaker's remarks. Ms. Asat reported that participants hijacked her screen-share during her presentation and wrote crude, harassing terms across her slides and images of her imprisoned brother, Ekpar Asat.[85] "We're up against a very powerful government, and we need universities to stand by us," she said in an interview with us. "These campuses are some of the last remaining platforms we have left, and China is doing everything in its power to close them off to us."[86]

Uyghurs living in Canada have also reported attempts by the Chinese government to coerce them into committing espionage. A Uyghur speaking to the *Globe and Mail* on the condition of anonymity in 2015 said that Chinese security services used a variety of threats to coerce him into committing espionage in Canada and reporting back to the Chinese government over the course of his visits to the XUAR. Another Uyghur Canadian, Quttapay (pseudonym), was approached by two state security officers at a train station in the Uyghur Region, who then tried to recruit him.

---

[84] "Nowhere Feels Safe," Amnesty International.

[85] Lin Yang, "China-Sensitive Topics at US Universities Draw More Online Harassment," *Voice of America*, November 20, 2020, https://www.voanews.com/a/usa_china-sensitive-topics-us-universities-draw-more-online-harassment/6198648.html/;

[86] Rayhan Asat (Uyghur diaspora member), interview by Bradley Jardine, Washington, DC, July 18, 2021.

They were unsuccessful, and Quttapay was given 48 hours to leave the country. Bekkri (pseudonym) and Yusup (pseudonym), Uyghurs living in Canada, told the Canadian press that they had to ensure that they had the right combination of documents to leave China. Before they left, the Chinese police offered to issue them the necessary passports—a rarity for Uyghurs—only if they were willing to commit espionage abroad. Bekkri found another way to secure a passport; Yusup managed to talk his way out of committing espionage for the moment but was left with a warning from the security services: "We are patient."[87]

The Facebook phishing scheme that targeted Uyghurs worldwide included Canadian and U.S. citizens. Facebook Canada planned to notify the "fewer than 20" people in Canada who were targeted. Facebook said the operation used a variety of techniques to reach the people they were targeting. The company said the hackers set up Facebook accounts where they posed as "journalists, students, human rights advocates or members of the Uyghur community to build trust with people they targeted and trick them into clicking on malicious links." Facebook said that they also set up malicious websites that looked like popular Uyghur or Turkish news sites and launched "watering hole attacks" to infect visitors to legitimate websites, Facebook said. Facebook added that the hackers also set up fake third-party stores with Uyghur-themed apps that contained malware. These stores included applications such as a keyboard app, prayer app, and dictionary app.

Mehmet Tohti, executive director of the Uyghur Rights Advocacy Project, said Chinese authorities have long targeted Canada's 2,000-member Uyghur community. Members of the Canadian parliament are calling on Prime Minister Justin Trudeau to implement laws that would protect Canadians online.[88] In a letter to lawmakers, Bill Blair, Minister of Public Safety in Canada, said that "foreign states, including the PRC, attempt to threaten and

[87] Craig Offman, "Uyghur-Canadians Say Chinese Officials Detained, Blackmailed Them," *Globe and Mail,* April 22, 2015, https://www.theglobeandmail.com/news/national/uyghur-canadians-say-chinese-officials-detained-blackmailed-them/article24056142/.

[88] Elizabeth Thompson, "Cyber Espionage Operation Targeted Canadia Uyghurs, Says Facebook," *Canadian Broadcasting Corporation*, March 24, 2021, https://www.cbc.ca/news/politics/china-uyghur-canada-espionage-1.5962221.

intimidate individuals around the world, including in Canada, through various state entities and non-state proxies."[89]

The UIGHUR Act of 2019 and Uyghur Human Rights Policy Act of 2020 seek to sanction CCP officials responsible for the genocide in the XUAR, as well as to protect Uyghur Americans from China's campaign of intimidation and harassment.[90] While effective at the former—the U.S. Treasury Department has placed several rounds of sanctions on various CCP officials in the XUAR through these acts and the Global Magnitsky Act—it is unclear if these Acts have helped protect the Uyghur diaspora community from the malign influence of the Chinese government.[91] The 2020 Uyghur Human Rights Act requires that relevant agencies of the U.S. government report to Congress on their efforts to protect the Uyghur community in the U.S. In August 2021, the FBI released an unclassified counterintelligence bulletin on the transnational repression of Uyghurs living in the United States, noting the intent of the Chinese government to "silence dissent, issue instructions, collect information, and compel compliance," and mentioning specific cases of Uyghurs in the United States who are facing harassment and coercion from overseas.[92] While the U.S. government and responding agencies have sought to educate the public on cybersecurity and created avenues for individuals and groups to report incidents, there is much work to be done in bridging the gap between these resources and vulnerable communities.[93]

---

[89] Bill Blair, "Response to the December 18, 2020 motion on Foreign Interference," Public Safety Canada, August 20, 2021, https://www.passengerprotect-protectiondespassagers.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/27-en.aspx.

[90] US Congress, Senate, *UIGHUR Act of 2019*, S 178, 166th Congress, introduced in Senate January 17, 2019, https://www.congress.gov/bill/116th-congress/senate-bill/178/text; US Congress, Senate, *Uyghur Human Rights Policy Act of 2020* S 3744, 116th Congress, introduced May 14, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3744.

[91] John Ruwitch, "U.S. Sanctions Chinese Officials, Including Politburo Member, For Xinjiang Abuses," *NPR*, July 9, 2020, https://www.npr.org/2020/07/09/889406296/u-s-sanctions-chinese-officials-including-politburo-member-for-xinjiang-abuses.

[92] "Chinese Government Transnational Repression Violates US Laws and US-based Uyghurs' Rights," FBI.

[93] "Chinese Government Transnational Repression Violates US Laws and US-based Uyghurs' Rights, FBI. See also "Cyber Incident Reporting," U.S. Federal Bureau of Investigation; "Report Incidents, Phishing, Malware or Vulnerabilities," Cybersecurity and Infrastructure Security Agency, accessed August 8, 2021, https://us-cert.cisa.gov/report; "What We Investigate: The Cyber Threat," U.S. Federal Bureau of Investigation, accessed August 8, 2021, https://www.fbi.gov/investigate/cyber.

Confronting China's harassment remains a more significant gap still.

VII. Welcome to the Machine: Digital Authoritarianism in the Uyghur Region and Beyond

In 2020, Chinese President and Party General Secretary Xi Jinping gave a series of speeches announcing his ambition to achieve A.I. supremacy by the end of the decade. In a competition billed by international media as "the new space race," China has sought to compete with leading research nations and turn itself into a global hub for A.I. innovation.[94] The CCP has established a number of partnerships with private companies and start-ups to achieve this goal by any means necessary, including recruiting top computer scientists from the United States.[95] These goals, as pointed out in a recent *Atlantic* article, may also serve to empower China's security services, arming them with A.I.-powered algorithms designed to anticipate dissent and counteract protests wherever they may occur. This technology, combined with the hundreds of millions of cameras that already exist across the Chinese mainland, could potentially allow the state to identify an individual and pair that information with data in one of several police databases that contain biometric information, travel records, purchases, call records, family, friends, and associates, etc. Computer algorithms designed to assess people and their loyalty and to look for threats will eventually be able to conduct "risk" assessments, assign people a status accordingly, and, if need be, target people for arrest prior to a crime being committed.[96] This effort to "predictively police" the

[94] Kai Strittmatter, *We Have Been Harmonized* (New York: Harper Collins, 2020), 176.

[95] Ibid., 167–213.

[96] Ross Andersen, "The Panopticon is already here," *Atlantic*, September 2020, https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/.

population of China has profound implications for Uyghurs and other Turkic Muslim-majority peoples living in the XUAR, where these very methods have been pioneered.

Three types of facial recognition software and A.I. algorithms in use by the Chinese government since 2018 claim to identify "Uyghur"-coded physical traits. Chinese companies Yitu, Megvii, Sensetime, and Cloud Walk have worked to improve their algorithms to recognize Uyghur features; in 2018, tech-giant Hikvision noted on its website that its facial recognition cameras could recognize gender, as well as whether targets were Uyghur.[97] Chinese company iFlytek, meanwhile, boasted it had helped "solve crimes" in the XUAR using its voice-recognition technology that can "read" the Uyghur language. This same company is helping the Chinese government build a voice and speech-pattern database.[98] Some of these companies, along with tech giant Huawei, have become the target of U.S. sanctions due to their role in implementing the surveillance state in the Uyghur Region.[99]

Crucially, many of the emerging technologies used to create this surveillance state are being sold to China by Western actors, often despite attempts by Western governments to curtail those sales.

A 2021 article by the *BBC* reported that facial recognition technology designed to read emotions had also been tested in detention centers in the Uyghur Region. These cameras are meant to read "negative" or "anxious" emotions to "prejudge" the subject.[100] This reading of emotions, also known as "automated affect recognition," is far from accurate in most cases. However, it relies on categorizing emotions without consideration for social, cultural, and individual factors that impact facial expressions and expressions of emotion. A U.S. Transportation Security Administration program relying on similar technology to spot people "likely to commit terrorism" after the events of September 11, 2001, yielded no results.[101] This technology, based on pseudoscience, acts as yet another data point for the persecution of Uyghurs on arbitrary grounds. Increasingly, these companies are

[97] Strittmatter, *We Have Been Harmonized,* 200.

[98] Ibid., 202–203.

[99] Ibid., 203.

[100] Jane Wakefield, "AI emotion-detection software tested on Uyghurs," *BBC*, May 26, 2021, https://www.bbc.com/news/technology-57101248.

[101] Kate Crawford, "Artificial Intelligence is Misreading Human Emotion," *Atlantic*, April 27, 2021, https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/.

implementing international smart-city programs along the Digital Silk Road, including in Central Asia and Pakistan—significant hubs for transnational repression of the Uyghurs.[102]

Crucially, many of the emerging technologies used to create this surveillance state are being sold to China by Western actors, often despite attempts by Western governments to curtail those sales. According to a June 2021 *New York Times* report, two U.S. companies, Promega and Thermo Fisher, have continued to sell DNA equipment to companies in China that then resell the technology to the police in the Uyghur Region. While DNA collection is standard for certain groups in China (e.g., in criminal cases, for migrant workers, etc.), in the Uyghur Region this data collection is much more far-reaching, extending to nearly the entire population.[103]

These technologies allow the XUAR Public Security Bureau (PSB) to collect and sequence thousands of unique blood samples and DNA samples collected by local police at stations across the Uyghur Region, where residents were summoned to for a "check-up" in a program eventually called "Physicals for All."[104] This information, collected along with details including height, weight, fingerprints, and face and voice recordings, was then added to databases used to surveil, track, and model the behaviors of Uyghurs. According to journalists citing the Chinese press, the program collected the data of more than 36 million individuals across the XUAR.[105] This case is only the most recent in a series that reveals how the Chinese state appropriates and exploits Western technology to commit human rights violations against Uyghurs.

---

[102] Bradley Jardine, "China's Surveillance State has Eyes on Central Asia," *Foreign Policy*, November 15, 2019, https://foreignpolicy.com/2019/11/15/huawei-xinjiang-kazakhstan-uzbekistan-china-surveillance-state-eyes-central-asia/; Bradley Jardine and Robert Evans, "Nets Cast from the Earth to the Sky."

[103] "China: Police DNA Database Threatens Privacy," Human Rights Watch, May 15, 2017, https://www.hrw.org/news/2017/05/15/china-police-dna-database-threatens-privacy.

[104] "China: Minority Region Collects DNA From Millions," Human Rights Watch, December 13, 2017, https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions#.

[105] Geoffrey Cain, *The Perfect Police State* (New York: Hachette Book Group, 2021), 115–18; Sui-Lee Wee, "China Still Buys American DNA Equipment for Xinjiang Despite Blocks," *New York Times*, June 11, 2021, https://www.nytimes.com/2021/06/11/business/china-dna-xinjiang-american.html.

The same technologies are being used against Uyghurs overseas. In 2018, Ahmad Talip, a Uyghur living in Dubai, noted that he was forced to provide a blood sample during arbitrary imprisonment.[106] Talip's claim fits into a larger pattern in which China's intelligence services collect data on Uyghurs living abroad. This new "ID card system," like that in the Uyghur Region, requires detailed information on subjects, including their DNA, and then uses that information to monitor Uyghur communities abroad.

Party cadres have explicitly requested information from Uyghurs residing in the United States and elsewhere so as to feed data into this dataset. In 2018, Barna (pseudonym) received a message from her mother, asking her to send over images of the license plate on her car as well as her bank card number, photo ID, and phone number, reportedly so that they could be added to the database behind a new system of Chinese state ID cards. This database and these ID cards are meant to include Uyghurs living abroad. Barna chose to lie about having a card or bank account in the United States, denying that she had either, but sent an image of her photo ID to her mother out of concern for her mother's safety—she understood from the tone of her messages that Chinese officials had coerced her mother.[107]

Jevlan Shirmemmet,[108] who left the XUAR to study in Turkey, gave the BBC a recording of a call he received a few weeks after he made a post on social media about the arrest of his family in the Uyghur Region. The caller, who said he was from the Chinese embassy in Ankara, told Jevlan to "write down everyone you've been in contact with since you left Xinjiang," and send an email "describing your activities," so that "the mainland might reconsider your family's situation." Mustafa Aksu, another Uyghur who previously lived in Turkey but now lives in the United States, showed the BBC messages from an old school friend who had become a police officer and attempted to pressure Mr. Mustafa to

---

[106] "Uyghur Speaks Out About Husband's 'Deportation' From UAE," *Middle East Eye*, February 8, 2021, https://www.middleeasteye.net/news/uighur-speaks-out-against-husbands-deportation-uae.

[107] Bethany Allen-Ebrahimian, "Chinese Cops Now Spying on American Soil," *DailyBeast*, August 14, 2018, https://www.thedailybeast.com/chinese-police-are-spying-on-uighurson-american-soil.

[108] His name is also spelled "Jewlan Shirmemet" in some sources.

provide information on the activities of Uyghur activists in Turkey.[109]

This internationalization of government repression has accelerated dramatically since 2017, mainly due to algorithmic surveillance. In the XUAR, police stations feed data into a powerful database known as the Integrated Joint Operating System (IJOP).[110] The IJOP categorizes Uyghurs as suspicious for any contact with people in 26 blacklisted countries, along with a host of other possible reasons.[111] People who have traveled to, have family members living in, or otherwise communicate with people in the 26 countries have been interrogated, detained, or imprisoned. Increasingly, the borders of China's advanced surveillance system are blurred, with intelligence gathering and harassment on the rise worldwide.

New troves of information further suggest that liberal democracies are catching the security state's eye. In March 2021, the Shanghai Public Security Bureau (PSB), a regional police station, was hacked, and 1.1 million surveillance records were leaked. One of the revelations from this trove of documents was an unprotected database with the codename "Uyghur Terrorist," which was part of an open-source database to which security agencies worldwide had access. The presence of this platform is just a tiny glimpse into the enormous scope of China's international campaign against Uyghurs. The database contains records of thousands of Uyghur "suspected terrorists" who have been detained, questioned, and/or monitored by the PSB. The inclusion of these "suspected terrorists" seems to have been based on far-reaching claims since more than 400 individuals in the database flagged for in-person examination were minors, some of whom were as young as five years old.[112] The database also included the information of more than 5,000

[109] Joel Gunter, "The cost of speaking up against China," *BBC*, March 31, 2021, https://www.bbc.com/news/world-asia-china-56563449.

[110] "China's Algorithms of Repression: Reverse Engineering a Xinjiang Police Mass Surveillance App," Human Rights Watch, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass.

[111] "'Eradicating Ideological Viruses': China's Campaign of Mass Repression in Xinjiang," Human Rights Watch September 9, 2018, https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs.

[112] Australians Flagged in Shanghai Security Files Which Shed Light on China's Surveillance State and Monitoring of Uyghurs," *ABC News* (Australia), April 1, 2021, https://www.abc.net.au/news/2021-04-01/shanghai-files-shed-light-on-china-surveillance-state/100040896.

foreigners—who were flagged simply for having traveled to Shanghai—for further monitoring. At least three Uyghur Australians were on the list, including two citizens—Nurgul Sawut and Maimaitaji Kasimu[113]—and an anonymous permanent resident whose mother was reportedly threatened with detention after he attended a protest. Several Uyghur community leaders in Australia have also been blacklisted as "terrorists" otherwise.[114] The Shanghai List stands as further evidence that they are targets of the Chinese government.

China's drive to intimidate, harass, and control Uyghurs has increased in the last five years, in correlation with China's activities in the Uyghur Region and its efforts to return or arrest Uyghurs living abroad. In particular, the Chinese government has focused its efforts on cyberattacks, a form of stage 1 transnational repression, with a recorded 2,774 cases, and intimidation, including phone calls, direct threats, and surveillance, with a recorded 526 cases in our dataset. In addition, the government has primarily focused stage 1 repression efforts on Uyghurs living in liberal democracies, with 3,040 recorded cases in Europe, 81 in the Asia Pacific, and an additional 130 in North America.

VIII. Cyberspace: The Next Frontier for Transnational Repression

Modern communications technology has rapidly expanded the reach of China's security services, created new methods and tactics for gaining information on Uyghurs residing overseas, and expanded opportunities for crowdsourcing intimidation. Increasingly, the Chinese state is using a combination of botnets and

[113] "Maimaitaji Kasimu" is a pinyin transliteration of the Chinese-language version of the name Memethaji Qasim.

[114] "Australian Uyghurs Say They've been Monitored and Threatened" (video), MSN, April 15, 2021, https://www.msn.com/en-au/lifestyle/lifestyleroyals/australian-uyghurs-say-theyve-been-monitored-and-threatened/vp-BB1fFzjr; "Australians Flagged in Shanghai Security Files," *ABC News* (Australia).

targeted disinformation campaigns to raise the stakes for individual Uyghurs speaking out about the abuse they face. These sustained attacks also undermine organizations' capacity to operate due to the high costs required for computer engineers to protect their infrastructure, allowing malicious actors to effectively "price out" civil society.

China's rising cyber capabilities have gained the attention of prominent Western officials and political commentators in recent months. In March 2021, Microsoft blamed China for starting a "free-for-all" in which numerous hackers used the Microsoft Exchange email program to break into organizations around the world.[115] In July 2021, the United States government accused China's Ministry of State Security (MSS) and its affiliated hackers of attacking and compromising more than 100,000 Microsoft Exchange servers worldwide.[116] Analysts have also linked several high-profile spyware campaigns to the People's Liberation Army (PLA) over the past decade.[117] China's hacking ecosystem more broadly appears to be expanding beyond state actors to include private for-hire actors and nationalist individuals, who hack on behalf of the Chinese government.[118]

Increasingly, the Chinese state is using a combination of botnets and targeted disinformation campaigns to raise the stakes for individual Uyghurs speaking out about the abuse they face.

According to the 2018 Internet Development Statistics Report, China's cybercriminal underground was worth more than US$15 billion, nearly twice the size of its information security industry. The same Chinese-language source also shows that China's cybercrime is growing at a rate of more than 30 percent per year, with an estimated 400,000 people working in underground cybercriminal

[115] Kevin Collier, "China Behind Another Hack as U.S. Cybersecurity Issues Mount," *NBC*, April 21, 2021, https://www.nbcnews.com/tech/security/china-another-hack-us-cybersecurity-issues-mount-rcna744.

[116] John Hudson and Ellen Nakashima, "U.S., Allies Accuse China of hacking Microsoft and Condoning Other Cyberattacks," *Washington Post*, July 19, 2021, https://www.washingtonpost.com/national-security/microsoft-hack-china-biden-nato/2021/07/19/a90ac7b4-e827-11eb-84a2-d93bc0b50294_story.html.

[117] "China Sharpens Hacking to Hound its Minorities, Far and Wide," *New York Times*, October 22, 2019, https://www.nytimes.com/2019/10/22/technology/china-hackers-ethnic-minorities.html.

[118] Paul Mozur and Chris Buckley, "Spies for Hire: China's New Breed of Hackers Blends Espionage and Entrepreneurship," *New York Times*, August 26, 2021, https://www.nytimes.com/2021/08/26/technology/china-hackers.html; Patrick Howell O'Neill, "How China turned a prize-winning iPhone hack against the Uyghurs," *MIT Technology Review*, May 6, 2021, https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/.

networks.[119] These cybercriminal networks often feed into state power. For example, the cybersecurity firm FireEye reported that a group of state-sponsored hackers in China ran activities for personal gain while undertaking spying operations for the Chinese government in 14 different countries since 2012. In its 2019 report, the company stated that the hacking group APT41 was different from other China-based groups tracked by security firms in that it used non-public malware typically reserved for espionage to profit off attacks on video game developers.[120]

Such networks have also targeted human rights groups and journalists. Chinese spyware campaigns have expanded beyond China's borders and toward think tanks, government agencies, human rights groups, and law firms around the globe.[121] Chinese government denials of hacking activity often have an air of plausibility because many of the organizations they target lack sophisticated network security, as well as the fact that individual hackers, motivated by patriotism or simple mischief, can take action without the need for state encouragement. Further, attribution remains a lingering challenge in the field of cybersecurity, as actors can mask their identities, origins, and code to evade or misdirect attribution.[122] Uyghur advocacy groups remain especially exposed. The World Uyghur Congress (WUC), in particular, has been subject to regular DDoS attacks and phishing schemes. The table below outlines the attacks and harassment against the WUC:

[119] Allen Bernard, "Chinese Cybersecurity Criminals are Getting More Organized and Dangerous," *TechRepublic*, February 13, 2020, https://www.techrepublic.com/article/chinese-cyber-criminals-are-getting-more-organized-and-dangerous/.

[120] Josh Taylor, "Chinese Cyber hackers 'Blurring Boundary Between State Power and Crime," *Guardian*, August 7, 2019, https://www.theguardian.com/technology/2019/aug/08/chinese-cyberhackers-blurring-line-between-state-power-and.

[121] Andrea Peterson, "Chinese Cyberspies Have Hacked Middle East Experts at Major U.S. Think Tanks," *Washington Post*, July 7, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/07/07/chinese-cyberspies-have-hacked-middle-east-experts-at-major-u-s-think-tanks/.

[122] Myriam Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," *Science and Engineering Ethics*, vol. 20, no. 3 (2014): 709, https://www.researchgate.net/publication/261997877.

Year	Description
2011	Beginning on June 28, 2011, the World Uyghur Congress experienced a significant Distributed Denial of Service (DDoS) attack to disrupt commemoration events for the second anniversary of the 2009 unrest in Ürümchi. WUC staff created an alternative WordPress site to ensure its events could continue but had to shut that site down after it too faced DDoS attacks. These DDoS attacks forced the WUC website to remain entirely shut down until July 11, nearly one week after the anniversary. In addition to attacks on websites, WUC officers were inundated with spam emails and incoming calls from unidentified numbers to disrupt communications.[123]
2012	In advance of its 2012 Executive Committee meeting, the World Uyghur Congress was one of 10 organizations whose websites were crippled by a virus. WUC servers were also "forced to distribute fake emails targeting activists from related organizations."[124]
2013	In a phishing campaign that lasted at least four years (2009–2013), WUC employees received thousands of emails from compromised email addresses and addresses that otherwise looked familiar. These messages also leveraged familiar themes, languages, and topics to facilitate downloading malware onto WUC devices.[125]

[123] "World Uyghur Congress Facing DDoS Attacks, Electronic Spamming, Telephone Blockade Ahead of July 5, 2009 Anniversary," World Uyghur Congress, July 4, 2011, https://www.uyghurcongress.org/en/world-uyghur-congress-wuc-facing-ddos-cyber-attacks-electronic-spamming-and-telephone-blockade-ahead-of-5-july-2009-anniversary/.

[124] "Hackers Target Uyghur Groups," *Radio Free Asia*, September 6, 2012, https://www.rfa.org/english/news/uyghur/hackers-09062012153043.html.

[125] Engin Kirda, "A Look at Advanced Targeted Attacks Through the Lens of a Human-Rights NGO, World Uyghur Congress," *Lastline*, August 12, 2014, https://www.lastline.com/labsblog/a-look-at-advanced-targeted-attacks-through-the-lense-of-a-human-rights-ngo-world-uyghur-congress/.

2013	Uyghurs involved in advocacy against the Chinese government, including contacts at the WUC, became the victims of a spear phishing campaign designed to install malware on Androids after they received an email sent from the hacked account of a high-level Tibetan activist. The email, concerning details of a WUC conference, was sent to the recipient's entire contact list with an attached file containing malware that would steal and export information from infected devices to an external command and control. Researchers at Kaspersky Labs traced the export to a C2 server located in Beijing.[126]
2019	The World Uyghur Congress Facebook page was attacked by the Diba Central Army, a Chinese nationalist group that has attacked other pages in the past. The WUC page was bombarded with thousands of images—watermarked with the logo of the Diba Central Army—of idyllic life in Xinjiang and posts decrying Uyghurs for being "terrorists."[127]

Table 3: Table of cyberattacks on the World Uyghur Congress between 2011 and 2019. Source: Oxus Society for Central Asian Affairs and World Uyghur Congress.

Muhemmedeli Niyaz, web developer at WUC since 2016, spoke with us about his work securing the organization's website. He noted:

> The main attacks are DDoS, and these usually occur when we host important events or release reports. The website won't open on those days, and we need to work around the clock to keep it

[126] "Chinese Hacking Impact on Human Rights and Commercial Rule of Law," Hearing before the Congressional-Executive Commission on China, 113th Congress, First Session, Washington, D.C., June 25, 2013, https://www.govinfo.gov/content/pkg/CHRG-113hhrg81855/html/CHRG-113hhrg81855.htm; "Researchers Identify Targeted Email Attack Distributing Android Trojan App: A Recent Attack Against Human Rights Activists That Used Android Malware Might be the First of Many," *Network World* via The World Uyghur Congress, March 26, 2013, https://www.uyghurcongress.org/en/researchers-identify-targeted-email-attack-distributing-android-trojan-app-a-recent-targeted-attack-against-human-rights-activists-that-used-android-malware-might-be-the-first-of-many/; Kurt Baumgartner and Danie Maslennikov, "Android Trojan Found in Targeted Attack," SecureList by Kaspersky, March 26, 2013, https://securelist.com/android-trojan-found-in-targeted-attack-58/35552/.

[127] Elizabeth Law, "China's social media 'army' wages war on Uighurs," *Agence France-Presse* via *Hong Kong Free Press*, May 7, 2019, https://hongkongfp.com/2019/05/07/chinas-social-media-troll-army-wages-war-uighurs/.

> online. In more recent years, we have had our Uyghur language YouTube channel hacked to remove content and our organization's Twitter account.

The WUC has also faced phishing attacks that used malware sent through bad links and attachments. Niyaz noted that "these activities place substantial financial burdens on WUC, which has a limited budget."[128]

In 2012 and 2013, researchers at Kaspersky further analyzed the attacks against the World Uyghur Congress, discovering that Uyghur Mac OS X users were vulnerable to malware. Once installed, the malware exploited a backdoor in the Mac OS X operating system that allowed an external command and control center to take control of the device. Analysts successfully decoded the C2 location, which they noted as Lanzhou, China.[129] They further noted that this advanced persistent threat (APT) was intensifying as of their reporting.[130]

Two WUC volunteers reported receiving 1,493 suspicious emails over four years. Of those, 1,116 contained malware attachments. These emails, analyzed in a 2014 Usenix Symposium report "A Look at Targeted Attacks Through the Lens of an NGO," were found to be socially engineered to entice specific individuals into installing malware through the use of familiar names (including compromised email accounts), messages, themes, languages (often the native language of the recipient), and tone. In addition, a reported 84% of the emails were sent from an impersonated sender. Taken together, this email campaign suggests that hackers targeting Uyghur activists focus on socially engineering messages to ensure their

[128] Muhammedeli Niyaz (web developer at WUC), online interview by Bradley Jardine, July 16, 2021.

[129] Costin Rau, "New Mac OS X backdoor variant used in APT attacks," Securelist (blog) by Kaspersky, June 29, 2012, https://securelist.com/new-macos-x-backdoor-variant-used-in-apt-attacks/33214/. A screengrab clearly notes the C2 location as Lanzhou.

[130] Kurt Baumgartner and Costin Rau, "Cyber Attacks Against Uyghur Mac OS X Users Intensify," Securelist (blog) by Kaspersky, February 13, 2019, https://securelist.com/cyber-attacks-against-uyghur-mac-os-x-users-intensify/64259/. Costin Rau, "New Mac OS X backdoor variant used in APT attacks."

receipt so that unwitting recipients will open and download the malicious attachments and install malware onto their computers.[131]

"Communities @ Risk," a 2014 report by the Toronto University-based Citizen Lab, characterized Chinese cyberespionage as persistent, adaptive, and technically unsophisticated but with a high level of social engineering. These phishing schemes and malware packages were of low quality. Still, the attackers went to substantial and persistent lengths to hide their nature: the hackers often embedded the packages in emails made to look like they were coming from known contacts, even from within the organization. Once downloaded, the malware would allow a third party to read keystrokes, download files, and turn on the webcam and microphone of any infected device. The report further underscored that civil-society organizations are particularly vulnerable to this sort of attack, as they have fewer resources to defend themselves than government or commercial-sector actors. As the report notes, these efforts extend the reach of the state into supposed "safe havens."[132] Organizations such as the WUC remain vulnerable to Chinese espionage efforts.

IX. Botnets and Coordinated Social Media Campaigns

Uyghur activists, employees of human rights organizations, and many others who have spoken out about the genocide in the Uyghur Region have become the targets of Chinese government accounts, Chinese bots, and Chinese disinformation, all of which continue to escalate as of the writing of this report.[133] This campaign,

[131] Stevens Le Blond, Adina Uritesc, Cédric Gilbert, Zheng Leong Chua, Prateek Saxena, and Engin Kirda, "A Look at Targeted Attacks through the Lense of an NGO," 23rd USENIX Security Symposium, San Diego, CA, August 20–22, 2014, https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/le-blond.

[132] "Communities @ Risk: Targeted Digital Threats Against Civil Society," Citizen Lab, Munk School of Global Affairs, University of Toronto, November 11, 2014, https://targetedthreats.net/media/1-ExecutiveSummary.pdf, 5.

[133] Albert Zhang and Jacob Wallis, "Strange bedfellows on Xinjiang: The CCP, Fringe Media, and U.S. Social Media Platforms," Australian Strategic Policy Institute, March 30, 2021, https://www.aspi.org.au/report/strange-bedfellows.

waged across social media accounts on Twitter, YouTube, Facebook, and TikTok, seeks to distract from human rights abuses and instead refocus international attention towards positive narratives and outright disinformation. The social media campaign about Xinjiang is the most extensive global propaganda campaign on a single theme that China researchers have seen in the last 25 years, according to University of Canterbury professor Anne-Marie Brady, and is becoming more "dogmatic . . . and aggressive."[134] Researchers at ASPI analyzed this campaign, showing how Chinese government and "fringe media" content is disseminated, shared, and re-shared thousands of times across hundreds of accounts on Twitter and Facebook in a push to discredit statistics and factual information about the human rights abuses in the XUAR, discredit Western media and human rights organizations, and assert Chinese government claims. Several organizations funded by the Xinjiang Audio-Video Publishing House under the United Front Work Department have made videos of Uyghurs who have been "re-educated" and "rehabilitated" back into the society, including footage extolling the virtues of the CCP in XUAR.[135]

In 2019, Chinese government-aligned trolls attacked the Talk to East Turkestan Facebook page, run by Arslan Hidayat. Within an hour, Hidayat's page had received over 1,400 comments promoting sanitized images of Xinjiang and decrying all Uyghurs for being "terrorists" and "no different than ISIS." The hacker group, Diba Central Army, is thought to be part of China's 50 Cent Army of trolls.[136] These trolls—whom many observers suspect to be government employees in a variety of positions and departments—are leveraged by the Chinese government to promote Chinese state narratives and propaganda; to cheerlead fellow trolls, bots,

Uyghur activists, human rights organizations, and many others who have spoken out about the genocide in the Uyghur Region have become the targets of Chinese government accounts, Chinese bots, and Chinese disinformation, all of which continue to escalate as of the writing of this report.

[134] "China Tries to Counter Xinjiang Backlash With… A Musical?" *New York Times*, April 5, 2021, https://www.nytimes.com/2021/04/05/world/asia/china-uyghurs-propaganda-musical.html.

[135] Zhang and Wallis, "Strange Bedfellows," 6–7. See also "'The Happiest Muslims in the World': Disinformation, Propaganda, and the Uyghur Crisis," Uyghur Human Rights Project, July 28, 2020, https://uhrp.org/report/uhrp-report-happiest-muslims-world-disinformation-propaganda-and-uyghur-crisis-html/.

[136] Strittmatter, *We Have Been Harmonized*, 72.

diplomats, and nationalist "netizens"; and to distract from stories that might be dangerous to the government.[137]

In 2021, *Reuters* revealed that Chinese hackers had used Facebook to target Uyghurs abroad. Using fake accounts, the group of hackers infiltrated Uyghur groups online and developed trust with them before sharing links to fake and corrupted sites embedded with malware. Once an individual in the group clicked on these links, the links downloaded malware onto that individual's platform. Part of a group called Evil Eye, these hackers also developed websites specifically tailored to a Uyghur audience meant to look like Android apps that had malware connected to them. Nearly 500 Uyghurs from Turkey, Kazakhstan, the United States, Australia, Canada, and Syria were targeted in this campaign. In response, Facebook removed the group of hackers from the website and blocked all of the corrupted and fake domains.[138] However, Facebook continued to allow China to run advertisements on its platform that denied the genocide in the Uyghur Region.[139]

Facebook appears to have knowledge of Chinese government-led targeting of Uyghurs on its platform. In October 2021, Facebook whistleblower Frances Haugen noted in her testimony to the Senate Commerce Committee's Subcommittee on Consumer Protection, Product Safety, and Data Security that the Chinese government regularly used Facebook as a tool by the Chinese government to surveil Uyghurs around the world. She noted that Facebook is aware of this and other espionage activities, but that the

---

[137] Elizabeth Law, "China's social media 'army wages a war on Uighurs," *Hong Kong Free Press*, May 7, 2019, https://hongkongfp.com/2019/05/07/chinas-social-media-troll-army-wages-war-uighurs/; Henry Farrell, "The Chinese government fakes nearly 450 million social media comments a year, this is why," *Washington Post*, May 19, 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/; Kaveh Wadell, "'Look, a Bird!' Trolling by Distraction," *Atlantic*, January 27, 2017, https://www.theatlantic.com/technology/archive/2017/01/trolling-by-distraction/514589/.

[138] Elizabeth Culliford and Raphael Satter, "Chinese hackers used Facebook to target Uighurs abroad, company says," *Reuters*, March 24, 2021, https://www.reuters.com/article/us-facebook-china-cyber/chinese-hackers-used-facebook-to-target-uighurs-abroad-company-says-idUSKBN2BG2UU.

[139] Isobel Asher Hamilton, "Facebook is letting China run state ads denying the abuse of Uyghur Muslims in Xinjiang, and staffers are reportedly raising concerns internally," *Business Insider*, April 6, 2021, https://www.businessinsider.com/facebook-internal-tension-china-xinjiang-ads-adverts-uyghurs-2021-4.

counterespionage team has been consistently understaffed by the company.[140]

In contrast to Facebook, Twitter has sought to push back on China's use of its platform as a tool of harassment. Twitter listed some accounts as foreign state actors and permanently banned them from the website: in 2020, the company de-platformed 23,750 core accounts that generated content to be retweeted, as well as an additional 150,000 accounts run by bots and trolls.[141]

The near-constant harassment, intimidation, and coercion outlined in this section have a devastating effect on Uyghurs individually, as well as in diaspora communities. However, data we collected suggests that this pressure placed on Uyghurs by the Chinese government galvanized a response: 34.4% of the Uyghurs we surveyed—a majority of our respondents—have begun to speak out *after* facing the Chinese government's coercion and harassment. This indicates that Chinese transnational repression drives some Uyghurs towards political activism rather than coercing them into silence.

Uyghurs abroad are a vulnerable population whose members have relied on technology to maintain contact with home while attempting to establish new lives abroad, leaving them open to intimidation, harassment, and coercion from their home country.

[140] Caitlin Hu, "'Terrifying': Facebook whistleblower cites violence in Myanmar and Ethiopia, spying by China and Iran," *CNN*, October 6, 2021, https://amp.cnn.com/cnn/2021/10/05/world/meanwhile-in-america-oct-6-intl/index.html; Sheera Frenkel, "Whistle-Blower Warns of Foreign Influence on Facebook" (video), *New York Times,* October 5, 2021, https://www.nytimes.com/2021/10/05/technology/what-happened-at-facebook-whistleblower-hearing.html.

[141] Kate Conger, "Twitter Removes Chinese Disinformation Campaign," *New York Times,* June 11, 2020, https://www.nytimes.com/2020/06/11/technology/twitter-chinese-misinformation.html.

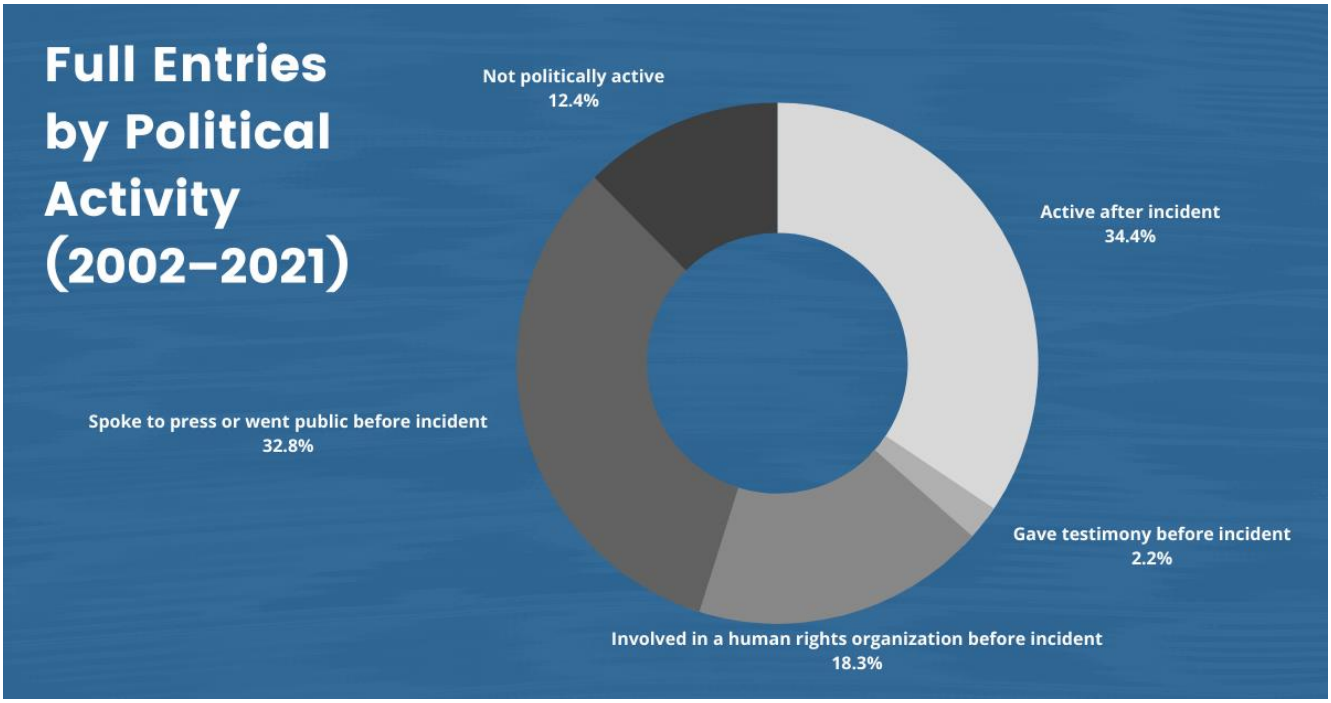

Image 10. Full Entries by Political Activity (2002–2021). This chart represents the political activities of the 186 Full Entries incidents recorded in the dataset. More detailed information about the incidents in question allowed us to determine when and how Uyghurs decided to become politically active (including speaking to the press). Source: Oxus Society for Central Asian Affairs.

X. Conclusion

Uyghurs abroad are a vulnerable population whose members have relied on technology to maintain contact with home while attempting to establish new lives abroad. Sadly, their desire to maintain contact with home has left them open to intimidation, harassment, and coercion by the Chinese state. Our dataset records 5,530 cases of stage 1 transnational repression in which the Chinese government has used intimidation and harassment to target, monitor, and silence Uyghurs abroad. These efforts act as an extension of China's surveillance and censorship regime within the borders of the Uyghur Region. Moreover, they directly infringe upon the rights of Uyghurs living abroad by denying them the right to free speech and the right to assembly—values enshrined in liberal democratic constitutions that are meant to be shared by all.

The regime of surveillance, data collection, harassment, and intimidation we have outlined in this report can—and often do—

breed fear. From its inception, the internet was intended to be a place of freedom, liberty, and exchange; it has also become a tool of authoritarian states. The internet allows such states to extend their reach, surveil actors both within and beyond their sovereign borders, and engage in online harassment. Indeed, as protesters and organizers have moved their operations online, so too have the governments they seek to oppose. This shift has resulted in self-censorship, the direct censorship of individuals, and a tremendous emotional toll on those individuals impacted by transnational repression. The freedoms of people subject to clandestine data collection and surveillance are at risk, as is the Internet's overall capacity as a space for freedom of expression. As autocrats and leaders of illiberal regimes around the world learn from one another and acquire technologies to surveil individuals, control their access to information, manipulate their ability to express themselves, and turn personal data against them in systems that categorize and rank people, the Internet may become an increasingly restricted space.

Moreover, online harassment and other cyber threats have real-world consequences, with some Uyghurs in countries such as the United States refusing to participate in protests for fear of repercussions. But it is not just Uyghurs who are at risk. Our study indicates that citizens of other states who speak out on behalf of the Uyghurs are also being monitored and harassed, potentially increasing the span of self-censorship and fear of public engagement. Thus, governments must move to secure the rights of their citizens and residents if they are to resist democratic backsliding brought on by an onslaught of 21st-century transnational repression.

Our previous studies indicate that this transnational repression is becoming all-too-common. Since 1997, 427 Uyghurs worldwide have been deported or extralegally rendered from their host country back to China; 146 of these deportations have occurred since 2017 alone. An additional 1,149 Uyghurs have been detained in their host country, with 582 detentions occurring since 2017.[142] These numbers only represent known cases; there are likely many more that have

[142] "China's Transnational Repression of Uyghurs Dataset," The Oxus Society for Central Asian Affairs, last accessed on August 8, 2021, https://oxussociety.org/viz/transnational-repression/; Lemon and Jardine, "No Space Left to Run."

not been reported. This alarming fact clarifies the need for better protection against transnational repression worldwide.

XI. Policy Recommendations

Based on the findings of this report, we recommend that democratic states and international organizations take the following steps to counter China's use of transnational repression around the world:

Recommendations for Civil Society and the Private Sector

- **Refugee case managers should work with Uyghurs on digital safety**. Case managers are trusted sources for refugees and could serve as a resource for technical knowledge and assistance on privacy.
- **Private-sector digital platforms should monitor threats** in all relevant languages, including Uyghur, Chinese, Turkish, and others; develop tools to identify state-actor harassment; and make secure communication platforms available in relevant languages.
- **Developers should implement strict rules and independent oversight to bring transparency and accountability to the market for spyware**. Companies should ensure that they fully comply with all laws and regulations throughout the entire chain of development, and sales and export licenses should be made conditional upon independent human rights review. Government use of surveillance technology needs to be subject to public debate and critical investigation, and there must be mechanisms for international sanctions and redress in cases of abuse. Companies providing surveillance tools that are used to target and surveil Uyghurs, and therefore infringe on their rights, should be named and shamed, and their deceptive practices targeted by strategic litigation.

Recommendations for National Policy

- **Increase refugee quotas.** Uyghur refugees in third countries of transit such as Turkey, Pakistan, and Central Asia are at risk of being rendered back to China and must be protected.
- **Create a dedicated refugee resettlement program for Uyghurs.** Governments should establish safe pathways for Uyghurs outside China to apply for resettlement without the need for UNHCR processing.
- **Expedite the processing of documentation for Uyghurs.** Many Uyghurs find themselves trapped as stateless persons, without sufficient documentation to get a job or to send their children to school. Expediting the asylum applications of Uyghurs should be a priority.
- **Impose targeted sanctions on Chinese citizens responsible for acts of transnational repression.** International sanction mechanisms such as the Global Magnitsky Act should be triggered in response to the grave human rights violations carried out by China against the Uyghur diaspora. By triggering these provisions, key groups and security personnel perpetrating these crimes can have their assets frozen and travel restricted.
- **Continue to speak publicly, with allies, about transnational repression.** Raising awareness of the threat transnational repression poses to national sovereignty and to the human rights of targeted individuals is critical to formulating a coalition and a coherent multilateral response in forums such as Interpol and the UN.
- **Continue to selectively ban technology exports to China.** Previous efforts by democratic governments to ensure that technology used to code Uyghur DNA, surveil Uyghurs, and otherwise contribute to the human rights violations taking place in the Uyghur Region have been successful. However, as more technologies become available, preventing their use in these human rights violations is paramount.

Recommendations for International Community

- **The UN High Commissioner for Refugees (UNHCR) should improve digital security among INGOs that work with refugees.** INGOs are entrusted with refugees' personal information. It is critical that this information be protected and remain confidential. Unfortunately, current procedures and policies do not necessarily guarantee those protections.
- **Include digital rights in discussions of international human rights.** Discussions on the civil liberties and rights of refugees and persecuted minorities should include discussions of their digital rights: freedom from surveillance, intimidation, and harassment, and freedom of speech and expression. Discussions of digital rights should be focused on the voices of Uyghurs and include the toll that harassment, intimidation, and coercion take on their lives.
- **Like-minded countries should work together to create a unified vision of democratic digital governance.** This vision, in tandem with policy language and objectives, will better protect the digital rights and human security of vulnerable populations, as well as the global community.[143]
- **Create an international convention on transnational repression** that calls for an end to all acts of transnational repression, including intimidation and harassment, arrests, and deportations.

[143] Adapted from Steven Feldstein's recommendations in *The Rise of Digital Repression* (New York: Oxford University Press, 2020).

1602 L Street NW | Washington, DC 20036
+1.202.478.1920 | www.uhrp.org | info@uhrp.org

www.oxussociety.org | info@oxussociety.com