Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**687**
Land:	Kina
Kilde:	Immigration and Refugee Board of Canada
Titel:	China: Monitoring of Chinese citizens outside of China, including Falun Gong Falun Dafa) practitioners, by Chinese authorities; consequences upon return to China (2020-September 2022)
Udgivet:	12. oktober 2022
Optaget på baggrundsmaterialet:	6. november 2023

Responses to Information Requests

Responses to Information Requests (RIR (Responses to Information Request)s) are research reports on country conditions. They are requested by IRB decision-makers.

The database contains a seven-year archive of English and French RIR (Responses to Information Request)s. Earlier RIR (Responses to Information Request)s may be found on the European Country of Origin Information Network website.

Please note that some RIR (Responses to Information Request)s have attachments which are not electronically accessible here. To obtain a copy of an attachment, please e-mail us.

Related Links

- Advanced search help

▶ Disclaimer

12 October 2022

CHN201173.E

China: Monitoring of Chinese citizens outside of China, including Falun Gong (Falun Dafa) practitioners, by Chinese authorities; consequences upon return to China (2020–September 2022)
Research Directorate, Immigration and Refugee Board of Canada

1. Monitoring of Chinese Citizens Outside of China by

Chinese Authorities

A Freedom House case study analysis of China's "transnational repression" provides the following information:

China conducts the most sophisticated, global, and comprehensive campaign of transnational repression in the world. Efforts by the Chinese Communist Party (CCP) to pressure and control the overseas population of Chinese and members of minority communities are marked by three distinctive characteristics. First, the campaign targets many groups, including multiple ethnic and religious minorities, political dissidents, human rights activists, journalists, and former insiders accused of corruption. Second, it spans the full spectrum of tactics: from direct attacks like renditions, to co-opting other countries to detain and render exiles, to mobility controls, to threats from a distance like digital threats, spyware, and coercion by proxy. Third, the sheer breadth and global scale of the campaign is unparalleled. Freedom House's conservative catalogue of direct, physical attacks since 2014 covers 214 cases originating from China, far more than any other country.

…

[T]he CCP targets entire ethnic and religious groups, including Uighurs [Uyghurs], Tibetans, and Falun Gong practitioners, which together number in the hundreds of thousands globally. … the list of targeted populations has expanded to also include Inner Mongolians and Hong Kongers residing outside the People's Republic of China (PRC). (Freedom House Feb. 2021, 15–16)

According to a book on China's global influence and surveillance efforts abroad by Joanna Chiu—a senior reporter at the *Toronto Star* who focuses on China—Chinese authorities "feel anyone of Chinese descent is fair game and that they have a right to curtail their freedom of speech years or even generations after they settled abroad" (Chiu 2021, 102, 369). In correspondence with the Research Directorate, an assistant professor at Simon Fraser University in British Columbia, whose

research interests include Chinese technological surveillance and China's governance of Uyghur people, stated that citizens outside of China belonging to "targeted ethnic groups," and especially Uyghurs and Tibetans, as well as "political and religious minorities such as Hong Kong democracy advocates and members of Falun Gong" are all of "general interest" to authorities (Assistant Professor 29 Sept. 2022). The same source added that within those groups, people "active in public protests and social media protest campaigns" are of notable interest (Assistant Professor 29 Sept. 2022). In an interview with the Research Directorate, a senior lecturer at the University of Adelaide in Australia, who has conducted research on the United Front Work Department (UFWD) [1], similarly indicated, regarding Chinese citizens outside of China, that the authorities are interested in Uyghurs, Tibetans, and activists of Taiwan or Hong Kong causes, regardless of the individual's rank or public-facing nature (Senior Lecturer 3 Oct. 2022). However, the same source added that unlike a higher rank Falun Gong member, such as a recruiter, promoter or other public-facing person, the authorities are not "too concerned" with ordinary Falun Gong members (Senior Lecturer 3 Oct. 2022).

A 2020 Human Rights Watch (HRW) report states that authorities "routinely threaten" the relatives in China of "dissidents abroad" in an effort to "silence their criticisms" (HRW 14 Jan. 2020, 15). A *New York Times* article—based on Chinese government procurement documents, police manuals, interviews, and information received from a government contractor "working on overseas internet investigations"—states that authorities are "harassing critics" in China and abroad with "growing frequency," including "threatening relatives" to encourage them to "delete content deemed criminal" (*The New York Times* 31 Dec. 2021).

According to the Assistant Professor, surveillance is focused on countries with a large population of "'dissidents'": Turkey, Kazakhstan, Germany and the US are of particular interest due to the presence of

Uyghur and Kazakh population; Washington, DC is another location of interest since it is the "headquarters of Falun Gong and Tibetan institution building activities"; London, San Francisco and Vancouver are also of interest due to the presence of the Hong Kong diaspora (Assistant Professor 29 Sept. 2022). The same source further noted that in Canada, Chinese authorities are "most focused" on places with a large Chinese population, such as Vancouver and Toronto (Assistant Professor 29 Sept. 2022).

1.1 Institutional Framework

The Freedom House report provides the following information about the Chinese state apparatus tasked with monitoring targeted citizens abroad:

> The harshest forms of direct transnational repression from Chinese agents—espionage, cyberattacks, threats, and physical assaults—emerge primarily from the CCP's domestic security and military apparatus: agencies like the Ministry of State Security (MSS), the Ministry of Public Security (MPS), and the People's Liberation Army (PLA), although the precise division of labor among these entities is often unclear. Persecution of Uighurs, Tibetans, and political dissidents is typically managed by the MSS, but MPS is often involved in threats against family members within China, or cases where regional authorities call exiles to threaten them from within China … . Hackers from the [PLA] run spyware campaigns from within China. (Freedom House Feb. 2021, 16, footnotes omitted)

According to Chiu, China's Public Security Bureaus (PSBs) occasionally work with the UFWD to monitor Chinese citizens living overseas, while the Ministry of State Security secret police will usually do so for "higher-profile cases" (Chiu 2021, 99). The Assistant Professor noted that the UFWD and Chinese embassies are involved in the surveillance of overseas Chinese citizens (Assistant Professor 29 Sept. 2022).

The Freedom House report provides the following information:

China's overt transnational repression activities are embedded in a broader framework of influence that encompasses cultural associations, diaspora groups, and in some cases, organized crime networks, which places it in contact with a huge population of Chinese citizens, Chinese diaspora members, and minority populations from China who reside around the world. (Freedom House Feb. 2021, 16)

The Freedom House report indicates that "United Front work" abroad is partly coordinated by the UFWD and includes "regional diaspora associations, student groups, and scholarly bodies that officially represent specific regions of China abroad" (Freedom House Feb. 2021, 17).

According to Chiu, in 2016 the CCP added a new bureau to the UFWD called the New Social Classes Work Bureau (Chiu 2021, 99). The same source cites the UFWD chairwoman as stating that this bureau would "target" the following groups: "professionals in private and foreign-owned enterprises; people working in NGOs, including lawyers and accountants; 'new media' professionals (those working for online news sources); and returning Chinese overseas students" (Chiu 2021, 99).

1.2 Surveillance and Monitoring Tools

1.2.1 Social Networks

The Assistant Professor indicated that there are Chinese informants in "major institutions," such as universities, in "most" North American and European countries (Assistant Professor 29 Sept. 2022). However, the same source further noted that "some" informants are "unaware" that they are acting as informants (Assistant Professor 29 Sept. 2022). The Senior Lecturer indicated that United Front groups can identify an individual's friends and coopt the friend into becoming an "unwitting accomplice" of monitoring (Senior Lecturer 3 Oct. 2022).

1.2.2 Hacking, Including Use of Spyware

The *New York Times* indicates that Chinese security authorities are committing "new technical expertise and funding" to monitoring Chinese citizens of interest abroad (*The New York Times* 31 Dec. 2021). The Freedom House report notes that Chinese authorities can conduct "sophisticated hacking and phishing attacks" (Freedom House Feb. 2021, 16). The Assistant Professor indicated that the authorities use "spyware and other forms of hacking" against "particular individuals who are explicitly targeted by Chinese authorities" (Assistant Professor 29 Sept. 2022).

A 2019 blog post by Volexity—a US-based company specializing in cybersecurity threat analysis and prevention (Volexity n.d.)—on surveillance efforts against Uyghur people, indicates that this surveillance occurs beyond China's borders as well, and has "fully entered the digital realm" and "cyberspace" (Volexity 2 Sept. 2019). The same source identifies "at least 11 Uyghur and East Turkestan [Xinjiang] related websites"—comprising a "significant" percentage of the total websites providing Uyghur and East Turkestan information—that have been "compromised and leveraged for surveillance and exploitation" by measures including the insertion of "malicious code" (Volexity 2 Sept. 2019). The same report states that some of this "malicious code" was intended to "target" Android mobile users and the personal email accounts of Gmail users (Volexity 2 Sept. 2019). The 2019 Volexity report indicates that because all of the targeted websites are blocked inside China, "it can be seen that the Uyghur diaspora" abroad are the "primary targets of these digital surveillance operations," which "can be used to track the movements of Uyghurs outside of China and spy on those they are communicating with" (Volexity 2 Sept. 2019).

A 2019 article by TechCrunch [2] further reported on a Google security discovery of a group of "malicious websites" "targeting Uyghur Muslims" which were "used to hack into iPhones over a two-year period";

the article cites unnamed sources who state that the "websites were part of a state-backed attack" "likely [perpetrated by] China" (TechCrunch 31 Aug. 2019). A 2019 article by *Forbes*, an American business magazine, which also builds on Google security's discovery of these websites, as well as on TechCrunch's reporting that the websites targeted Uyghurs, cites unnamed sources who indicate that "Google's and Microsoft's operating systems were targeted via the same websites that launched the iPhone hacks" (*Forbes* 1 Sept. 2019).

A 2019 report on the online monitoring of Tibetan groups by Citizen Lab, an "interdisciplinary laboratory" based at the Munk School of Global Affairs and Public Policy at the University of Toronto that analyzes the privacy and security of popular applications, indicates that a campaign with "similarities" to those found by Google and Volexity which "target[ed] Uyghur groups" was also launched to "exploit and install spyware on iPhone and Android devices" belonging to "Tibetan groups" (Citizen Lab 24 Sept. 2019, 3, 6, 7). The same report adds that the "exploits, spyware, and infrastructure" used in the effort targeting the Tibetan groups "link it" to the previously identified "digital espionage campaigns targeting Uyghur groups," and the "similarities" between the campaigns makes "it likely [they] were "conducted by the same operator, or a coordinated group of operators, who have an interest in the activities of eth[nic] minority groups that are considered sensitive in the context of China's security interests" (Citizen Lab 24 Sept. 2019, 7).

A 2020 report by the Threat Intelligence team of Lookout—a cybersecurity company specializing in mobile security (Lookout June 2020, 37)—provides the following information:

The Lookout Threat Intelligence team has discovered four Android surveillanceware tools, which are used to target the Uyghur ethnic minority group. Our research indicates that these four interconnected malware tools are elements of much larger mAPT (mobile advanced persistent threat) campaigns that have been active for years. Although

there is evidence that the campaigns have been active since at least 2013, Lookout researchers have been monitoring the surveillanceware families — SilkBean, DoubleAgent, CarbonSteal and GoldenEagle — as far back as 2015.

…

Lookout researchers have evidence to suggest that while the main target of this activity is indeed the Uyghur ethnic minority in China, these tools have also been used to target Uyghurs living outside China, Tibetans, and Muslim populations around the world.

Titles and in-app functionality suggest targets speak a variety of languages including: Uyghur (in all its four scripts: Arabic, Russian, Uyghur Cyrillic and Chinese), English, Arabic, Chinese, Turkish, Pashto, Persian, Malay, Indonesian, Uzbek and Urdu/Hindi. (Lookout June 2020, 3)

1.2.3 Chinese Social Media

The Freedom House report notes that

[o]ne of China's newest avenues for deploying repressive tactics overseas has been via the WeChat platform, a messaging, social media, and financial services app that is ubiquitous among Chinese users around the world, and through which the party-state can monitor and control discussion among the diaspora. (Freedom House Feb. 2021, 16)

According to a 2020 report by Citizen Lab, WeChat (*Weixin*) accounts which were first registered to a mainland Chinese phone number [China-registered account] continue to operate under WeChat China's terms of service, even if the user later links their account to a non-Chinese phone number (Citizen Lab 7 May 2020, 8). The same report notes that files and communications sent to, or from, WeChat

accounts registered to a mainland Chinese phone number are "assessed for political sensitivity[,] among other content categories" (Citizen Lab 7 May 2020, 8).

Sources indicated that Chinese authorities monitor WeChat (Senior Lecturer 3 Oct. 2022) or can access data on WeChat (Assistant Professor 29 Sept. 2022). The 2020 Citizen Lab report indicates that WeChat China, which oversees China-registered accounts, and WeChat International, which administers non-China-registered accounts, "acknowledge that they may share information with law enforcement organizations under certain conditions" (Citizen Lab 7 May 2020, 34). The same source adds that WeChat China "strongly implied" that it would disclose private user information to law enforcement organizations, but did not specify whether a court order was required in such cases or if law enforcement organizations nationwide were entitled to such information (Citizen Lab 7 May 2020, 34). The same report states that WeChat International's privacy protection summary notes that it would provide user information to authorities when it is required to do so by a legal process, and the report indicates that WeChat International "did not commit" to informing users when making such disclosures to authorities (The Citizen Lab 7 May 2020, 34).

According to the 2020 Citizen Lab report, documents and images that are shared "among non-China-registered accounts are subject to content surveillance" (Citizen Lab 7 May 2020, 6).

1.2.4 International Social Media

The Assistant Professor indicated that Chinese authorities use "data-scraping and analysis tools" to monitor Chinese citizens' social media activities on non-Chinese applications, such as Facebook (Assistant Professor 29 Sept. 2022). The *New York Times* article states that Chinese authorities have harnessed "sophisticated technological methods" equipping them to "expand [their] reach" and "list of targets,"

and to "unmask and silence" critics who are using international social media platforms including Twitter and Facebook (*The New York Times* 31 Dec. 2021). The same source adds that these methods include the use of "advanced investigation software, public records and databases to find [targets'] personal information and international social media presence," and notes that these operations sometimes focus on Chinese citizens abroad and "minor critics" (*The New York Times* 31 Dec. 2021).

The *New York Times* article, citing a [Chinese] government contractor—a "specialist in tracking people living in the United States"—indicates that a surveillance investigation against a person often begins after they have posted a "single tweet or Facebook post" that draws official attention (*The New York Times* 31 Dec. 2021). The contractor, the same source states, will then use voter registries, driver's license records, and "hacked databases on the dark web to pinpoint" the source of the posts, and adds that personal photographs available online can help determine relevant addresses and friends (*The New York Times* 31 Dec. 2021).

The same article provides the following information:

> A Chinese police manual and examination for online security professionals detailed and ranked the types of speech crimes that investigators seek out, labelling them with a one, two or three depending on the severity of the violation. One denotes criticism of top leadership or plans to politically organise or protest; two includes the promotion of liberal ideology and attacks on the government; and three, the least urgent, refers to content ranging from libel to pornography. The manual specifically called for monitoring activity on foreign websites.
>
> The contractor said he used the rankings to classify infractions on dossiers he submitted to his bosses in China's security apparatus. In a sample document reviewed by [t]he *Times*, he listed key details about each person he looked into, including personal and career information and professional and family connections to China, as well as a statistical

analysis of the reach of the person’s account. His approach was corroborated by procurement documents and guides for online security workers.

Over the past year, he said, he had been assigned to investigate a mix of Chinese undergraduates studying in the United States, a Chinese American policy analyst who is a US citizen and journalists who previously worked in China. (*The New York Times* 31 Dec. 2021)

1.3 Monitoring of Chinese Citizen Falun Gong Members Outside of China by Chinese Authorities

The Senior Lecturer noted stated that Falun Gong members who publicly proselytize or discuss the *Nine Commentaries on the Communist Party* [3] will attract the attention of Chinese authorities (Senior Lecturer 3 Oct. 2022). The Assistant Professor indicated that overseas Falun Gong practitioners, "particularly" individuals involved in "protest and media activities," are monitored by Chinese authorities (Assistant Professor 29 Sept. 2022).

According to the Freedom House report, Chinese state campaigns focused on Falun Gong practitioners abroad are steered by the "6-10 Office, an extralegal security agency tasked with suppressing banned religious groups," as well as by the MPS, although "local officials from various regions are also involved in monitoring Falun Gong exiles from their provinces" (Freedom House Feb. 2021, 16, footnote omitted).

1.4 Incidents of Surveillance and Monitoring

Chiu describes the situation of a Chinese student at a Canadian university, who, from within China, used access to a virtual private network provided by his university to create a Twitter account using a fake name, fake location, and setting his gender to female, and who, once within Canada, retweeted three posts using the account—one about the death of a Chinese democracy advocate, one satirizing

Chinese President Xi Jinping, and one displaying information about Chinese government corruption; the student was later contacted by his father who told him that the PSB called his parents twice on the telephone (Chiu 2021, 97–100). Chiu also reports that soon after, a police officer contacted the student using the social media app WeChat and stated to him that the MPS tracked him through his IP address, was aware of his address in Canada, and had evidence of his association to his Twitter account (Chiu 2021, 100).

According to the *New York Times* article, a Chinese student living in Australia, who created a Twitter account parodying Chinese leader Xi Jinping, received a call placed by the Chinese police from her hometown, who used her father's telephone (after he had been summoned to a local police station) to inform her that they were aware that her Twitter account was being operated from Australia (*The New York Times* 31 Dec. 2021). Three weeks later, the same source adds, the student's father was again summoned by police who then used video chat to contact the student and tell her that she was to report to the police station upon her return to China and to ask her about the remaining validity of her Australian visa (*The New York Times* 31 Dec. 2021). The student, the article indicates, notes that "the police harassment has continued" despite her relocation to Europe to study (*The New York Times* 31 Dec. 2021).

The information in the following paragraph was provided in a US Department of Justice press release:

One US citizen and four officials belonging to China's MSS were charged in an indictment "with conspiracy and other charges related to an espionage and transnational repression scheme" "in the US and abroad." The US citizen, surnamed Wang, is a "well-known academic and author who helped start a pro-democracy organization in Queens[, New York,] that opposes the current communist regime in China"; "as alleged, since at least 2011, Wang has used his position and status within the Chinese diaspora and dissident communities to covertly collect

information about prominent activists and human rights leaders on behalf of the MSS and PRC." The four MSS officials "acted as Wang's handlers, directing Wang to target specific individuals and groups that the PRC considers subversive, such as Hong Kong pro-democracy activists, advocates for Taiwanese independence, and Uyghur and Tibetan activists, and obtain information on particular topics and matters of importance to the MSS." Wang delivered information to the MSS through "encrypted messaging applications and emails," as well as during in-person meetings in China, and this information included details about Wang's "private conversations with prominent dissidents, as well as the activities of pro-democracy activists and human rights organizations." "At least one Hong Kong democracy activist and dissident" about whom Wang reported details to the MSS was "subsequently arrested by the PRC." Wang provided the MSS with the telephone numbers and contact information of "Chinese dissidents" (US 18 May 2022).

The *New York Times* article indicates that the parents of a Chinese student living in Taiwan who "criticised China" "disappeared for 10 days"; following their reappearance, the student, who also had his Chinese social media accounts shut down, remained unaware of what happened to his parents, and had not asked them because he learned that "local security forces" continued to "monito[r] them" (*The New York Times* 31 Dec. 2021).

According to a 2019 article by the *Washington Post*, ahead of a talk by a Uyghur activist at McMaster University about the internment of Muslims in China's northwest, a group of Chinese students reached out to the Chinese embassy; the embassy asked the students to attend the event and "see whether university officials attended and whether Chinese nationals had organized the talk" (*The Washington Post* 14 Feb. 2019). The same source adds that the students also sent photos of the event to Chinese officials (*The Washington Post* 14 Feb. 2019).

The HRW report cites a Vancouver resident who states that if they were to criticize the CCP publicly, their parents' retirement or health insurance benefits could be stripped, as well as a Toronto-based journalist for a Chinese-language newspaper who noted her parents had been "harassed" because of her work (HRW 14 Jan. 2020, 15). According to the mayor of Port Coquitlam in British Columbia, as cited by Chiu, "dozens of his constituents"—"mostly first- or second-generation immigrants from China"—had received "threatening phone calls and … [in some cases] in-person visits from Chinese government officials" who "expressed anger" over social media posts or attendance at certain events (Chiu 2021, 102–103). Sources indicate that, while attending a January 2020 [or January 2019 (Chiu 2021, 103)] conference in Vancouver, the executive director of the Alliance Canada Hong Kong advocacy group received a phone call to her hotel room stating that people were coming to get her (Chiu 2021, 103; CBC 10 Sept. 2020; CTV 24 Apr. 2021), and "demanding" that she "leave immediately" (Chiu 2021, 103; CBC 10 Sept. 2020).

2. Extradition Campaigns

The Freedom House report notes that China uses its "geopolitical and economic clout" to pressure foreign governments to use their own security forces to detain and "in some cases" deport to China party critics, "targeted ethnic or religious minorities" and refugees (Freedom House Feb. 2021, 17, footnotes omitted). According to a report by Safeguard Defenders [4] on Chinese extradition campaigns against targeted citizens abroad, Operation Fox Hunt—described by authorities as a campaign to return fugitives to China to face criminal charges—those recruited for "targeting and tracking suspects" are

hired from around China, with priority given to men in their 30s, many recruited from the MPS' Arrest and Investigation Team of Economic Investigation Bureau. In total, there are around 20 members. Hunters are required to be skilled in investigation, law, and foreign languages; have a

high EQ, IQ and the ability to deal with emergencies and risky situations. They are generally well educated, most with masters' degrees and a multidisciplinary background in finance, economics, foreign languages, law, computers, business management, or criminal investigation. (Safeguard Defenders Feb. 2022, 38, footnote omitted)

An article by *Global Times*, a Chinese state-run newspaper (*The Guardian* 16 Dec. 2021), states that in April 2015 China launched "Sky Net operation" and that a statement by the Central Commission for Discipline Inspection (CCDI) of the CCP indicates that the operation is designed to "capture corrupt officials, crack down on fake passports, bust underground banks, recover assets involved in criminal cases and persuade fugitive suspects to return home" (*Global Times* 27 Mar. 2015). The same article indicates that the Fox Hunt campaign would continue under the Sky Net operation, and the MPS' oversight (*Global Times* 27 Mar. 2015).

A report by Safeguard Defenders on Chinese transnational policing indicates, citing a January 2022 announcement from the Director of the Overseas Chinese Police Office in Fuzhou City, that the Fuzhou PSB launched 30 overseas police service stations in 25 cities in 21 countries and, according to the report, 3 of these stations are in Toronto (Safeguard Defenders 12 Sept. 2022, 10, 13). Citing an article from the authorities, the report notes that the overseas police stations are involved in "'persua[ding]'," through direct contact, targeted overseas Chinese citizens to return to China (Safeguard Defenders 12 Sept. 2022, 12). However, the *Globe and Mail*, who visited the three Toronto addresses listed for the overseas police stations, notes that the locations were respectively a private home, a mall with Chinese businesses and a business park owned by a federally incorporated non-profit organization called the Canada Toronto FuQing Business Association (*The Globe and Mail* 21 Sept. 2022).

3. Consequences Upon Return

According to the Assistant Professor, the treatment of the individual upon return varies depending on their "social position" (Assistant Professor 29 Sept. 2022). The same source explained that if the individual belongs to the majority Han ethnicity and has "politically powerful" social connections, they "may" face interrogation and be given a "warning"; however, Muslims, Falun Gong members and Hong Kong democracy organizers will not have these "protections" "in the vast majority of cases" and are "likely" to be detained upon arrival (Assistant Professor 29 Sept. 2022).

The Senior Lecturer indicated that the treatment upon return depends on the returnee's location, the conditions of their hometown, as well as the policies at the time (Senior Lecturer 3 Oct. 2022). The same source added that individuals who are "more obviously" engaged in activities abroad are "more likely" to face retribution upon return; however, it is difficult to determine a "clear cut 'cause and effect'" in terms of punishment (Senior Lecturer 3 Oct. 2022).

Axios, a news website (Axios n.d.), citing Chinese court documents, notes that a University of Minnesota student was sentenced to six months in prison when he returned to China for posting caricatures of Xi Jinping on Twitter (Axios 22 Jan. 2020).

This Response was prepared after researching publicly accessible information currently available to the Research Directorate within time constraints. This Response is not, and does not purport to be, conclusive as to the merit of any particular claim for refugee protection. Please find below the list of sources consulted in researching this Information Request.

Notes

[1] The United Front Work Department (UFWD) is an official state agency that is "primarily focused on influencing civilians and civil society organizations around the world to try to shape these individuals' and groups' attitudes toward Beijing" (Chiu 2021, 74, 76).

[2] TechCrunch is a technology media organization (Business Wire 20 Sept. 2021).

[3] *The Nine Commentaries on the Chinese Communist Party* is a book criticizing the party written by the Falun Gong organization and published by the *Epoch Times*, an international media company and publication founded in the US by practitioners of Falun Gong; however, the *Epoch Times* denies its ties with Falun Gong (openDemocracy 10 Mar. 2022).

[4] Safeguard Defenders is a Spain-based human rights NGO that "undertakes and supports local field activities" in Asia (Safeguard Defenders n.d.). Safeguard Defenders "inherited the mission of China Action," its Beijing-based precursor NGO which was shut down in 2016 "after Chinese authorities targeted it in a major crackdown"; at that time, "many of its staff and partners were detained, disappeared or imprisoned" (Safeguard Defenders n.d.).

References

Assistant Professor, Simon Fraser University. 29 September 2022. Correspondence with the Research Directorate.

Axios. 22 January 2020. Bethany Allen-Ebrahimian. "University of Minnesota Student Jailed in China over Tweets." [Accessed 5 Oct. 2022]

Axios. N.d. "About Axios." [Accessed 5 Oct. 2022]

Business Wire. 20 September 2021. "TechCrunch Disrupt 2021 Announces Startup Battlefield Competitors and Judges." [Accessed 26 Sept. 2022]

Canadian Broadcasting Corporation (CBC). 10 September 2020. Evan Dyer. "'We Know Where Your Parents Live': Hong Kong Activists Say Canadian Police Helpless Against Online Threats." [Accessed 11 Oct. 2022]

Chiu, Joanna. 2021. *China Unbound: A New World Disorder*. House of Anansi Press.

Citizen Lab. 7 May 2020. Jeffrey Knockel, et al. *We Chat, They Watch: How International Users Unwittingly Build Up We Chat's Chinese Censorship Apparatus*. Citizen Lab Research Report No. 127. University of Toronto. [Accessed 11 Oct. 2022]

Citizen Lab. 24 September 2019. Bill Marczak, et al. *Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits*. Citizen Lab Research Report No. 123. University of Toronto. [Accessed 20 Sept. 2022]

CTV News. 24 April 2021. Christy Somos. "Hong Kongers Say They're Being Targeted by Chinese Agents on Canadian Soil." [Accessed 11 Oct. 2022]

Forbes. 1 September 2019. Thomas Brewster. "iPhone Hackers Caught by Google also Targeted Android and Microsoft Windows, Say Sources." [Accessed 22 Sept. 2022]

Freedom House. February 2021. Nate Schenkkan and Isabel Linzer. "Case Studies: China." *Out of Sight, Not Out of Reach: The Global Scale and Scope of Translational Repression*. [Accessed 20 Sept. 2022]

Global Times. 27 March 2015. Liu Sha. "'Sky Net' Cast over Corrupt Officials Abroad." [Accessed 27 Sept. 2022]

The Globe and Mail. 21 September 2022. James Griffiths and Irene Galea. "Chinese Police Establish Stations Overseas in 'Worrying' Crackdown on Citizens Abroad." [Accessed 5 Oct. 2022]

The Guardian. 16 December 2021. Vincent Ni. "Outspoken Editor of Chinese State Tabloid Global Times Retires." [Accessed 27 Sept. 2022]

Human Rights Watch (HRW). 14 January 2020. Kenneth Roth. "China's Global Threat to Human Rights." *World Report 2020: Events of 2019*. [Accessed 20 Sept. 2022]

Lookout. June 2020. "Mobile APT Surveillance Campaigns Targeting Uyghurs: A Collection of Long-Running Android Tooling Connected to a Chinese mAPT Actor." *Security Research Report*. [Accessed 26 Sept. 2022]

The New York Times. 31 December 2021. Muyi Xiao and Paul Mozur. "A Digital Manhunt: How Chinese Police Track Critics on Twitter and Facebook." [Accessed 21 Sept. 2022]

openDemocracy. 10 March 2022. Darren Loucaides and Alessio Perrone. "The Media Giant You've Never Heard of, and Why You Should Pay Attention." [Accessed 4 Oct. 2022]

Safeguard Defenders. 12 September 2022. *110 Overseas: Chinese Transnational Policing Gone Wild*. [Accessed 5 Oct. 2022]

Safeguard Defenders. February 2022. *Hide and Seek: China's Extradition Problem*. [Accessed 20 Sept. 2022]

Safeguard Defenders. N.d. "About Us." [Accessed 27 Sept. 2022]

Senior Lecturer, The University of Adelaide, Australia. 3 October 2022. Interview with the Research Directorate.

TechCrunch. 31 August 2019. Zack Whittaker. "Sources Say China Used iPhone Hacks to Target Uyghur Muslims." [Accessed 21 Sept. 2022]

United States (US). 18 May 2022 (updated 25 July 2022). Department of Justice. "U.S. Citizen and Four Chinese Intelligence Officers Charged with Spying on Prominent Dissidents, Human Rights Leaders and Pro-Democracy Activists." [Accessed 3 Oct. 2022]

Volexity. 2 September 2019. Andrew Case, Matthew Meltzer, and Stephen Adair. "Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs." [Accessed 20 Sept. 2022]

Volexity. N.d. "About." [Accessed 26 Sept. 2022]

The Washington Post. 14 February 2019. Gerry Shih and Emily Rauhala. "Angry over Campus Speech by Uighur Activist, Chinese Students in Canada Contact Their Consulate, Film Presentation." [Accessed 3 Oct. 2022]

Additional Sources Consulted

Oral sources: Australian Strategic Policy Institute – International Cyber Policy Centre; Center for Strategic and International Studies; Citizen Lab; Mercator Institute for China Studies; professor at a university in Pennsylvania who has conducted research on Chinese intelligence operations; professor at a university in Texas who works on authoritarianism and China's policy priorities; *The Wall Street Journal*.

Internet sites, including: Amnesty International; Australia – Department of Foreign Affairs and Trade; Austrian Red Cross – ecoi.net; BBC; Bertelsmann Stiftung; *China Daily*; The Daily Beast; Deutsche Welle; Factiva; International Crisis Group; *Maclean's*; Reuters; *South China Morning Post*; UK – Home Office; UN – Refworld; The Unrepresented Nations and Peoples Organization; US – Congressional-Executive Commission on China, Department of State; Xinhua News Agency.

Date modified:

2023-10-03