Annotated Bibliography

Digital Transnational Repression

By Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Adam Senft, and Ronald J. Deibert

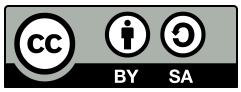
Last Updated: May 2021

THECITIZENLAB

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

Copyright



Citizen Lab engages in research that investigates the intersection of digital technologies, law, and human rights.

Document Version: 2.0

New changes in this annual update include:

- Change of terminology from “transnational digital repression” to “digital transnational repression” to align with the discourse
- New summaries collected between October 2020 - May 2021 and added to the document

Acknowledgements

The design of this document is by Mari Zhou.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Introduction

This Annotated Bibliography compiles and summarizes relevant literature on "***digital transnational repression***", i.e. where states seek to exert pressure—using digital tools—on citizens living abroad in order to constrain, limit, or eliminate political or social action that threatens regime stability or social and cultural norms within the country. While transnational repression itself is not a new phenomenon, there has been limited research on how such repression is enabled and expanded by ***digital tools***.

The resources included in this Annotated Bibliography are divided into ***four sections***: (1) media reports and analysis, (2) technical reports, (3) academic literature, and (4) government inquiries and prosecution. These resources begin to paint a picture of how digital transnational repression works, which regimes engage in such activities and using what digital tools, and how these efforts impact diaspora communities. Media reports published in the past few years show that countries such as Saudi Arabia, China, Rwanda, and others use a range of digital tools in order to silence human rights activists, political dissidents, and journalists living abroad. These are in addition to 'traditional' mechanisms of repression such as in-person harassment and surveillance or threats to family, which are also touched on in this bibliography but are not the focus. Technical reports provide in-depth analysis regarding the types of digital tools utilized to engage in such repression. These reports reveal that the sophistication of digital techniques utilized varies; from phishing campaigns dependent on savvy social engineering to the deployment of sophisticated and expensive spyware to social media harassment. Academic articles—several relying on semi-structured interviews with different diaspora communities—examine how digital transnational repression affects the activities and lives of diaspora in different ways by bringing to the forefront the voices and experiences of those repressed. Government inquiries and prosecutions addressing aspects of digital transnational repression have taken place in some states. While the discussion around this problem appears to be growing at a government-level, these efforts are still relatively nascent.

Research into digital transnational repression is still in its early stages. Perhaps one of the most pressing questions to tackle is how digital transnational repression can be addressed once identified. Targets of digital transnational repression have attempted to use the legal system to seek justice and relief against such targeting by bringing legal actions against states undertaking, sponsoring or facilitating the targeting activities, as well as related actors, such as the companies producing the technology that facilitate such activities. However, these efforts have limits—for example, a lack of prosecutorial interest or expertise and challenges with attribution and state immunity under existing legal doctrines. A legal approach needs to be complemented with more research and policy guidance regarding what makes prevention and accountability so difficult in this space, and how it might be addressed through other means, such as the enactment of new domestic laws or providing more resources to digital security training and technical support for activists in the diaspora.

More generally, further research is required to understand how digital transnational repression affects the social and political lives of targets. Such research may provide a persuasive basis for policy-makers and governments in host countries in which targets reside to take specific action to prevent these

types of activities. In particular, there remains limited research on not only how digital transnational repression facilitates the repression of political voices abroad, but also how it undermines the ability of individuals to live in and integrate into their new communities in their respective host countries. As the world continues to migrate online and as the Internet remains one of the key vehicles for international communications, academics are right to predict that digital transnational repression is likely to become a favourite tool of authoritarian regimes seeking to repress social and political action originating from abroad and will require further attention in order to ensure the protection of freedom of expression and opinion of all persons.

Annotated Bibliography

Media Reports & Analysis

Bahrain

Bahrain: Human Rights Defenders in Exile Threatened, Along With Their Families, While Ongoing Court Cases Continue Against Other Defenders
Gulf Center For Human Rights

Gulf Center For Human Rights. *"Bahrain: Human Rights Defenders in Exile Threatened, Along With Their Families, While Ongoing Court Cases Continue Against Other Defenders." Gulf Center For Human Rights*, March 11, 2017. https://www.gc4hr.org/news/view/1511.

Crux
While Bahraini human rights defenders at home are being imprisoned and threatened, the ones in exile have also been repressed in digital and traditional means.

Highlight
- Bahraini human rights defenders in exile have been subjected to various types of transnational repression and digital transnational repression.
- Sayed Yousif Al-Muhafdah; Vice-President of the Bahrain Center for Human Rights, an exile in Germany, has reported that he has received threats messages threatening him to harm his family in Bahrain if he continues to speak about human rights abuses in Bahrain.
- Sayed received the threat messages on Instagram and WhatsApp, who were linked to the government supporters. He was told to "Stop tweeting" otherwise his brother would be arrested.

UK Malware Used Against Bahraini Activists
Ben Knight

Knight, Ben. "UK Malware Used Against Bahraini Activists." *DW*, May 9, 2012. https://www.dw.com/en/uk-malware-used-against-bahraini-activists/a-16219440.

Crux
The article describes how Bahraini activists living in the United Kingdom were targeted with malware.

Highlights

- The targets included Husain Abdulla, “a naturalized US citizen and director of Americans for Democracy and Human Rights in Bahrain (ADHRB).”
- Abdulla describes his surprise at being the target of a cyber-attack, which he considers to be a new mechanism by which the government is coming after human rights activists.
- The software used in the cyber-attack was FinSpy, which was produced by Gamma Group, a UK company.

Bahraini Activists Hacked by Their Government Go After UK Spyware Maker

Kim Zetter

Zetter, Kim. “Bahraini Activists Hacked by Their Government Go After UK Spyware Maker.” *Wired*, October 13, 2014. https://www.wired.com/2014/10/bahraini-activists-go-after-spyware-source/.

Crux

This article describes how Bahraini activists who live in the UK and were targeted by the Bahraini government with malware lodged a criminal complaint against the UK firm that produced it.

Highlights

- Mohammad “Moosa” Abd-Ali describes how he discovered that he had been targeted with Gamma Group’s malware. Ali had been a human rights activist in Bahrain, where he was tortured. He fled to the UK where he was granted asylum in 2006.
- Al was targeted by a surveillance tool called FinFisher, produced by UK firm Gamma International.
- In 2014, Privacy International sent a criminal complaint against Gamma Group to the National Cyber Crime Unit of the National Crime Agency. They are seeking a “formal investigation” into the company.

China

China: Spies, Lies and Blackmail: How China Controls Its Citizens Inside and Outside the Country Where No Criticism or Dissent is Allowed

Al Jazeera

Al Jazeera. “China: Spies, Lies and Blackmail: How China Controls Its Citizens Inside and Outside the Country Where No Criticism or Dissent is Allowed.” *Al Jazeera*, April 5, 2018. https://www.aljazeera.com/programmes/101east/2018/04/china-spies-lies-blackmail-180404145244034.html?xif=.

Crux

Al Jazeera investigates how Chinese authorities persecute dissidents living outside China.

Highlights

- Al Jazeera found that targets of the Chinese authorities included “human rights lawyers, democracy activists and even students who say they sent tweets that the government disliked.”
- The type and nature of the targeting varied. Some Chinese targets abroad received death threats or were threatened in person. Another was the victim of a “malicious smear campaign” that spread online.

Why Some Chinese Immigrants Living in Canada Live in Silent Fear

Yaqiu Wang

Wang, Yaqiu. “Why Some Chinese Immigrants Living in Canada Live in Silent Fear.” *The Globe and Mail*, February 25, 2019. https://www.theglobeandmail.com/opinion/article-why-some-chinese-immigrants-living-in-canada-live-in-silent-fear/.

Crux

This article describes how Chinese authorities engage in repressive activities against Chinese immigrants in Canada.

Highlights

- Canadian Chinese immigrants are concerned “that if they criticize the government openly, their job prospects, business opportunities and chances of going back to China would be affected or that their family members who remain in China would be in danger.”
- Interviewees explained that they decided not to ask questions at public events, attend protests or other events out of fear of Chinese government agents watching them.
- The author notes that the Chinese government has engaged in various forms of repressive activities against Chinese citizens living abroad.

Zoom says it Acted on Tiananmen Accounts After China Demand

Al Jazeera

Al Jazeera. “Zoom Says it Acted on Tiananmen Accounts after China Demand.” *Al Jazeera*, June 11, 2020. https://www.aljazeera.com/news/2020/06/zoom-acted-tiananmen-accounts-china-demand-20061202 4129555.html.

Crux

This article shows how Zoom, the popular video-conferencing platform, suspended user accounts and ended a meeting linked to the anniversary of China's Tiananmen Square crackdown, and hosted by exiled Tiananmen activists, to comply with the Chinese government request.

Highlights

- Zhou Fengsuo, the US-based founder of Humanitarian China, said his account was suspended after holding a Zoom event to commemorate the 31st anniversary of the brutal military crackdown in Tiananmen Square. Viewers from mainland China, where Tiananmen has been all but erased, joined the event.
- Zoom said the Chinese government had notified it about four large planned commemoration meetings that were being published on social media. The authorities demanded they terminate the events and linked accounts.
- Zoom decided to end three of those meetings and temporarily suspend the host accounts as it is currently unable to remove specific participants from a meeting or block participants from a certain country from joining a meeting.
- Wang Dan, an exiled Tiananmen Square student leader whose account was also shut down, said he was shocked to hear Zoom admit it had interrupted meetings. His June 3 event with about 200 participants was deactivated midstream.
- Zoom said that it did not provide any user information or meeting content to the Chinese government.

China's Software Stalked Uighurs Earlier and More Widely, Researchers Learn

Paul Mozur and Nicole Perlroth

Mozur, Paul and Nicole Perlroth. "China's Software Stalked Uighurs Earlier and More Widely, Researchers Learn." *The New York Times*, July 1, 2020. https://www.nytimes.com/2020/07/01/technology/china-uighurs-hackers-malware-hackers-smartphones.html.

Crux

This article describes how Chinese authorities have been researching and developing surveillance technology to threaten dissidents living abroad.

Highlights

- The article describes findings by security firm Lookout regarding the activities of Chinese hackers against the Uighur diaspora.
- The company's research suggests that a "hacking campaign was an early cornerstone in China's Uighur surveillance efforts that would later extend to collecting blood samples, voice prints, facial scans and other personal data to transform Xinjiang into a virtual police state. It also shows the lengths to which China's minders were determined to follow Uighurs as they fled China for as many as 15 other countries."
- A threat intelligence engineer at Lookout noted that "Wherever China's Uighurs are going, however far they go, whether it was Turkey, Indonesia or Syria, the malware followed them there...It was like watching a predator stalk its prey throughout the world."

Chinese Police Are Making Threatening Video Calls to Dissidents Abroad

David Gilbert

Gilbert, David. "Chinese Police Are Making Threatening Video Calls to Dissidents Abroad." *Vice News*, July 14, 2020. https://www.vice.com/en_us/article/jgxdv7/chinese-police-are-video-calling-citizens-abroad-with-threats-not-to-criticize-beijing.

Crux

This article discusses how Chinese authorities target dissidents abroad through video calls with their family sitting next to them.

Highlights

- A Chinese dissident based in Australia under the pseudonym Horror Zoo was targeted with video calls over her tweets. She criticized Xi Jinping, supported pro-democracy protests in Hong Kong, and supported Dr. Li Wenliang for whistleblowing about COVID-19.
- The video calls are one of the tactics used "in a months-long campaign against Zoo." Harassment ramped up after she attended a high profile Tiananmen Square memorial on Zoom which took down many participants' Zoom accounts.
- Although Zoo operates anonymously online, the Chinese authorities found her family members and threatened their safety. Zoo also notes that someone from China tried to hack into her Apple account.

China Threatens and Intimidates People Within Canada as Ottawa Remains Silent

Charles Burton

Burton, Charles. "China Threatens and Intimidates People Within Canada as Ottawa Remains Silent." *The Toronto Star*, September 8, 2020. https://www.thestar.com/opinion/contributors/2020/09/08/china-threatens-and-intimidates-people-within-canada-as-ottawa-remains-silent.html.

Crux

This article describes how the Canadian Commons Subcommittee on International Human Rights and the Commons Special Committee on Canada-China Relations heard harrowing reports regarding how Chinese authorities are threatening individuals living in Canada, as well as families back in China.

Highlights

- The article describes how Canadian Chinese and Canadian Uighur activists provided testimony describing how they were "threatened with rape or even death" if they kept "speaking out against violations committted by China against the Uighurs, or the persecution of Hong Kong residents clinging to political rights."

- The witnesses, who were testifying in front of the Commons Subcommittee on International Human Rights and the Commons Special Committee on Canada-China Relations, "pleaded for Canada to stop this intimidation campaign being coordinated by the Chinese Embassy in Ottawa and its consulates in Montreal, Toronto, Calgary and Vancouver."
- The author comments on the lack of political action by the Trudeau government in the face of these stories regarding Chinese activities in Canada against activists.

Beijing's Assault on Privacy Goes Global

Clive Hamilton

Hamilton, Clive. "Beijing's Assault on Privacy Goes Global." *The Globe and Mail*, September 8, 2020. https://www.theglobeandmail.com/opinion/article-beijings-assault-on-privacy-goes-worldwide/.

Crux

This op-ed notes that the government of Canada has chosen a China-based company founded by the son of former President Hu to provide security systems in Canadian embassies around the world. He argues that alongside issues like Canada's delay in announcing a decision on the use of Huawei 5G telecommunications equipment, this represents a privacy and security risk not just for Canadian citizens, but any "Chinese dissidents, asylum seekers and defectors" who may step into a Canadian embassy.

Highlights

- China-based Nutech was selected to install X-ray scanners in Canadian embassies and high commissions around the world. Nutech was founded by the son of Hu Jintao.
- Cites a recent expert report commissioned by Australia's Department of Foreign Affairs that found "that Huawei deliberately installed encryption software in a new data centre for the government of Papua New Guinea, allowing Beijing to hoover up secret government files at its leisure".
- The author notes that "[i]f Beijing instructs Nuctech to send data on who has entered Canada's embassies, then Nuctech is legally obliged to obey. That's the risk that most of the world understands about Chinese companies with state entanglements – with the glaring exception, it seems, of Canada."

Ethiopia

Surveillance Follows Ethiopian Political Refugee to the UK

Privacy International

Privacy International. *Surveillance Follows Ethiopian Political Refugee to the UK.* Privacy International, February 16, 2014. https://privacyinternational.org/blog/1199/surveillance-follows-ethiopian-political-refugee-uk.

Crux
Ethopian refugee, Tadesse Kersmo, was tracked through his computer through “a Trojan that is part of a commercial intrusion kit called FinFisher.”

Highlights
- Tadesse Kersmo fled to the UK and was granted asylum in 2009. Previously, he was subjected to “years of persistent harassment, violence, and surveillance” by the Ethiopian government.
- However, despite fleeing Ethiopia, he was subjected to tracking through FinFisher spyware on his computer. He used his computer to stay in touch with friends and relatives, and to continue to advocate for democracy in Ethiopia.
- Tadesse explained that the surveillance “made him feel insecure and very uncomfortable, as if he was constantly being watched. He hopes that sharing his experience will make other vulnerable groups such as human rights activists and journalists aware of the risk that their computers may be compromised without them knowing as well.”

Iran

Exclusive: Iran-Linked Hackers Pose as Journalists in Email Scam
Raphael Satter, and Christopher Bing

Satter, Raphael and Christopher Bing. “Exclusive: Iran-Linked Hackers Pose as Journalists in Email Scam.” *Reuters*, February 5, 2020.
https://www.reuters.com/article/us-iran-hackers-exclusive-idUSKBN1ZZ1MS.

Crux
This report covers an Iranian backed phishing attack against an Iranian-born German academic.

Highlights
- Erfan Kasraie is a well known critic of the Iranian regime. He received a suspicious email from the Wall Street Journal requesting to interview him. Afterwards, he received an email from Farnaz Fassihi; an Iranian-American journalist who covers the Middle East.
- The follow-up email instructed Kasraie to enter his Google password to see the interview questions, which was an attempt to compromise his email account.
- This attack is a part of a wider campaign targeting journalists, as confirmed by three cybersecurity firms.
- Hassan Sarbakhsian, an Iraninan filmmaker was also targeted by a suspicious email claimed to be from Fassihi from the Wall Street Journal.

Edmonton Software Engineer Says Iranian Regime Attempted to Make Him Their Spy
Wallis Snowdon

Snowdon, Wallis. “Edmonton Software Engineer Says Iranian Regime Attempted to Make Him Their Spy.” *CBC News*, August 27, 2020. https://www.cbc.ca/news/canada/edmonton/edmonton-software-engineer-arrest-iranian-regime-informant-1.5700744.

Crux

This article describes how the Iranian authorities attempted to forcibly recruit US/Canada-based software engineer Behdad Esfahbod to spy for the Iranian regime.

Highlights

- Behdad Esfahbod was employed by Facebook in the United States. On a trip back to Iran, he was arrested, detained, and interrogated for nearly a week. The Iranian regime wanted him to feed them information regarding the Iranian tech sector.
- After he was released from jail and left Iran, he started receiving encrypted messages on his social media accounts including Instagram. His sister in Tehran was threatened on the phone and received a summons for her brother to report to the courts for questioning.
- Esfahbod’s life fell apart after his return from Iran. He went on medical leave from Facebook and eventually quit and moved in with his sister in Edmonton.

Iranian Regime Using Dutch Server to Spy on Dissidents: Investigation

Arab News

Arab News. “Iranian Regime Using Dutch Server to Spy on Dissidents: Investigation.” *Arab News*, February 19, 2021. https://www.arabnews.com/node/1811671/middle-east.

Crux

A Dutch radio program reports that a server in the Netherlands is being used by the Iranian authorities for espionage against political opponents, including in the Netherlands.

Highlights

- An investigation by a Dutch radio program (original in Dutch) identified a server in the Netherlands being used to hack into phones and computers in the Netherlands, Germany, Sweden, and India.
- The server is a command and control server and the software being used by the server has been linked to the Iranian regime by security experts.

Victims Recount Foreign State-Sponsored Harassment

Steven Chase

Chase, Steven. “Victims Recount Foreign State-Sponsored Harassment.” *The Globe and Mail*, November 27, 2020.

Crux

Canadians are being harassed by foreign governments through digital means, such as Facebook.

Highlights

- Javad Soleimani's wife died in the Ukrainian International Airlines Flight 752 when it was shot down by the Iranian military.
- After these events, Soleimani criticized the Iranian government online. He started receiving messages warning him that the Islamic Revolutionary Guard Corps was "able to do anything in Canada" and that he should be careful.
- Soleimani stated that the "head of Iran's Aircraft Accident Investigation Bureau contacted him via Instagram and 'threatened me to remove my Instagram posts'" when he criticized the regime. His family in Iran was also called by the intelligence services when he refused.
- Canada's Foreign Affairs Minister told Canadians to call the police if they are being harassed. But individuals say they have been bounced from one law-enforcement organization to another. The speakers urged Ottawa to set up a national "hotline to take complaints of foreign harassment, and a registry to monitor those working in Canada on behalf of foreign governments."
- Chemi Lhamo, a student at a Canadian university of Tibetan origin, said she received "thousands of intimidating messages, including threats of murder and rape" when she ran for student union president at her university.
- Marcus Kolga, who is a Canadian of Estonian origin and a human rights activist, said he also received threats via Facebook. He received the "runaround" from the RCMP when he presented these threats. The York Regional Police eventually tracked down the perpetrator.
- He argued that Canada must develop a "national reporting mechanism for victims of political intimidation" and should follow Australia, where the country has created a "foreign-agents registry."

Palestine

Palestinian journalist Muath Hamed Questioned in Spain by Alleged Israeli Intelligence Agent

Committee to Protect Journalists

Committee to Protect Journalists. "Palestinian Journalist Muath Hamed Questioned in Spain by Alleged Israeli Intelligence Agent." *Committee to Protect Journalists,* April 15, 2021. https://cpj.org/2021/04/palestinian-journalist-muath-hamed-questioned-in-spain-by-alleged-israeli-intelligence-agent/.

Crux

Mouath Hamed, a Palestinian journalist and an asylum seeker, was interrogated in Spain by an alleged Israeli agent regarding sources mentioned in his reporting. Hamed believes that the incident is associated with the hacking of his phone.

Highlights

- Hamed was asked by a Spanish Civil Guard officer to go to the Civil Guard headquarters in Madrid to talk about his asylum status.

- Once at headquarters, Hamed was introduced by the Spanish officer to someone who said his name was “Omar” and claimed to be a Belgian agent of Palestinian origin.
- Hamed was familiar with the accent and the methods of Israeli intelligence having been previously detained by them. It was clear to Hamed that his interviewer was an Israeli agent.
- The agent’s questions to Hamed were about sources in an investigation report Hamed had prepared. Hamed was shocked because he kept the sources confidential and, in his report, only mentioned pseudonyms. This appeared not to have been enough because the agent knew the sources’ real names.
- Hamed suspected his phone might be hacked in January 2021 when he received a suspicious Skype call from an unknown number. After that, his phone acted strangely.
- Hamed described: “Since that call, I had to recharge my battery up to five times a day, the phone slowed down and looked as if something was constantly uploading, it was so hot I could hardly touch it and whenever I was talking there was a constant background noise.”

Rwanda

‘I Was a Victim of the WhatsApp Hack’

Joe Tidy

Tidy, Joe. “‘I Was a Victim of the WhatsApp Hack’.” *BBC News*, October 31, 2019. https://www.bbc.com/news/technology-50249859.

Crux

Faustin Rukundo was a target of a cyberattack using Pegasus spyware on the WhatsApp platform. Rukundo is a member of the Rwandan National Congress (RNC), an opposition party in Rwanda. He fled Rwanda and lives in exile in the UK.

Highlights

- In April 2019, Rukondo received mysterious phone calls on WhatsApp that he could not trace back to a contact.
- After these calls, he noticed that files were missing on his phone. He spoke with colleagues in the RNC who confirmed they were experiencing the same missed calls issue as he was.
- Citizen Lab later confirmed that his device was one of the 1,400+ devices targeted in the 2019 WhatsApp hack.
- Rukondo says that he has been feeling “paranoid and scared” since the original hack.

Digital Technology Helps Governments Target Critics Across Borders

Isabel Linzer

Linzer, Isabel. "*Digital Technology Helps Governments Target Critics Across Borders*." Slate, February 24, 2021. https://slate.com/technology/2021/02/paul-rusesabagina-rwanda-trial-digital-technology-critics-abroad.html.

Crux
This article describes how digital technology is facilitating transnational repression. In particular, it mentions the case of Rwandan dissidents in exile who allege to have been targeted through such means by Rwandan authorities.

Highlights
- The trial of Paul Rusesabagina began in February 2021 in Rwanda. He is "only in Rwandan custody because of the Rwandan government's illegal campaign of transnational repression."
- Linzer notes that "Rwandan critics in exile—including one who was previously targeted with spyware—have posited that digital surveillance may have played a role in Rusesabagina's abduction."
- The article describes how "[s]tates use spyware, social media monitoring, and online harassment to disrupt, intimidate, surveil, and attack exiles from across the globe."

Saudi Arabia

Human Rights Activist Launches Legal Claim Against Saudi Arabia For "Hacking Phone" in UK

Lizzie Dearden

Dearden, Lizzie. "Human Rights Activist Launches Legal Claim Against Saudi Arabia For 'Hacking Phone' in UK." *The Independent UK*, May 29, 2019. https://www.independent.co.uk/news/uk/home-news/saudi-arabia-spying-phones-ghanem-dosari-uk-spyware-pegasus-a8935331.html.

Crux
Ghanem al-Dosari, a Saudi refugee living in the United Kingdom, believes he was targeted by Saudi authorities through digital means.

Highlights
- Al-Dosari believes that "two of his iPhones were corrupted with spyware that enabled agents to extract communications data and access microphones and cameras." He launched a legal claim against the Saudi authorities.
- Analysis by the Citizen Lab found that the malicious texts had led to internet domains associated with Pegasus spyware, which is developed by the Israeli surveillance company NSO Group.
- Al-Dosari's lawyers said that analysts "concluded with a high degree of confidence that the state responsible was Saudi Arabia."

- Al-Dosari has also received other threats. He reported having been attacked by Saudi men prior to this targeting by digital means. He has also "received death threats and abuse" over his satirical videos.

The Dark Side of Israel's Cold Peace With Saudi Arabia: The Saudis Are Using Israeli-made Cyberweapons to Monitor and Intimidate Dissidents Abroad

Eli Lake

Lake, Eli. "The Dark Side of Israel's Cold Peace With Saudi Arabia: The Saudis Are Using Israeli-made Cyberweapons to Monitor and Intimidate Dissidents Abroad." *Bloomberg*, June 3, 2019. https://www.bloomberg.com/opinion/articles/2019-06-03/israel-s-cold-peace-with-saudi-arabia-has-a-dark-side.

Crux

The article describes surveillance technology developed in Israel by NSO Group that is used against Saudi dissidents abroad.

Highlights

- The article describes the targeting of dissidents living abroad by the Saudi authorities using Israeli surveillance tools produced by NSO Group.
- In particular, the article mentions the case of Iyad Al-Baghdadi who was informed that he was the target of Saudi authorities while living in Norway. Al-Baghdadi is a Palestinian blogger and journalist. He is a "critic of Islamist totalitarian movements and the autocracies aligned against them."
- The author explains how "Saudi phone hacking need not end in murder for it to be sinister" with his interview with Al-Baghdadi: An invasion of privacy is also traumatic...They are trying to defame you or get a sexual scandal or a financial scandal to blackmail you. Sometimes it's just tracking your location to beat you up."
- The article notes that the Saudi phone hacking is "enabled by a privately owned Israeli company called the NSO Group Ltd." The surveillance technology has been used in efforts to "hack the phones of journalists and human-rights activists."

No One Is Safe: How Saudi Arabia Makes Dissidents Disappear

Ayman M. Mohyeldin

Mohyeldin, Ayman M. "No One Is Safe: How Saudi Arabia Makes Dissidents Disappear." *Vanity Fair*, July 29, 2019. https://www.vanityfair.com/news/2019/07/how-saudi-arabia-makes-dissidents-disappear.

Crux

This article describes how the Saudi authorities "abduct, repatriate—and sometimes murder—citizens it regards as enemies of the state."

Highlights

- The article describes the practices of the Saudi authorities in an attempt to limit and or eliminate dissent among Saudi nationals living abroad.
- The article mentions several forms of targeting of activists and dissidents abroad and silencing anyone who criticizes or poses any kind of threat to the government authority. For example: physical threats, kidnapping and forcible transfers to the Saudi kingdom to be imprisoned, suspending financial aid, monitoring online activities of citizens and students abroad and holding them prisoner when they return home, and executing cyber attacks on dissidents using malware and spyware.
- The article considers the situations of Prince Khaled bin Farhan al-Saud in Germany, Omar Abdulaziz in Canada, and Yahya Assiri, who is now living in the UK. For example, Omar Abdulaziz, an activist living in Canada, was approached multiple times by Saudi authorities in person in Montreal. He was later targeted with spyware.
- The article describes how the Internet and the rise of online communications has facilitated this type of repressive activity by the Saudi government and efforts by the Saudi authorities to leverage this reality against dissidents.

He Claimed Asylum in Canada and Spoke Out Against the Saudi Regime. So Why Has Ahmed Alharby Gone Home?

Toronto Star

Toronto Star. “He Claimed Asylum in Canada and Spoke Out Against the Saudi Regime. So Why Has Ahmed Alharby Gone Home?”. *Toronto Star*, February 19, 2021.

Crux

Ahmed Alharby, a twenty-four year old refugee in Canada, has returned to Canada less than two years after seeking asylum. It is unclear why he returned, and his friends believe the Saudi government is involved.

Highlights

- Twenty-four year old Ahmed Alharby came to Canada less than two years ago seeking political asylum. He recently returned back to Saudi Arabia.
- There are dueling narratives regarding why he went back to Saudi Arabia. A newly created Twitter account under his name presented Alharby as a “dissident turned believer, having returned to the land of his birth - Saudi Arabia - and repented his public criticisms of its ruling regime.”
- However, Alharby’s friends in Montreal describe the situation differently. “Three friends recalled to the Star phone calls each had with Alharby weeks ago in which he described having gone to the Saudi embassy in Ottawa, underwent some kind of interrogation and was now seeking their help.”
- In May 2019, Alharby posted a video on Twitter in which he expressed support for those facing injustice in Saudi Arabia. After that, his friends said he decided to work less publicly because of fear of backlash for friends and family in Saudi Arabia.

- On January 30, 2021, a friend of Alharby said he got a call from Alharby who said he was “lost” and needed advice. Alharby explained that he had gone to Ottawa and visited the embassy. “During the visit, Alharby said, he felt like he was under investigation and was questioned about his friends and the projects he had worked on.”
- During the visit to the embassy, Alharby was given travel documents for returning to Saudi Arabia. Someone from the embassy accompanied him to the airport earlier that day; however, Alharby fled at the airport. Omar Abdulaziz, who has similarly been targeted by the Saudi authorities in Canada and is a friend of Alharby, said he believed that Alharby did not go voluntarily.
- The following day, another friend called Alharby but received no answer. A few days later, on February 1, 2021, Alharby called Omar Alzuhairi, another friend, and said he was in a hotel in Ottawa. Alzuhairi asked why, and Alharby explained he was going back to Saudi Arabia. Alharby asked, however, that he come pick him up in Ottawa.
- The next day, Alzuhairi called Alharby but couldn’t reach ihm. A few weeks went by without a word. Abdulaziz eventually called the RCMP in mid-February. That same day, Abdulaziz posted a video recounting the events. The next day, a new Twitter account under Alharby’s name was posted.
- Alharby’s friends say that the series of events do not add up and they believe the Saudi government “pushed him” and that he was trying to talk to them.

Syria

Life in the digital shadows of the Syrian war

Naheed Mustafa

Mustafa, Naheed. “Life in the digital life of the Syrian War.” *Open Canada*, October 18, 2016. https://www.opencanada.org/features/life-digital-shadow-syrian-war/.

Crux

This article shows how digital connections puts refugees, activists, and human rights defenders who are involved in the Syrian conflict at risk. It profiles Mariam Hamou, a Syrian activist living in Canada, who was digitally targeted. She is the North American director of public relations and media for the National Coalition of the Syrian Revolutionary and Opposition Forces (SNC).

Highlights

- Hamou was part of the Syrian diaspora who took a stand in the early days of the demonstrations of March 2011.
- For Hamou, digital connectivity is crucial to stay connected with activists on the ground and to be able to organize with other Syrian diaspora communities.
- In November 2013, Hamou’s SNC email had been compromised and sexually graphic pictures were sent by the hackers to every man in her contact list. Her Facebook profile was also compromised.

- Hamou was targeted with phishing attacks. A suspicious email was sent to her email from a Saudi source, and sent her to a site that asked for her password to access a video and she typed it in.
- The attacks are not solely on her digital accounts but also as a way for the attackers to "vilify her and sabotage her reputation. She says that their use of sexually explicit material to embarrass her reveals a carefully crafted plan to poison people's minds."
- The author notes how "[t]he attack on Hamou was consistent with the actions of the Syrian Electronic Army, a group of pro-Assad regime hackers that has tried to counteract anti-regime stories coming out of Syria, and which later turned to premeditated attacks against political opposition groups, news outlets and aid workers."
- "Hamou has stepped away from her activism to focus on her family's well-being, and her own. But she still feels a surge of excitement and dread, not knowing what will follow, when a new email pings its arrival."

Vietnam

Lined Up in the Sights of Vietnamese Hackers

BR24

BR24. "Lined Up in the Sights of Vietnamese Hackers." *BR24*, October 7, 2020. https://web.br.de/interaktiv/ocean-lotus/en/.

Crux

This report describes how a group of Vietnamese hackers have been pursuing Vietnamese dissidents living in Germany, and the failure of the German authorities to intervene.

Highlights

- This report describes in detail how Bui Thanh Hieu, a Vietnamese dissident living and working in Berlin, has been pursued with the use of cyber tools.
- Hieu was not the only victim of such cyber activity. The report also notes that research by BR and Zeit Online showed that "numerous persons" were affected, including "opposition members and human rights activists."
- The report notes that many of these targets "felt alone in Germany. If they are lucky, information security specialists will contact them and notify them about their website having been hacked. German authorities, on the other hand, usually do not contact them. Research suggests that they are overwhelmed. There are hardly any established procedures to help dissidents in cases of cyber espionage."
- Interviews with targets led the report's author to conclude that there is a group of hackers pursuing these targets, "presumably acting in Vietnam's strategic interest." In Hieu's case, traces were left behind to a group that has been named "APT 32" or "Ocean Lotus." Experts have agreed that "this is a Vietnamese group spying, in particular, on its own compatriots." The Vietnamese embassy in Berlin denied any links to the group.
- The report's author reviewed the State's response to such events, which has ultimately been lacking. Vu Quoc Dung, another target of hacking over multiple years, explained that he was

not provided assistance after being targeted. Dung eventually pursued legal action, but it ended up being handled by the police as a fraud case.

Technical Reports

For a summary of additional technical reports related to the deployment of dual-use technologies against civil society and human rights defenders more generally, see Siena Anstis, Sharly Chan, Adam Senft, and Ronald J. Deibert. Dual-Use Technologies: Network Traffic Management and Device Intrusion for Targeted Monitoring. *Citizen Lab*, October 2020. https://citizenlab.ca/2019/09/annotated-bibliography-dual-use-technologies-network-traffic-management-and-device-intrusion-for-targeted-monitoring/.

General

Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. Citizen Lab, University of Toronto, September 18, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Crux

This report by the Citizen Lab uncovers how NSO Group's Pegasus Spyware has been used to infect targets' devices in at least 45 countries. Within a two year period between August 2016-August 2018, the Citizen Lab used Internet scanning to find fingerprints and domain names that matched with NSO Group's Pegasus spyware. Out of the 45 countries identified, at least ten Pegasus operators appeared to be actively engaged in cross-border surveillance. The Citizen Lab also found suspected NSO Pegasus infections associated with 33 of the 36 Pegasus operators. These findings paint a bleak picture of the human rights risks of NSO Group's global proliferation – Pegasus is being used by countries with poor human rights records. Moreover, the Citizen Lab found evidence of possible political themes within targeting materials in several countries, calling into question the legitimacy of criminal investigations that use Pegasus.

Highlights

- The Citizen Lab developed and used a novel technique (named *Athena* by the researchers) to cluster their fingerprint and domain matches into 36 distinct Pegasus systems, each one which appears to be run by a separate operator.
- The Pegasus mobile phone spyware suite is produced and sold by Israel-based cyber warfare vendor, NSO Group. Pegasus customers can infect phones by sending their targets specially crafted exploit links. Once a phone is infected and Pegasus is installed, it begins contacting the operator's command and control servers to receive and execute operators' commands. The customer has full access to a victim's files and can have access to the microphone and camera to eavesdrop.

- Pegasus exploit links and command and control servers use HTTPS, which requires operators to register and maintain domain names. These domain names for exploits often look benign at first glance because they impersonate legitimate services.

Azerbaijan

False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan

Claudio Guarnieri, Joshua Franco and Collin Anderson

Guarnieri, Claudio and Joshua Franco from Amnesty International, and Collin Anderson, independent researcher. "*False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan.*" Amnesty International, March 10, 2017. https://www.amnesty.org/en/latest/research/2017/03/False-Friends-Spearphishing-of-Dissidents-in-Azerbaijan/.

Crux

A mass government-backed digital surveillance campaign targeted dissidents in Azerbaijan, including exiled dissidents.

Highlights

- The campaign used multiple tactics, including impersonating a human rights activist and a well-known former detainee, to send malicious malware through attachments by fake emails claiming to be the email of Rasul Jafarov.
- The campaign also targeted dissidents in exile, such as Leyla Yunus who lives in the Netherlands.
- Several of Leyla's online accounts were compromised through the use of fake Facebook accounts and fake email addresses that impersonated her. It was also discovered that her computer was compromised by malware.

Activist's YouTube Channel Down

Azerbaijan Internet Watch

Azerbaijan Internet Watch. "Activist's YouTube Channel Down." *Azerbaijan Internet Watch*, December 5, 2019. https://www.az-netwatch.org/news/activists-youtube-channel-down/.

Crux

This article discusses how the YouTube channel of an Azerbaijani activist living abroad was taken down after requests were made by Milli TV, Qanun TV and AnTV.

Highlights

- On December 5, 2019, Shakir Zade, an activist from Azerbaijan living abroad, "reported his YouTube channel was taken down by the platform following takedown requests made by Milli

TV, Qanun TV and AnTV." An admin of AnTV also told Zade that his "personal account was hacked during the reporting."
- Later that same month, Zade's YouTube account was "again reportedly taken down by the YouTube platform after a series of 'copyright violation' reports sent in by AnTV and Qafqaz News accounts."
- His channel was closed yet again in January 2020 by what appeared to be another "false copyright violation report."

China

Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114

Katie Kleemola, Masashi Crete-Nishihata, and John Scott-Railton

Kleemola, Katie, Masashi Crete-Nishihata, and John Scott-Railton. *Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114.* Citizen Lab, University of Toronto, June 15, 2015. https://citizenlab.ca/2015/06/targeted-attacks-against-tibetan-and-hong-kong-groups-exploiting-cve-2014-4114/

Crux

This report analyzes malware intrusion attempts against groups in the Tibetan diaspora and pro-democracy groups in Hong Kong. These intrusion attempts against Tibetan groups are not isolated as the report demonstrates how there has been a change in tactics from previous campaigns.

Highlights

- This technical report by the Citizen lab analyzed targeted malware intrusion attempts against groups in the diaspora and pro-democracy groups in Hong Kong. All of these intrusion attempts were delivered via malicious Microsoft Powerpoint Slideshow files (*.pps), and one attack sent to Tibetan groups used a link to a file on Google Drive to deliver the malware.
- The team observed a total of five malware campaigns that used CVE-2014-4114 and a range of social engineering tactics to persuade recipients to either open an attachment, or visit a URL that downloaded a malicious file.
- The intrusion attempts against Tibetan groups shows changes in tactics from previous intrusion attempts. These intrusion attempts used CVE-201404114 and were delivered via Microsoft Powerpoint Slideshow files. The majority of the previous intrusion attempts against Tibetan groups use CVE-2010-3333 or CVE-2012-0158.
- As the report argues, the use of Google Drive to deliver the malware may be evidence of intrusion attempts adapting to the behavioral countermeasures promoted by the "Detach from Attachments" awareness campaign to educate the community about common attack vectors. The campaign urges users to avoid sending or opening email attachments, and to use cloud-based storage to send files through Google Drive, etc.
- In addition to the use of the same CVE, some of the intrusion attempts targeting Tibetan rights groups and Hong Kong groups have overlap in malware family (PlugX) and Command and Control (C2) domains. The similarities between these intrusion attempts suggests that either

they are being conducted by the same threat actor or that threat actors targeting these groups are sharing tactics, techniques, and procedures (TTPs).

Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns

Matt Brooks, Jakub Dalek, and Masashi Crete-Nishihata

Brooks, Matt, Jakub Dalek, and Masashi Crete-Nishihata. *Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns.* Citizen Lab, University of Toronto, April 18, 2016. https://citizenlab.ca/2016/04/between-hong-kong-and-burma/

Crux

This report analyzes two malware families used in an espionage campaign that targeted Hong Kong democracy activists. Citizen Lab builds upon previous reporting by other groups and has named the malware families as UP007 and SLServer. Citizen Lab "speculate[s] that either a single threat actor is targeting these groups or some level of formal or informal resource sharing is occurring between the operators behind the campaigns."

Highlights

- Malicious emails were sent to Hong Kong-based pro-democracy activists a week before the 2016 Taiwanese General election. The sender purported to come from a Taiwanese non-profit organization and the content offered information about the election. The Google Drive link led to a RAR archive with malicious and benign documents.
- In addition to targeting Hong Kong activists, "the UP007 malware family has been found in previous campaigns targeting Burmese interests. In addition, the campaigns share some C2 infrastructure with previous operations against targets in Thailand and the Tibetan community."

We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus

Jeffrey Knockel, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert

Knockel, Jeffrey, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert. *We Chat, They Watch: How International Users Unwittingly Build Up WeChat's Chinese Censorship Apparatus.* Citizen Lab, University of Toronto, May 7, 2020. https://citizenlab.ca/2020/05/we-chat-they-watch/.

Crux

Technical experiments reveal that WeChat communications conducted entirely among non-China-registered accounts are subject to pervasive content surveillance that was previously

thought to be exclusively reserved for China-registered accounts. This case provides an example of how surveillance practices within a nation state can be exported abroad.

Highlights

- Technical experiments conducted by the Citizen Lab show that documents and images transmitted among non-China-registered accounts underwent content surveillance. Those files were analyzed for content that was politically sensitive to China. The files deemed politically sensitive to China were used to invisibly train and build up WeChat's Chinese political censorship system.
- The report notes that it is unclear how Tencent uses non-Chinese-registered users' data to enable content blocking or what policy rationale permits the sharing of data used for blocking between international and Chinese regions of WeChat. Tencent failed to respond to a number of data access requests seeking further information on this issue.

Taking Action Against Hackers in China

Mike Dvilyanski and Nathaniel Gleicher

Dvilyanski, Mike and Nathaniel Gleicher (Facebook). *Taking Action Against Hackers in China*. Facebook, March 24, 2021. https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/.

Crux

Facebook has taken action against a group of hackers in China ("Earth Empusa" or "Evil Eye") in order to "disrupt their ability to use their infrastructure to abuse [Facebook's] platform, distribute malware and hack people's accounts across the internet." Targets were Uyghurs from Xinjiang in China primarily living abroad.

Highlight

- Facebook has taken action to stop a group of Chinese hackers—known as Earth Empusa or Evil Eye—who have been targeting Uyghurs from China now living abroad in Turkey, Kazakhstan, the United States, Syria, Australia, Canada, and other countries.
- Facebook describes that the group used "various cyber espionage tactics to identify its targets and infect their devices with malware to enable surveillance." It noted that "the activity had the hallmarks of a well-resourced and persistent operation" that hid who was behind it.
- On Facebook, "it manifested primarily in sending links to malicious websites rather than direct sharing of the malware itself." Facebook also noted a number of features to this activity, such as: selective targeting, exploit protection, the compromise and impersonation of news websites, social engineering, the use of fake third party app stores, and the outsourcing of malware.

Ethiopia

Hacking Team and the Targeting of Ethiopian Journalists

Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. *Hacking Team and the Targeting of Ethiopian Journalists*. Citizen Lab, February 12, 2014. https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/.

Crux

This Citizen Lab report is the first of three reports documenting the global proliferation and use of Hacking Team's Remote Control System (RCS) spyware, which is allegedly sold exclusively to governments. The Citizen Lab reported how the Milan-based Hacking Team's RCS spyware was used to target the Ethiopian Satellite Television Service (ESAT), an independent satellite television, radio, and online news media outlet run by members of the Ethiopian diaspora. The malware communicated with an IP address belonging to Ariave Satcom, a satellite provider that services Africa, Europe, and Asia.

Highlights

- ESAT broadcasts are frequently critical of the Ethiopian government. Their broadcasts have been jammed from within Ethiopia several times over the years.
- The Committee to Protect Journalists (CPJ) reports that Ethiopia jails more journalists than any other African country besides Eritrea, and says that the Ethiopian government has shut down more than seventy-five media outlets since 1993.
- In the space of two hours on December 20, 2013, an attacker made three separate attempts to target two Washington-based ESAT employees with Hacking Team's RCS.
    - RCS is a trojan sold exclusively to intelligence and law enforcement agencies. It works by infecting a target's computer or mobile phone to intercept data before it is encrypted, and it can also intercept data that is never transmitted. RCS can copy files from a hard disk, record Skype calls, emails, instant messages, and passwords typed into a web browser. It can also turn on a device's webcam and microphone.
    - Hacking Team was in the public spotlight in 2012 when RCS was used against award-winning Moroccan media outlet Mamfakinch and United Arab Emirates (UAE) human rights activist Ahmed Mansoor.
- At the time of publication, Hacking Team stated how "they do not sell RCS to 'repressive regimes,'" and that RCS is not sold through "independent agents." They also noted how all their sales are reviewed by a board that includes external engineers and lawyers and has veto power over any sale. Before authorizing a sale, Hacking Team said that it considers whether a country would use surveillance technologies to facilitate human rights abuses, as well as "due process requirements" for surveillance.
- This case demonstrates a broader pattern of government abuse of lawful intercept spyware. It also raises questions about whether more mechanisms are needed to regulate the use, sale, and development of commercial spyware and dual-use technologies.

Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware

Bill Marczak, John Scott-Railton, and Sarah McKune

Marczak, Bill, John Scott-Railton, and Sarah McKune. *Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware*. Citizen Lab, University of Toronto, March 9, 2015. https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

Crux

This report details how a governmental attacker targeted journalists from the Ethiopian Satellite Television Service (ESAT) in the United States with Hacking Team's RCS spyware. See also: Hacking Team and the Targeting of Ethiopian Journalists (above).

Highlights

- In November and December 2014, journalists based in Washington, D.C. with ESAT were targeted with what appeared to be new versions of Hacking Team's RCS spyware.
- Research suggests the involvement of governmental attacker Ethopian Information Network Security Agency (INSA) and appeared to be the same entity documented in prior attacks against ESAT journalists in Belgium and the United States.

Champing At the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware

Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert

Marczak, Bill, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert. *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware*. Citizen Lab, University of Toronto, December 6, 2017.
https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/

Crux

This report explains how Ethiopian dissidents in the United States, United Kingdom, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins. The targets included a US-based Ethiopian diaspora media outlet, the Oromia Media Network in Ethiopia, a PhD student, and a lawyer. One of the Citizen Lab report authors was also targeted. The analysis of the spyware indicates that it is a product called PC Surveillance System (PSS), a commercial spyware product with a novel exploit-free architecture manufactured and sold by Cyberbit, a cybersecurity company that is a wholly owned subsidiary of Elbit Systems.

Highlights

- This report describes a campaign of targeted malware attacks apparently carried out by Ethiopia. Targets received an email with a link to a malicious website impersonating an online video portal. Clicking on the link led to an invitation to download an Adobe Flash update containing spyware before viewing the video. In other cases, targets were prompted to install a fictitious app called "Adobe PdfWriter" in order to view a PDF file. The spyware appeared to be Cyberbit's PSS product.

- Researchers identified a public logfile on the PSS spyware's command and control server and monitored it over more than a year. Researchers saw the spyware operators connecting from Ethiopia and infected computers connecting from IP addresses in 20 countries, including IP addresses traced to Eritrean companies and government agencies.
- Internet scanning led to the discovery of other servers associated with PSS and several that appeared to be operated by Cyberbit. The public logfiles on these servers appeared to have tracked Cyberbit employees as they carried infected laptops around the world, apparently giving demonstrations of the PSS product to government authorities in Thailand, Uzbekistan, Zambia, the Philippines, and at ISS World Europe (Intelligence Support Systems for Electronic Surveillance) in 2017. Other demonstrations appeared to have been provided to France, Vietnam, Kazakhstan, Rwanda, Serbia, and Nigeria.
- The report contributes to a growing body of research showing the wide abuse of nation-state spyware by authoritarian leaders to covertly surveil and invisibly sabotage entities they deem to be political threats. After FinFisher, Hacking Team, and NSO Group, Cyberbit is the fourth vendor of nation-state spyware whose tools Citizen Lab has seen abused. Ethiopia has also previously used Hacking Team's RCS spyware to target US-based journalists, as well as FinFisher's FinSpy spyware to target against political dissidents.

Iran

London Calling: Two-Factor Authentication Phishing From Iran

John Scott-Railton and Katie Kleemola

Scott-Railton, John and Katie Kleemola. *London Calling: Two-Factor Authentication Phishing From Iran.* Citizen Lab, University of Toronto, August 27, 2015.
https://citizenlab.ca/2015/08/iran_two_factor_phishing/.

Crux

This report from the Citizen Lab describes a phishing campaign against targets in the Iranian diaspora and a Western human rights activist.

Highlights

- This report describes a 2-Factor-Authentication (2FA) phishing attack against Iranian targets in the diaspora and provides extensive details regarding the operation of these attacks.
- The attacks pointed to "extensive knowledge of the targets' activities, and share infrastructure and tactics with campaigns previously linked to Iranian threat actors."

Fake Interview: The New Activity of Charming Kitten

Certfa Lab

Certfa Lab. *Fake Interview: The New Activity of Charming Kitten.* Certfa Lab, January 30, 2020.
https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/.

Crux

This report by Certfa Lab identifies a phishing attack from Charming Kitten, an Iranian hacking group that has a close relationship with the Iranian authorities and Intelligence services. This phishing campaign targeted email accounts of public figures around the world.

Highlights

- This new series of phishing attacks targeted journalists, academics, political and human rights activists. The campaign targeted two groups: Iranian dissidents and non-Iranian researchers.
- The investigation found that the attacks attempted to compromise the email accounts of the targets and get access to their contacts and networks.
- In this campaign, Charming Kitten used the identity of a former Wall Street Journal journalist, Farnaz Fassihi, and generated a fake interview request via email.
    - Within the email, there were legitimate, URL-shortened links to Fassihi's social media, the Wall Street Journal, and the DOW Jones website.
    - When clicked, the hackers can guide the victim to legitimate addresses while getting basic information about the victim's device such as IP address, the type of Operating System, and the browser.
- The second step in the attack vector was through a follow-up email. This email included an exclusive link with a file that contained the interview questions.
    - Once the target clicked the link to download the file, it redirected to another fake page to a two-step-check up domain where login credential details of their email (e.g. password and two factor authentication (2FA) code) are requested by phishing kits.
- In addition to this phishing attack, the report uncovered how Charming Kitten has participated in designing a malware for Windows devices that might be used for their future attacks.

Of Kittens and Princes: Latest Updates on Two Iranian Espionage Operations

Check Point

Check Point. *Of Kittens and Princes: Latest Updates on Two Iranian Espionage Operations*. Check Point, February 2021. https://blog.checkpoint.com/2021/02/08/of-kittens-and-princes-the-latest-updates-on-two-iranian-espionage-operations/.

Crux

This report describes a cyber-warfare and espionage campaign by the Iranian government against dissidents, minorities, and ideological exiles.

Highlight

- In two research investigations, Check Point (along with SafeBreach), "reveal how two Iran-based advanced cyber groups have been conducting ongoing, extensive attacks against opposition groups in Iran and abroad for many years" ("Domestic Kitten" and "Iffy").
- They have identified over 1,200 individuals with more than 600 successful infections under the Domestic Kitten campaign. This includes "Iran (251 victims), the United States (25 victims),

Great Britain (3 victims), Pakistan (119 victims), Afghanistan (8 victims), Turkey (1 victim), and Uzbekistan (2 victims)."

- The Infy campaign has been operating since 2007, and "previously attacked Iranian dissidents across multiple countries, Persian speaking media and diplomatic targets such as the Danish Foreign Ministry."
- Victims in this latest round of research are also global, including victims in the UK, Germany, Canada, Turkey, US, Netherlands, and Sweden.

Secondary Targets: When You Can't Punish a Journalist, Family Will Do Just Fine

Sirwan Kajjo

Kajjo, Sirwan. *Secondary Targets: When You Can't Punish a Journalist, Family Will Do Just Fine*. VOA News, undated. https://projects.voanews.com/press-freedom/secondary-targets/.

Crux

The VOA describes how journalists around the world are being intimidated through their family members who remain in their countries of origin.

Highlights

- For example, Nazenin Ansari, the managing editor of the Iranian news websites *Kayhan London* and *Kayhan Life*, where she covers Tehran, describes receiving emails and messages from Iranian authorities regarding her family in Iran and threatening to harm them.
- Targeting the relatives of journalists is proving to be one popular mechanism of intimidation of the press.
- A survey by UK-based BBC Persian shows that "of the 102 staff journalists who responded to the survey, 69 said one or more relatives in Iran had been questioned, harassed or threatened by Iranian authorities."
- The article also describes how other regimes, including China and Egypt, target family members in order to intimidate and silence nationals who have fled the country.

Kazakhstan

I Got a Letter From the Government the Other Day: Unveiling Campaign of Intimidation, Kidnapping and Malware in Kazakhstan

Eva Galperin, Cooper Quintin, Morgan Marquis-Boire, and Claudio Guarnieri

Galperin, Eva, Cooper Quintin, Morgan Marquis-Boire, and Claudio Guarnieri. *I Got a Letter From the Government the Other Day: Unveiling Campaign of Intimidation, Kidnapping and Malware in Kazakhstan.* The Electronic Frontier Foundation (EFF), August 2016. https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf.

Crux

This report analyzes malware linked to the government of Kazakhstan, which targeted exiled journalists, political activists, and lawyers.

Highlights

- This report from EFF covers a phishing and malware campaign that they named "Operational Manul," which was likely to have been carried out on behalf of the government of Kazakhstan. The campaign targeted exiled dissidents in Europe, their family members, known associates, and their lawyers.
- Links have been found between this campaign and other campaigns that have been referred to an Indian security company called Appin Security Group. There are also possible links between this campaign and "Arcanum Global Intelligence, a private intelligence company with headquarters in Zurich, which was allegedly hired by the government of Kazakhstan to perform a surveillance and data extraction operation against a high profile dissident."
- The emails sent to the targets contained invoices or legal documents with an attachment containing a blurry image.
- Several victims of Operation Manul also claimed other types of targeting. For example, being physically followed, home break-ins, or being tracked using GPS devices.
- Operation Manul appears to primarily use two different commercially available malware families: JRat and Bandook.
    - JRat is a commercially available remote access tool, and it "is a cross platform RAT, able to target hosts running Windows, OSX, Linux, BSD, and even Solaris."
    - JRat modules include the following functionality: "keylogging, reverse proxy, password recovery, turning on the host webcam, disabling webcam indicator light, listing host processes, opening a shell on the host, editing the host registry, and even chatting with the remote host. JRat also provides a controller application, which is written in Java. This controller application allows the attacker to manage all of their JRat instances and view uptime, operating system, and other information about all infected hosts." It also provides a web version of the controller.
    - Unlike JRat, Bandook is only able to target Windows computers.
    - The following features were identified in the Bandook version used in this campaign: "screen capture, webcam recording, audio recording, file search, creation, deleting and exfiltration, spawn a shell, get list of available Wireless networks, get list of MTP devices, and monitor USB devices."

Palestine

Taking Action Against Hackers in Palestine

Mike Dvilyanski and David Agranovich

Dvilyanski, Mike and David Agranovich. *Taking Action Against Hackers in Palestine*. Facebook, April 21, 2021. https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/.

Crux

Facebook published information regarding actions taken against two hacker groups in Palestine. One was a network linked to the Preventive Security Service (PSS) and another a threat actor known as Arid Viper. It removed their ability to use Facebook infrastructure, distribute malware, and hack people.

Highlights

- Facebook noted that the threat actor linked to PSS targeted "audiences in the Palestinian territories and Syria and to a lesser extent Turkey, Iraq, Lebanon and Libya."
- It focused on a "wide range of targets, including journalists, people opposing the Fatah-led government, human rights activists and military groups including the Syrian opposition and Iraqi military. They used their own low-sophistication malware disguised as secure chat applications, in addition to malware tools openly available on the internet."

Saudi Arabia

NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident

Bill Marczak, John Scott-Railton, and Ron Deibert

Marczak, Bill, John Scott-Railton, and Ron Deibert. *NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident.* Citizen Lab, University of Toronto, July 31, 2018. https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/.

Crux

Citizen Lab corroborates Amnesty International's conclusion that one of Amnesty International's researchers, as well as a Saudi activist based abroad, were targeted with NSO Group Pegasus spyware.

Highlights

- Amnesty International shared SMS and WhatsApp messages received by the targets with the Citizen Lab. The domain names in the messages appeared to be part of NSO Group's infrastructure, which was put into place after the Citizen Lab's initial reporting on the company in August 2016. The report concludes that if the targets had clicked on the links, their phones would likely have been infected with NSO Group's Pegasus spyware.
- This report also provides a review of Citizen Lab's findings regarding how the NSO Group infrastructure works based on leaked NSO Group Pegasus documentation and prior reporting on NSO Group by Citizen Lab.
- Citizen Lab identifies NSO infrastructure through digital fingerprints. Citizen Lab has identified three different fingerprints (or versions) of NSO Group infrastructure.

Amnesty International Among Targets of NSO-Powered Campaign

Amnesty International

Amnesty International. *Amnesty International Among Targets of NSO-powered Campaign.* Amnesty International, August 1, 2018. https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.

Crux

This Amnesty International report details the investigation into how an Amnesty International researcher and a Saudi activist who is based abroad were targeted with an NSO Group campaign. They both were targeted with Saudi Arabia-related bait content carrying malicious links sent via a WhatsApp message. Through their technical investigation, Amnesty found connections with infrastructure they believe to be linked to NSO Group.

Highlights

- The malicious message was crafted in an attempt to trick the Amnesty International staff member to click it. NSO Group documents describe this as an "enhanced social engineering message (ESEM)."
    - The phone number that sent this message belongs to a commercial provider that offers a virtual phone number management system for bulk SMS messages. These are normally used for promotional campaigns and automated systems. The domain name belongs to network infrastructure previously linked to NSO Group by Citizen Lab.
- The Saudi activist also received a malicious SMS message with a shortened link. The text used an Amnesty International headline verbatim in an effort to get the activist to click the link.
    - Amnesty International found that this domain was connected to the same infrastructure that was involved in the targeting of an Amnesty International staff member.
- Amnesty International uses this case to demonstrate how the unregulated and unchecked use of surveillance technology can have a serious chilling effect on civil society.

The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil

Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert

Marczak, Bill, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert. *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*. Citizen Lab, University of Toronto, October 1, 2018. https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

Crux

This Citizen Lab report examines the case of Saudi dissident and Canadian permanent resident, Omar Abdulaziz. He was targeted with a fake mail package delivery notification text message. The Citizen

Lab attributes this suspected infection, with a high degree of confidence, to a Saudi operator of NSO Group's Pegasus spyware.

Highlights

- Omar Abdulaziz has been outspoken on an ongoing diplomatic feud over human rights issues between Canada and Saudi Arabia. The targeting occurred while Abdulaziz, who received asylum in Canada, was attending university in Quebec. He has been a target of great interest to the Saudi government for several years. The Saudi government has tried to discourage his advocacy by revoking his scholarship to study in Canada in 2013, and threatening his family and friends in 2018.
- In Citizen Lab's September 2018 report, Hide and Seek: Tracking NSO Group's Pegasus Spyware to 45 Countries, they located a suspected infection in Quebec, Canada operated by what they inferred was a Saudi Arabia-linked Pegasus operator. Researchers matched the pattern of infection to Abdulaziz's movements and found a text message with an infected link that looked like a notification from a mail package tracker.
- Citizen Lab was not aware of any legal authorization for the infection and monitoring of Abdulaziz in Canada by a foreign government. This means that the operators may have committed *Criminal Code* offences because these actions were not properly authorized under Canadian law.
- Further, Abdulaziz had also been in close contact with murdered Saudi journalist Jamal Khashoggi. In a lawsuit filed by Abdulaziz after this targeting was discovered, he claimed "that in the months before the killing, the Saudi authorities had access to Mr. Khashoggi's communications with Mr. Abdulaziz by infecting Mr. Abdulaziz's phone with Pegasus spyware."

Syria

Behind the Syrian Conflict's Digital Frontlines

Daniel Regalado, Nart Villeneuve, and John Scott-Railton

Regalado, Daniel, Nart Villeneuve, and John Scott-Railton. *Behind the Syrian Conflict's Digital Frontlines.* Fire Eye, February, 2015. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf.

Crux

Between 2013 and 2014, hackers stole a cache of documents and Skype conversations regarding the Syrian opposition's "strategy, tactical battle plans, supply needs. It stole "troves of personal information and chat sessions belonging to the men fighting against Syrian President Bashar al-Assad's forces" (4). This report describes technical details regarding the operation, and the victims.

Highlights

- The stolen data ranged from "Skype account databases to planning documents and spreadsheets to photos." The majority of the data was created by victims between May 2013 and December 2013. Some of the Skype databases included data from as far back as 2012. The

nature of the stolen information included military, political, humanitarian activities and financing, refugee personal information, and media communications (6).

- The victims of the attack served in various roles in the opposition. Most targets were inside Syria, but there were also targets in Lebanon, Ukraine, Jordan, Egypt, Spain, the UAE and Turkey (10).
- The primary mechanism for the cyber attack was the use of “female avatars” to start conversations on Skype and on Facebook. The attackers also “used a fake, pro-opposition website seeded with malicious content” (11).
- In conclusion, the report authors observed that the activity in question was not just “cyber espionage aimed at achieving an information edge or a strategic goal. Rather, this activity, which takes place in the heat of a conflict, provides actionable military intelligence for an immediate battlefield advantage” (18).

Group5: Syria and the Iranian Connection

John Scott-Railton, Bahr Abdul Razzak, Adam Hulcoop, Matt Brooks, and Katie Kleemola

Scott-Railton, John, Bahr Abdul Razzak, Adam Hulcoop, Matt Brooks, and Katie Kleemola. *Group5: Syria and the Iranian Connection.* Citizen Lab, University of Toronto, August 2, 2016. https://citizenlab.ca/2016/08/group5-syria/.

Crux

This report analyzes an organized malware attack using a range of techniques aimed at Windows computers and Android phones in an attempt to penetrate the computers of well-connected individuals in the Syrian opposition.

Highlights

- In late 2015, an exiled member of the Syrian opposition reported a suspicious email containing a PowerPoint slideshow. The email led Citizen Lab to uncover a watering hole website with malicious programs, malicious PowerPoint files, and Android malware, all apparently designed to appeal to members of the opposition.
- The Citizen Lab called the attackers “Group5,” which was intended to reflect that four other known malware groups have targeted Syrian dissidents since the early days of the conflict (in particular, regime-linked malware groups, the Syrian Electronic Army, ISIS, and a group linked to Lebanon reported by FireEye in 2015.)
- Group5 is distinguishable from prior operations previously reported in the following ways: “some of the tactics and tools used have not been observed in this conflict; the operators seem comfortable with Iranian Persian dialect tools and Iranian hosting companies; and they appear to have run elements of the operation from Iranian IP space.”
- Group5 borrowed the Syrian opposition text and slogans for email messages and watering holes, showing evidence of good social engineering and targeting.
- The target received an email from an unknown human rights organization “Assad Crimes.” The sender, using the e-mail address office@assadcrimes[.]info, claimed to be sharing information about Iranian “crimes." The email also included an attached Microsoft PowerPoint Slideshow (PPSX) document that, when clicked, directly opens and runs a PowerPoint slideshow.

- Al-Ameer (the target)'s own name was used in the assad crimes[.]info domain registration, along with other false information. While entering the website, several directories had been identified that auto-download a further malicious file (assadcrimes.info.ppsx). These links seem designed for other forms of social engineering.
- Android malware also was identified in the website, seeded via a fake Adobe Flash Player update notification.
- The website contained several HTML pages that, when visited, triggered the downloading of a malicious executable. When executed, the program pulls images hosted on while simultaneously infecting the target machine with malware.
- In this malware operation, Group5 used a range of attacks from malicious PowerPoint slideshows using exploits to executable files that directly drop malware.

Tibet

Tibetan Uprising Day Malware Attacks

Katie Kleemola, Masashi Crete-Nishihata, and John Scott-Railton

Kleemola, Katie, Masashi Crete-Nishihata, and John Scott-Railton. *Tibetan Uprising Day Malware Attacks.* Citizen Lab, University of Toronto. March 10, 2015. https://citizenlab.ca/2015/03/tibetan-uprising-day-malware-attacks/.

Crux

This report documents how hundreds of members of the Tibetan community were targeted using email-based malware that leveraged the anniversary of the March 10, 1959 Tibetan Uprising.

Highlights

- The March 10, 1959 Tibetan Uprising is a significant event in the Tibetan diaspora, which is commemorated with a day of global protesting. Attacks leveraged heightened activity around this time to launch social-engineered, targeted malware attacks. This report considers two March 10th anniversary related cyber attacks.
- The first attack used a malware family, which the Citizen Lab named "MsAttacker." It was done using an email titled '10th March 2015 campaign for Tibet' and sent to hundreds of individuals in the Tibetan community. The email included a malicious .doc file and an exploit. Once downloaded, the malware connected to a command and control server in China.
- Another attack was undertaken using the "ShadowNet" malware family and command and control infrastructure related to previous campaigns that have targeted the Tibetan community. It was also executed using an email with a malicious .doc file.

Shifting Tactics: Tracking Changes in Years-Long Espionage Campaign Against Tibetans

Jakub Dalek, Masashi Crete-Nishihata, and John Scott-Railton

Dalek, Jakub, Masashi Crete-Nishihata, and John Scott-Railton. *Shifting Tactics: Tracking Changes in Years-Long Espionage Campaign Against Tibetans.* Citizen Lab, University of Toronto, March 10, 2016. https://citizenlab.ca/2016/03/shifting-tactics/

Crux

This report examines "a malware campaign active between January to March 2018 that targeted Tibetan activists, journalists, members of the Tibetan Parliament in exile, and the Central Tibetan Administration." The report notes how the attackers continuously shift their tactics to their targets. They are often highly sophisticated in social engineering but typically are not technically advanced. When the Tibetan community was "promoting a move from sharing attachments via e-mail to using cloud-based file sharing alternatives such as Google Drive" the attack vector changed to target new behaviours.

Highlights

- Citizen Lab "connect[s] the attack group's infrastructure and techniques to a group previously identified by Palo Alto Networks, which they named Scarlet Mimic."
- The report demonstrates how "servers used as malware C2 infrastructure by Scarlet Mimic are now hosting phishing pages designed to steal Google credentials from Tibetan activists and journalists."
- At the time of the report, Scarlet Mimic has been active for four years. They use well-known vulnerabilities (e.g. CVE-2012-0158&lt and CVE-2010-3333) and the "FakeM" malware family, "which attempts to disguise its malicious traffic as commonly used protocols."
- While previous campaigns used document-based malware attacks, Scarlet Mimic's C2 infrastructure was "repurposed to host phishing attacks against the TIbetan community."
    - The social engineered email shared a malicious link to a lookalike Google login page. "If a victim enters their credentials, the data is sent to the attackers via an HTTP POST."
    - Once credentials are entered, they are redirected to decoy content geared towards the victim.
- "When Scarlet Mimic shifted tactics, they failed to properly compartmentalize their phishing and malware operations, relying on known C2 infrastructure for the new phishing campaigns" — allowing Citizen Lab to track the campaign over time through infrastructure analysis.

Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community

Masashi Crete-Nishihata, Jakub Dalek, Etienne Maynier, and John Scott-Railton

Crete-Nishihata, Masashi, Jakub Dalek, Etienne Maynier, and John Scott-Railton. *Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community*. Citizen Lab, University of Toronto, January 30, 2018.
https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/

Crux

This report examines an extensive but simplistic phishing operation that targets the Tibetan community, "and potentially other groups including ethnic minorities, social movements related to China, a media group, and government agencies in South and Southeast Asia." This operation was simple, inexpensive, and only required basic system administration and web development skills. Digital security practices such as two-factor authentication could have blunted the phishing tactic.

Highlights

- The phishing operation ran for 19 months and "used a range of phishing tactics including pages impersonating popular email provider logins, custom webmail login pages to target specific providers and organizations, and malicious OAuth applications for harvesting Google credentials."
    - "Open Authentication (OAuth) is a protocol designed for access delegation and has become a popular way for major platforms (e.g., Facebook, Google, Twitter, etc.) to permit sharing of account information with third party applications."
- The sender would use general social engineering tactics to increase the credibility of the message. In the email, it would include a link to a login phishing page that would lead to decoy content. The majority of decoy content collected (96%) was hosted on Google Drive.
- Decoy documents had diverse themes but "[a] commonality across these themes is that they are all of political interest to the government of China" such as:
    - Tibetan politics and culture but also around ethnic minorities (Uyghurs), Falun Gong-related media (Epoch Times), South Asian and Southeast Asian governmental agencies, and "other decoy content referenced Hong Kong-based companies and a mail provider operated by a Burmese Internet Service Provider."

Familiar Feeling: A Malware Campaign Targeting the Tibetan Diaspora Resurfaces

Geoffrey Alexander, Matt Brooks, Masashi Crete-Nishihata, Etienne Maynier, John Scott-Railton, and Ron Deibert

Alexander, Geoffrey, Matt Brooks, Masashi Crete-Nishihata, Etienne Maynier, John Scott-Railton, and Ron Deibert. *Familiar Feeling: A Malware Campaign Targeting the Tibetan Diaspora Resurfaces.* Citizen Lab, University of Toronto, August 8, 2018.
https://citizenlab.ca/2018/08/familiar-feeling-a-malware-campaign-targeting-the-tibetan-diaspora-resurfaces/.

Crux

This Citizen Lab report considers a malware campaign between January to March 2018 targeting Tibetan activists, journalists, members of the Tibetan Parliament in exile and the Central Tibetan Administration.

Highlights

- The campaign used social engineering to trick targets to open exploit-laden PowerPoint and Microsoft Rich Text Format documents attached to email messages. This campaign had connections to a 2016 malware campaign that targeted Tibetan Parliamentarians.

- The report observes that the “threat of digital espionage has become a persistent reality for the Tibetan diaspora, which has been targeted by malware campaigns for over a decade.”
- Historically, these campaigns relied on “known exploits and Remote Access Trojans”. However, Citizen Lab has observed a shift towards phishing attacks designed to harvest credentials from online accounts.
- The report also notes that these campaigns originated from a “closed espionage ecosystem” in which parties involved are difficult to identify and segment.

Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits

Bill Marczak, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert

Marczak, Bill, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert. *Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits*. Citizen Lab, University of Toronto, September 24, 2019. https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/.

Crux

This report describes the targeting of senior members of Tibetan groups with malicious links sent in individually tailored WhatsApp text exchanges with operators posing as NGO workers, journalists, and other fake personas between November 2018 and May 2019. It is the first documented case of one-click mobile exploits used to target Tibetan groups and reflects an escalation in the sophistication of digital espionage threats faced by the community.

Highlights

- The Tibetan community has over a decade long history of being targeted with digital espionage (see TrackingGhostNet, below). Over the past decade, the tactics used have become familiar to Tibetans: emails laden with older exploits used to deliver custom malware to unpatched computers.
- This report documents a shift in tactics seemingly tied to the defensive posture of the community. Malware sent by email attachment used to be the most common threat; in response, groups in the community promoted user awareness. Subsequently, one observed a drop in malware campaigns against Tibetan groups and a rise in credential phishing, suggesting that operators were changing tactics.
- There is an asymmetry between the digital defenses of Tibetan groups and the capabilities of operators. Changing community behavior is a slow process, while an adversary can evolve overnight. In response to this, Tibetan groups formed the Tibetan Computer Emergency Readiness Team (TibCERT).
- In November 2018, TibCERT was notified of suspicious WhatsApp messages sent to senior members of Tibetan groups. These samples were shared with Citizen Lab, which concluded that the messages included links designed to exploit and install spyware on iPhone and Android devices. The campaign appeared to be carried out by a single operator the report calls “POISON CARP.” POISON CARP was linked to two other reported digital espionage campaigns targeting Uyghur groups.

United Arab Emirates

The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender

Bill Marczak and John Scott-Railton

Marczak, Bill and John Scott-Railton. *The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender.* Citizen Lab, University of Toronto, August 24, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Crux

This Citizen Lab report describes how Ahmed Mansoor, a human rights defender in the United Arab Emirates, was targeted with NSO Group's Pegasus spyware. Mansoor received text messages with links that were determined to lead to a chain of zero-day exploits (named "Trident" by the researchers) that would have remotely jailbroken Mansoor's iPhone 6 and installed spyware. His phone would have become a spy in his pocket, capable of using his iPhone camera and microphone, recording WhatsApp and Viber calls, loggings messages sent in mobile chat apps, and tracking movement.

Highlights

- This report demonstrates that not all state-sponsored spyware campaigns utilise "just enough" technical means coupled with carefully planned deception, as previous Citizen Lab research had shown. Exploits, such as the one used in this case, are rare, expensive, and technically sophisticated.
- The likely operator behind this targeting was the UAE in light of the high cost of the exploit at issue, the use of a tool sold exclusively to governments, and prior targeting of Mansoor by the UAE. Mansoor had also been targeted with Hacking Team and FinFisher spyware.
- According to documents in the Hacking Team materials, NSO Group offers two remote installation vectors for spyware onto a device: zero-click or one-click vectors.
- The spyware used against Mansoor confirmed a number of the spyware capabilities advertised in NSO Group documentation. Namely, researchers observed indications that the collection of the following types of data was supported: calls made by phone, WhatsApp, and Viber; SMS message and messages/other data from other applications like Gmail, WhatsApp, and Skype; and a wide range of personal data such as calendar data and contact lists and passwords (including WiFi).
- This report also sets out how a prior investigation by Citizen Lab into the mobile attack infrastructure of a threat actor named "Stealth Falcon," who was targeting individuals critical of the UAE government at home and abroad, was linked to NSO Group.
- Researchers linked a number of IPs and domain names to what appeared to be the NSO Group exploit infrastructure. These domain names were coded and the most common theme found was the use of news media in an attempt to get targets to click on spyware links.

The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit

Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert

Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert. *The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit*. Citizen Lab, University of Toronto, December 20, 2020. https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.

Highlight

NSO Group's Pegasus spyware was linked to the hacking of the phones of multiple journalists at Al-Jazeera and a journalist at London-based Al Araby TV.

Crux

- In July and August 2020, government operatives used NSO Group's Pegasus spyware to hack 36 personal phones belonging to journalists, producers, anchors, and executives at Al Jazeera. The personal phone of a journalist at London-based Al Araby TV was also hacked.
- The phones were compromised using an exploit chain that we call KISMET, which appears to involve an invisible zero-click exploit in iMessage. In July 2020, KISMET was a zero-day against at least iOS 13.5.1 and could hack Apple's then-latest iPhone 11.
- Based on logs from compromised phones, Citizen Lab believes that NSO Group customers also successfully deployed KISMET or a related zero-click, zero-day exploit between October and December 2019.
- The journalists were hacked by four Pegasus operators, including one operator MONARCHY attributed to Saudi Arabia, and one operator SNEAKY KESTREL that was attributed to the United Arab Emirates.
- Infrastructure used in these attacks included servers in Germany, France, UK, and Italy using cloud providers Aruba, Choopa, CloudSigma, and DigitalOcean.

Academic Articles & Research Reports

General/Theory

Authoritarianism Goes Global: Cyberspace Under Siege

Ronald Deibert

Deibert, Ronald. "Authoritarianism Goes Global: Cyberspace Under Siege." *Journal of Democracy* 26, no. 3 (2015): 64-78. https://doi.org/10.1353/jod.2015.0051.

Crux

Authoritarian regimes are "actively shaping cyberspace to their own strategic advantage." This article describes the arsenal of tools developed by authoritarian states who engage in "cyberspace authoritarianism."

Highlights

- The article describes three categories of information controls: first, second and third generation controls.
    - "First-generation controls tend to be 'defensive,' and involve erecting national cyberborders that limit citizens' access to information from abroad" (65).
    - "Second-generation controls are best thought of as deepening and extending information controls into society through laws, regulations, or requirements that force the private sector to do the state's bidding" (66).
    - "Third-generation controls are the hardest to document, but may be the most effective. They involve surveillance, targeted espionage, and other types of covert disruptions in cyberspace. While first-generation controls are defensive and second-generation controls probe deeper into society, third-generation controls are *offensive*" (68).
    - A fourth generation might be added to the three ones. This comes in the form of a more assertive authoritarianism at the international level (70).
- These third-generation information controls include, for example, the deployment of cyberespionage campaigns by China against "human-rights, prodemocracy, and independence movements outside China" (68).
- Other states may not be able to match China's cyberespionage or online-attack capabilities, but they do have options. Some might buy off-the-shelf espionage "solutions" from Western companies such as the United Kingdom's Gamma Group or Italy's Hacking Team—each of which Citizen Lab research has linked to dozens of authoritarian-government clients (69).
- In other countries; like Syria, security services and extreme groups such as ISIS are borrowing cybercriminals' targeted-attack techniques, downloading crude but effective tradecraft from open source and then using it to infiltrate opposition groups (69).

Intervention: Extraterritorial Authoritarian Power

Emanuela Dalmasso, Adele Del Sordi, Marlies Glasius, Nicole Hirt, Marcus Michaelsen, Abdulkader S. Mohammad & Dana Moss

Dalmasso, Emanuela, Adele Del Sordi, Marlies Glasius, Nicole Hirt, Marcus Michaelsen, Abdulkader S. Mohammad, and Dana Moss. "Intervention: Extraterritorial Authoritarian Power." *Political Geography* (2017): 1-10. https://doi.org/10.1016/j.polgeo.2017.07.003.

Crux

This article introduces a series of arguments regarding extraterritorial authoritarian power. Moss and Michaelsen, in particular, focus on the digital dimensions of such exercise of repressive power.

Highlights

- Glasius observes that the "authoritarianism literature … continues to leave its territorial assumptions unexamined" and has focused on domestic and comparative analysis (1). This leaves an "'extraterritorial gap': an inability to perceive and analyze extraterritorial state power in general, and extraterritorial authoritarian power in particular" (1).
- In this series of papers, the authors "show how authoritarian rule from the home state continues to be exercised over populations abroad, through the practices authoritarian regimes have developed to manage and offset risks mobility poses to them. As a consequence, contemporary authoritarian rule structures socio-political space in ways that partially transcend territorial jurisdiction and physical distance" (2).
- The literature observes that "extraterritorial repression is more pervasive" today "and authoritarian states have various functional equivalents to physical control at their disposal." "Authoritarian states can exert control in the digital sphere, hacking social media accounts, obtaining confidential information, planting malware or sending death threats. And they can exert control and induce fear via relatives still in the country" (2).
- Moss and Michaelsen observe that "[t]ransnational repression' has been a long-standing, though largely overlooked, problem for diasporas with ties to authoritarian sending-states … Traditional means of spying, the assassinations of prominent activists, and retribution against dissidents' families and colleagues at home have haunted numerous émigré communities … Activists' use of social media in the digital age further increase their visibility and exposure to regimes intent on countering dissent in the diaspora. Regimes have also adopted these communication technologies to identify and track dissident networks, monitor their activities, hack and deface social media accounts and websites, plant malware, phish for confidential information, steal identities, and transmit private and public threats … This proliferation of digital communication technologies has therefore not only expanded the activist toolkit, but the state's repressive repertoire as well" (3).
- The authors observe that "[d]igitally-enabled repression may not deter public advocacy by exiles who have long made their views public, but it poses significant threats to dissidents' relatives and members of clandestine advocacy networks. In addition, these threats deter the wider diaspora who wish to avoid being caught in the blacklisting dragnet from expressing their views. Although regime opponents in the diaspora may enjoy relative freedoms in the host country and unfettered access to platforms such as YouTube, Twitter and Facebook, they face serious dilemmas when using these technologies to contest abuses at home" (4).

Extraterritorial Authoritarian Practices: A Framework

Marlies Glasius

Glasius, Marlies. "Extraterritorial Authoritarian Practices: A Framework." *Globalizations* 15, no. 2 (2018): 179-197. https://doi.org/10.1080/14747731.2017.1403781.

Crux

This article, which introduces a *Special Edition* on the topic of extraterritorial authoritarian practices, "develops a new theory to better understand how authoritarian rule is exercised over populations abroad and to connect this extraterritorial dimension to the character and resilience of contemporary authoritarian rule" (179). This article summaries the evolution of authoritarianism literature,

introduces the articles in the *Special Edition*, develops the theoretical framework, illustrates concrete state practices based on case studies, and identifies further areas for research (180). The author "concludes that authoritarian rule should not be considered a territorially bounded regime type, but rather as a mode of governing people through a distinct set of practices" (179).

Highlights

- This series of articles attempts to transcend the "separation between the study of migration and the study of authoritarianism, to better understand how authoritarian rule is exercised over populations abroad and to connect this extraterritorial dimension to the character and resilience of contemporary authoritarian rule" (179).
- This paper series presents "six country case studies: on the response to political dissidents abroad by Iran and Syria; on the handling of large-scale migration and remittances by Eritrea and Morocco; on the sponsorship of study abroad and the governance of their return by Kazakhstan; and on the Russian distribution of passports to help stabilize its rule over Crimea" (179-180).
- The articles "eschew the methodological nationalism … of authoritarianism studies, showing how authoritarian practices today rest on a conception of the state as a collection of people to be governed, more than as a territorial entity. They also challenge the liberal bias of the migration literature, showing that citizenship is not an appropriate lens for understanding the authoritarian emigrant state" (180).
- The articles show that "the authoritarian state approaches its populations abroad, and includes or excludes them, as subjects to be repressed and extorted, as clients to be co-opted, or as patriots to be discursively manipulated" (180).
- "The theoretical framework presented here intersects the 'authoritarian pillars of stabilization' repression, co-optation and legitimation … with the 'state controls of transnational space' theorized by Collyer and King … and the concepts of inclusion and exclusion commonly used in migration and citizenship studies" (180).

Suppressing Transnationalism: Bringing Constraints Into the Study of Transnational Political Action

Ali R. Chaudhary & Dana M. Moss

Chaudhary, Ali R. and Dana M. Moss. "Suppressing Transnationalism: Bringing Constraints Into the Study of Transnational Political Action." *Comparative Migration Studies* 7, no. 9 (2019). https://doi.org/10.1186/s40878-019-0112-z.

Crux

This article offers an overview of how immigrants and diaspora groups engage in transnational political action (TPA) and how socio-political circumstances can restrict TPA. It proposes a theoretical framework to understand these constraints.

Highlights

- The authors note that there has been limited research on how socio-political forces can constrain TPA among immigrant/diaspora communities (1). This theoretical article "presents a

framework to account for the conditions and factors that constrain immigrant and diaspora TPA" (1).

- The authors illustrate how decisions to opt-out of political activity is not just apathy, and "illustrate how demobilization and refraining from TPA are produced by hostile sociopolitical forces that circumscribe transnational action. These forces include the policies and practices of origin and receiving-country governments, as well as the broader sociopolitical contexts of reception in which immigrants are embedded" (2).
- The framework of constraint elaborated by the authors refers to "four major causal conditions and mechanisms": "(1) geopolitics and interstate relations; (2) origin-country authoritarianism; (3) weak origin-country governance; and (4) exclusionary contexts of reception" (2, 8).
- The second constraint factor, origin-country authoritarianism, focuses on the fact that "authoritarian regimes actively work to repress and control their diasporas" (11).
- The authors find that "origin-country regimes that are intolerant of protest within their borders are also likely to be intolerant of oppositional mobilization by their nationals abroad...Because such authorities often view immigrant mobilization as a threat, they constrain TPA by targeting diaspora activists and organizations with slander, threats, and even violence" (11).

A Tightening Grip Abroad: Authoritarian Regimes Target Their Emigrant and Diaspora Communities

Gerasimos Tsourapas

Tsourapas, Gerasimos. *A Tightening Grip Abroad: Authoritarian Regimes Target Their Emigrant and Diaspora Communities.* Migration Policy, 2019. https://www.migrationpolicy.org/article/authoritarian-regimes-target-their-emigrant-and-diaspora-communities.

Crux

This article discusses how transnational authoritarianism is widespread, with many cases left out of the public eye. It builds upon James F. Hollifield's "liberal paradox" framework where there is a tension between the economic benefits of immigration versus the security and political risks it brings. Using this framework, an "illiberal paradox" refers to the tension between emigration and political and security risks in authoritarian regimes. The author argues that transnational authoritarianism to control dissent allows regimes to benefit from the economic exchange of emigration, while reducing political and security risks.

Highlights

- Common strategies authoritarian regimes use to control the "illiberal paradox" include emigration restrictions (e.g., exit visas, restricting dissidents from leaving, or more extreme forms like forced labour in re-education camps in the case of North Korea) or transnational authoritarianism (controlling dissent abroad).
    - The decision to use either strategy "depends on the developmental value that an authoritarian state ascribes to emigration."

- Transnational authoritarianism generally takes three forms:
    - States may engage in transnational authoritarianism directly (e.g. killing, kidnapping, monitoring, threatening family members, hacking, or entering interstate cooperation agreements for extradition treaties or to share information)
    - Multilateral organizations (regional or international) can be used to diffuse repressive measures.
    - Non-state actors may be implicated in transnational authoritarianism (e.g. using "threats, intimidation, and violence against rival migrants and diaspora organizations they see as competitors.")

At Home and Abroad: Coercion-By-Proxy As a Tool of Transnational Repression

Fiona B. Adamson and Gerasimos Tsourapas

Adamson, Fiona B. and Gerasimos Tsourapas. *At Home and Abroad: Coercion-by-Proxy as a Tool of Transnational Repression*. Freedom House, 2020. https://freedomhouse.org/report/special-report/2020/home-and-abroad-coercion-proxy-tool-transnational-repression.

Crux

This article describes how authoritarian regimes engage in transnational repression using tools that have facilitated its global nature (e.g. ICTs) and in particular engage in transnational repression through coercion-by-proxy, i.e. by pursuing the family members of diaspora activists who remain within the boundaries of the country.

Highlights

- The article notes how "[t]ransnational authoritarianism is characterized by the breaking down of the boundaries between state-led domestic forms of control over citizens living 'at home' and long-distance forms of repression targeting those who reside 'abroad.' When an authoritarian state employs strategies of transnational repression, it seeks to coerce those living outside its legal borders."
- Strategies can include "harassment, surveillance, enactment of mobility restrictions, or even more serious instances of kidnapping, physical attack, or assassination." They may also target family members, for example, living in the country as a form of "long-distance coercion-by-proxy."
- The authors note that it is "new" and of "particular interest" that these strategies of repression have "gone global":
    - "For one, international migration has facilitated citizens' mobility into and out of autocratic states. At the same time, new information and communications technologies (ICTs) have led to the globalization of many aspects of domestic politics, and the rise of diaspora politics. Diasporic activism operates largely outside the jurisdiction of the state of origin and has therefore often been assumed to be a space of opportunity for political opposition movements and groups, where they can operate without interference from homeland state authorities."

- The authors further note that "the transnationalization of politics has been accompanied by the transnationalization of family ties, social relations, and social networks, which perversely has provided an additional source of leverage for states to engage in transnational repression. New forms of digital surveillance—such as monitoring of social media accounts, private communications, and text messages—means that authoritarian states can quickly identify ties between activists abroad and family members and acquaintances 'back home.'"

Non-State Authoritarianism and Diaspora Politics

Fiona B. Adamson

Adamson, Fiona B. "Non-State Authoritarianism and Diaspora Politics." *Global Networks* 20, no. 1 (2020): 150-169. https://doi.org/10.1111/glob.12246.

Crux

While "opposition groups and political activists can mobilize beyond the territorial limits of the state … the literature on transnational and extraterritorial repression complicates this model, for it shows that states can use strategies of 'long-distance authoritarianism' to monitor, intimidate and harass diasporic populations abroad" (150). Non-state actors may also use these same strategies to "mobilize internally, gain hegemony within the diaspora, and marginalize or eliminate internal rivals" (150). This paper thus considers whether "diaspora politics can be authoritarian" and reviews the actions of state and non-state actors (150).

Highlights

- This article provides a review of diaspora politics, discusses non-state authoritarianism and transnational repression, reviews the types of transnational repressive practices utilized by states and non-state actors, and provides specific examples of state and non-state actors using these tactics (151).
- The relationship between "diaspora politics and authoritarianism is more complex than some of the literature suggests" (153). In particular, "[t]he location of diasporic spaces outside the physical boundaries of the state does not necessarily remove them from the pressures and effects of state authoritarianism. Rather, state repressive power can extend into the spaces of other states and take the form of 'transnational' or 'extraterritorial' repression, acting as a 'long-distance' deterrent to political organizing and posing a threat to populations living abroad" (153).

The Digital Transnational Repression Toolkit, and Its Silencing Effects

Marcus Michaelsen

Michaelsen, Marcus. *The Digital Transnational Repression Toolkit, and Its Silencing Effects*. Freedom House, 2020. https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects.

Crux

This article explains how digital tools facilitate transnational surveillance efforts by repressive regimes and make it easier for such governments to "control, silence, and punish dissent across borders." It also highlights the impact of the deployment of such tools against civil society in exile and advises on how host countries could provide greater protection.

Highlights

- The author observes that "[d]igital tools have...become essential components in the toolkit of transnational repression". While civil society has benefited from new technologies, their capacity to protect themselves against exploitation of this technology by authoritarian regimes is limited.
- Governments have begun to deploy "more aggressive measures of targeted surveillance" in light of activists' attempts to protect themselves using methods like encryption. "By penetrating computers, mobile devices, email, and social media accounts, they aim to gain access to confidential communications and contacts. Attacks often involve some form of social engineering, with perpetrators working to trick targets into opening a malicious link or attachment by impersonating a friend or an organization associated with their field of expertise. Such phishing attempts have been delivered via invitations to seminars, files on human rights violations, and interview requests, not only through email but also in messages on Facebook, WhatsApp, and other channels."
- Some regimes use "large-scale phishing campaigns against civil society, both inside and outside their territory." While not particularly technically sophisticated, this approach relies on "assiduous information gathering and target manipulation--tasks that the intelligence organizations of authoritarian regimes are well versed in. Attacks build on ties among activists to unravel entire groups and networks. In order to encircle high-profile targets, regime agents try to infiltrate the accounts of lesser-known and inexperienced users in activist networks--or even family members." The author also describes other techniques used by states, such as online harassment.
- The author observes that such digital tools allow the state to expand its authoritarian activities outside the nation state and notes the numerous effects of such transnational repressive activities on the diaspora.
    - For example, "[t]he knowledge or assumption of ongoing regime surveillance pushes many activists towards self-censorship. The uncertainty about the capabilities of monitoring authorities and the scope of their activities clearly has a chilling effect."
    - Further, such regimes are able to "intervene in activists' everyday routines and constrain some of the dynamics, impacts, and outreach of diaspora activism." It also causes targets to "carefully manage their ties to the home country" and "puts activists under pressure to effectively protect their contacts and communications."
    - There are also psychological effects to such activities. For example, the "risk of mental stress and burnout is even higher for activists targeted by online harassment and hate speech."

- The article notes that there are serious issues of accountability. In particular, "[d]igital threats are often carried out with little chance to identify perpetrators and hold them to account. Moreover, regimes can escalate these threats into other forms of transnational repression in the attempt to punish exiled dissidents for crossing a red line and shut them up."
- The article advises on how to counter these issues:
    - Strengthening and supporting the digital security practices of civil society members
    - Limiting the proliferation of cyber tools
    - Providing support to political emigrants who are harassed and threatened
    - Documentation by media and human rights organizations of such practices and awareness-raising
    - Developing legal instruments to counter such repressive activities (e.g. cyberlaw)

The Importance of Defending Diaspora Activism for Democracy and Human Rights

Dana M. Moss

Moss, Dana M.. *The Importance of Defending Diaspora Activism for Democracy and Human Rights*. Freedom House, 2020. https://freedomhouse.org/report/special-report/2020/importance-defending-diaspora-activism-democracy-and-human-rights.

Crux

This essay highlights the risks that pro-democracy diaspora activists face in relation to authoritarian states. It discusses how activism in the diaspora furthers democracy and human rights and how "transnational repression" undermines these efforts.

Highlights

- The article describes the role of diaspora activists in fighting for democracy and human rights. However, "transnational repression simultaneously erects a barrier to engaging lawful activism … tactics used by foreign governments to repress their critics abroad--including assassinations, the proxy punishment of family members, surveillance on- and offline, death and rape threats, and slander, among other means--cast a long shadow over diaspora communities."
- One of the consequences of transnational repression is self-censorship. "Tragically, this can lead victims of transnational repression to purposefully avoid alerting local law enforcement about threats to their personal safety." It also undermines the capacity of the diaspora to engage in independent journalism; curbs the ability of universities to ensure free speech; and makes public demonstrations in host countries a dangerous activity.
- The author also notes that transnational repression negatively impacts host countries, e.g. by undermining state sovereignty. The author makes the following recommendations for such host countries: "Local and national enforcement agencies need to be made aware of the potential threats against diaspora organizations and activists, and communicate with community leaders about how to lodge complaints. Governments must provide the fullest possible protections to diaspora activists and their organizations through legislation, which is

needed to sanction regimes for atrocities and protect diaspora communities from threats and interference."

The Repertoire of Extraterritorial Repression: Diasporas and Home States

Ahmet Erdi Öztürk & Hakkı Taş

Öztürk, Ahmet Erdi and Hakkı Taş. "The Repertoire of Extraterritorial Repression: Diasporas and Home States." *Migration Letters* 17, no. 1 (2020): 59-69. https://doi.org/10.33182/ml.v17i1.853.

Crux

This article looks at the practices of extraterritorial repression through an analysis of the case of Turkey's ruling AKP party's efforts to purge the global Gulen Movement following the failed coup of 2016. It examines the *repertoire of extraterritorial repression* (the constellation of tactics used by the Turkish Justice and Development Party (AKP)) and how this more comprehensive approach allows for further understanding of how extraterritorial repression works in practice, and how this repertoire of practices is adapted, invented and shared. This analysis of the repertoire of tactics concludes that the AKP has expanded its tactics both vertically (increased the number of actors engaged in repressive acts) and horizontally (intensifying and multiplying the instruments of repression).

Highlights

- The author reviews various tactics of transnational repression employed by the Turkish state and breaks down the 'vertical' expansion of extraterritorial repression into the following categories: abduction and extradition, confiscation, targeted violence, surveillance and profiling, negation and exclusion, negative propaganda, intimidation of relatives in the home country (62).
- Among other methods, the AKP has expanded the number of state institutions interacting with the diaspora community: intelligence, embassies, religious organizations, think-tanks, and diaspora associations. The national intelligence organization ('MIT') is reported to have used 800 operatives and 6000 informants in western Europe. Organizations such as embassies have been engaged in activities outside their traditional mandates, such as espionage and collecting intelligence (62). Further, "Turkish intelligence developed a smartphone application to be used to reveal GM members from among the Turkish diaspora" (63).
- These efforts have had the effect of isolating the GM from Turkish diaspora communities, both through cutting off the groups financial resources, and the fear of diaspora members being affiliated with the group. However, these actions also "strengthen the GM's victim status from the perspective of host countries, thus attributing greater legitimacy to its public presence" (66).

Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-Optation in World Politics

Gerasimos Tsourapas

Tsourapas, Gerasimos. “Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-Optation in World Politics.” *International Studies Review* (2020): 1-29. https://doi.org/10.1093/isr/viaa061.

Crux

This article examines how increased global migration flows contribute to transnational authoritarianism, “as autocracies aim to both maximize material gains from citizens’ ‘exit’ and minimize political risks by controlling their ‘voice’ abroad” (1). Drawing from a range of transnational authoritarian practices chosen from fifty countries categorized as “not free” by Freedom House in 2019, the author demonstrates how “autocracies employ to exercise power over populations abroad, while shedding light on the evolving nature of global authoritarianism” (1). Through this, the author identifies “four types of state-led transnational authoritarianism strategies: transnational repression, legitimation, co-optation, and co-operation with non-state actors” (3).

Highlights

- Most cases of transnational repression are out of the public eye — very few make international headlines.
- Using the works of Albert Hirschman (exit versus voice) and James Hollifield (liberal paradox), the author notes the historical evolution of transnational authoritarianism: autocracies have a contradictory need between “the desire to allow mass emigration and the urge to maintain control over political dissent” (3).
- The article notes how internet communication technologies (ICTs) and surveillance technology has contributed to the growth of extra-state repressive action.
- The author examines four types of state-led transnational authoritarianism strategies:
    1) Transnational repression: includes surveillance, threats, coercion-by-proxy, enforced disappearances, coerced return, and lethal retribution (7).
    2) Legitimation: includes sponsored patriotism across migrant and diaspora communities abroad (14-15), and exile to “undermine their claim to political legitimacy by branding them as disloyal and in effect no longer citizens” (16).
    3) Co-optation: includes patronage such as rewarding expatriates with complimentary annual return trips or offering benefits for intelligence, and blacklisting individuals at home and abroad.
    4) Co-operation with non-state actors: includes diaspora organizations (e.g. student organizations), multi-national corporations (e.g. treatment of specific employees), international organizations (e.g. cooperation councils, the International Criminal Police Organization), and Internet Communication Technologies (e.g. commercial spyware and censorship).

Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression

Nate Schenkkan and Isabel Linzer

Schenkkan, Nate and Isabel Linzer. *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression*. Freedom House, February 2021. https://freedomhouse.org/report/transnational-repression.

Crux

This report is based on a catalog of more than 600 instances of transnational repression compiled from various sources such as government documents, human rights reports, and the media, from January 2014 - November 2020. It includes 31 origin states conducting transnational repression in 79 host countries, with 160 unique origin/host pairings. It focuses on case studies from six states: China, Rwanda, Russia, Iran, SA, Turkey.

Key findings:

- Transnational repression is now a normal and common activity. "It is no longer unusual for regimes to target "their" citizens beyond their borders—it is par for the course" (4).
- Physical acts of transnational repression (two-thirds of their dataset) generally involve co-opting of host governments, effectively undermining the rule of law in host countries.
- There are currently insufficient consequences for transnational repression. It is necessary to create an "international norm of universal due process and against extraterritorial violence" (4).
- Important to examine the full spectrum of transnational repression tactics. Online harassment, coercion by proxy, etc. are less visible but common and connected to more overt physical tactics.

Recommendations:

- For Democracies/Host countries: States such as the US can implement targeted sanctions with more funding for enforcement, strengthen refugee resettlement programs, enhance export controls, combat interpol abuse, additional training for law enforcement, monitoring of dual-use tech used for surveillance.
- For civil society: Increase digital hygiene training, engagement with law enforcement, and conduct more research.

Highlights:

- Beyond physical acts (arrests, torture, violence) there is "everyday transnational repression": digital threats, family intimidation.
- "In essence, transnational repression is a means of injecting authoritarianism into another polity, imposing the origin country's restrictions on individuals who live in ostensibly more free environments" (4).
- Detentions and deportations represent two-thirds of their cataloged cases (4).
- Cites Yossi Shain's three factors influencing transnational repression: the threat perceived by states; capacity for suppression; states' cost-benefit calculations for engaging in such methods (5).
- Argues that the above three factors have increased: globalization leads to 'illiberal paradox' where states depend on open flows but are threatened by openness; regime capacity has grown with digital tools; norms against extraterritorial violence weakened by US/Israel activity
- Hostility towards migrants and delays introduced by increased security of migration processes creates further opportunities for individuals to be targeted, detained, returned. Similar, abuse of Interpol 'red notices' (6).

- Regional cooperation, including through organizations like SCO/GCC increase state capacity (7).
- 58% of catalogued cases involved accusations the individual was engaged in terrorism 78% of those catalogued appear to be people of Muslim origin (7). Growth of 'sharp power', tactics that do not rise to the level of open conflict (e.g. cyber attacks, disinformation, elite corruption) increase authoritarian power in democracies (7).
- The report notes that "while the immediate targets may be diaspora and exile populations, the host countries should understand that transnational repression also has an effect on their societies at large. Authoritarianism, rather than being a mode of governance confined to a specific sovereign jurisdiction, is a set of practices that can be expanded, copied, and exported and transnational repression is one of its means of reproduction abroad" (8).
- "The growth of transnational repression should be understood as a menace to the democratic aspirations of host countries as well as to the exiles and diasporas themselves" (8).
- The report defines four categories of transnational repression (9):
    1) Direct attacks (assassinations, violent renditions).
    2) Co-opting other countries (Interpol abuse, unlawful deportation).
    3) Mobility controls (passport cancellation, denial of consular services).
    4) Threats from a distance (within origin countries' own jurisdiction, "everyday transnational repression."
- "Detentions and unlawful deportations account for 62 percent of all cases compiled for this report" (10).
- Many renditions fall into a gray area; there may be a 'fig leaf' of legal process but these are often done so quickly as to be meaningless and comparable to a forced rendition by the country of origin (10).
- Country of origins often cite international cooperation as a means of legitimizing an otherwise illegal forced rendition (11).
- Special attention is paid to Interpol "red notices." The ability of states to abuse this system has increased with technical changes; there is inadequate vetting and the process lacks transparency (12).
- Targeting of an exile's family and friends in the country of origin is so common they did not code for it in this report (13).
- "Freedom House found that at least 17 countries engaged in physical transnational repression also use spyware abroad" (14).

Promote and Build: A Strategic Approach to Digital Authoritarianism (CSIS brief)

Erol Yayboke and Samuel Brannen

Yayboke, Erol and Samuel Brannen. "Promote and Build: A Strategic Approach to Digital Authoritarianism." *Center for Strategic International Studies*, October 15, 2020. https://freedomhouse.org/report/transnational-repression

Crux:

This post reviews how digital authoritarianism presents "overlapping and expanding challenges within autocracies and democracies." The authors note that the "ever evolving tools and techniques of digital

authoritarianism transcend boundaries and have over the past decade advanced the interests of authoritarian states while subverting human rights, democratic principles, and more." They advocate a "new strategic approach" that should be "grounded in fundamental principles and framed around promoting resilience while building affirmative alternatives, then executed across the U.S. government and multilateral system."

Highlights:

- Misinformation and disinformation are "far from the only digital tools authoritarians use to repress, disrupt, and spar with strategic competitors." While the growth of digital authoritarianism is well-documented and understood in Washington, the trend continues and is "accelerating within virtually ever nation on Earth."
- The authors warn that digital authoritarianism threatens to pull us backwards, including "potentially undoing decades of post-World War II political and multilateral progress". "From disinformation to corporate espionage, surveillance of citizens, and election interference, abuse of these technologies and the number of actors engaged in harm via online spaces increases by the day. At the same time, the Internet is being deliberately fragmented in a way that is likely to advantage authoritarian states." They are four challenges in particular:
    - (1) Expansion within authoritarian regimes
    - (2) Expansion by authoritarian regimes in their use of these tools abroad
    - (3) Digital authoritarian regimes are exporting these technologies to like-minded countries
    - (4) The same tools, techniques and strategies of digital authoritarianism are "being adopted within democratic countries...at the expense of public trust, personal privacy, and other civil liberties."
- The authors allege that democracies "lack a consistent and collective strategic approach to combat authoritarian use of digital and online space". In order to better understand next steps, CSIS convened a group of experts on two occasions in 2020. CSIS has set out a series of policy recommendations.
- The authors argue that democracies adoption of these tools "poses the most significant, long-term, and direct threat for the simple reason that although only democratic countries can stop digital authoritarianism, they are being actively consumed by it."
- The authors present the following strategic recommendations:
    - (1) "Promote resilience to digital authoritarianism by strengthening democracy and human rights at home."
    - (2) "Promote democratic and human rights principles in and around authoritarian-led states via free and secure communication over a free and secure internet."
    - (3) "Counter digital authoritarianism at home and abroad not only within tactical defenses, but with resilience rooted in affirmative alternative visions, norms, and principles."
    - (4) "Build affirmative alternatives to digital authoritarianism, especially for countries currently forced to decide between growth and stability with authoritarian strings attached or no growth and stability."

Burma

Surveillance Without Borders: The Case of Karen Refugees in Sheffield

Geff Green, Eleanor Grace Lockley

Green, Geff and Eleanor Grace Lockley. "Surveillance Without Borders: The Case of Karen Refugees in Sheffield." In *Emerging Trends in ICT Security*. Edited by Babak Akhgar and Hamid R. Arabnia (Waltham, MA: Elsevier, 2014), 519-533. https://doi.org/10.1016/B978-0-12-411474-6.00032-3.

Crux

This paper presents a case study of how a Burmese immigrant community in the UK was impacted by their use of modem communications technology. It considers how surveillance of new media can extend the reach of domestic conflicts and how fear and trauma can arise within a community even outside its country of origin.

Highlights

- The article describes a "hacking incident" regarding the community's blog site. The incident involved an "online smear campaign toward community members and activists from the Karen community" (524). The article describes how this incident impacted and affected the community in a profound way, particularly with regards to trust within the community (525).
- An investigation was conducted and revealed that the attacker was based in Thailand. The community saw this as "a dramatic manifestation of the long arm of the Burmese regime. They understood this to be part of the psychological and physical warfare that extended from the ethnic cleansing of Karen communities in Burma, now extended to a newer, 'virtual' location" (525).
- The article also explores the impact that this cyber-attack had on the community. The authors note that the attack was "most significant as it relates to their collective and individual experiences. They saw it implicitly as the Burmese government attempting to intimidate them at long distance; since the government was unable to physically oppress them, it sought to do so psychologically" (via new media) (529).
- The authors underline the importance of this incident, even though it did not involve any physical or in-person threats. As they observe, "[b]ecause totalitarianism relies on fear as much as on the physical repression that leads to fear, these types of events are important even though they don't make a physical mark" (530).

China

China's Global Threat to Human Rights

Human Rights Watch

Human Rights Watch. *China's Global Threat to Human Rights.* Human Rights Watch, 2020. https://www.hrw.org/world-report/2020/country-chapters/global.

Crux

This Human Rights Watch report describes how Chinese authorities are not only repressing dissent within China, but also abroad.

Highlights

- The report describes how China has "made technology central to its repression" and notes how "the surveillance state is exportable."
- The report notes how the Chinese government has a lot of capacity to devote to developing repressive technology (e.g. Xinjiang) that other governments may not. However,"the technology is becoming off-the-shelf and attractive to governments with weak privacy protections such as Kyrgyzstan, the Philippines, and Zimbabwe."
- The report notes how China engages in various forms of censorship of Chinese citizens living abroad, as well as Chinese companies.

Harassment & Intimidation of Individuals in Canada Working on China-Related Human Rights Concerns

Canadian Coalition on Human Rights in China & Amnesty International Canada

Canadian Coalition on Human Rights in China & Amnesty International Canada. *Harassment & Intimidation of Individuals in Canada Working on China-Related Human Rights Concerns.* Canadian Coalition on Human Rights in China & Amnesty International, 2020. https://www.amnesty.ca/sites/default/files/Canadian%20Coalition%20on%20Human%20Rights%20in%20China%20-%20Harassment%20Report%20Update%20-%20Final%20Version.pdf.

Crux

This report documents how activists living in Canada are harassed by the Chinese government, uncovering a "pattern of harassment and intimidation" as part of a "long standing trend of incidents that are consistent with a systematic campaign targeting human rights defenders in Canada who take action on human rights concerns in China, in which there is direct or indirect involvement by the Chinese government or its agents." (4). It also suggests that the "situation may well be worsening" with Chinese authorities becoming more emboldened in their efforts (4).

Highlights

- The report urges the Canadian government to address the issue, which has "resulted in insecurity and fear for human rights defenders in Canada working on Chinese human rights issues, as well as an unacceptable chilling effect on the exercise of free expression and other civil liberties and fundamental freedoms in the country" (5).
- The report notes that the response from the Canadian government "have been piecemeal and largely ineffective in compiling a comprehensive picture of what is happening and addressing the source of the intimidation and harassment faced by human rights defenders" (5).
- The report documents the type of intimidation suffered by human rights defenders and activists in Canada:
    - Cherie Wong, executive director of Alliance Canada HK, "describes having been subject to 'coordinated social medial attacks', including death threats and rape threats online, which increased notably following her participation in the October demontration in Ottawa" (30).

- Chemi Lhamo, a student leader at the University of Toronto and of Tibetan origin, “faced rampant online abuse and backlash” (33).

Egypt

Egypt: Escalating Reprisals, Arrests of Critics’ Families

Human Rights Watch

Human Rights Watch. *Egypt: Escalating Reprisals, Arrests of Critics’ Families*. Human Rights Watch, February 19, 2021. https://www.hrw.org/news/2021/02/19/egypt-escalating-reprisals-arrests-critics-families.

Crux

This report describes how Egypt is targeting the families of activists and human rights defenders living abroad, including activists using digital technologies to disseminate their criticism of the Egyptian regime.

Highlights

- 22 Egyptian, regional, and international organizations state that “Egyptian authorities’ targeting of families in Egypt of activists and human rights defenders living abroad has been escalating, demonstrating a clear pattern of intimidation and harassment.”
- The “authorities raided the homes of six members of the extended family of Mohamed Soltan, a US-based human rights advocate.” Previously, security agents arrested “five of the six targeted cousins in June 2020 and detained them without trial until shortly before Joe Biden won the US president election.” Soltan has been targeted with “Egyptian government and pro-government media defamation campaigns because of his human rights work.” His father was also forcibly disappeared in June 2020.
- Aly Hussein Mahdy, a graduate student at the University of Illinois, was subject to similar attacks. His father, uncle, and cousin were arrested because of Mahdy’s videos. Mahdy is a blogger with over 400,000 followers on Facebook.
- Security officers arrested two brothers of Mona el-Shazly, who is a UK-based political activist who “formerly published Facebook videos criticizing the government.” These are just some examples of the numerous others highlighted in the Human Rights Watch report.

Eritrea

Coercive Transnational Governance and Its Impact on the Settlement Process of Eritrean Refugees in Canada

Aaron Berhane and Vappu Tyyskä

Berhane, Aaron and Vappu Tyyskä. “Coercive Transnational Governance and Its Impact on the Settlement Process of Eritrean Refugees in Canada.” *Refuge: Canada’s Journal on Refugees/Refuge* 33, no. 2 (2017): 78-87. https://doi.org/10.7202/1043065ar.

Crux

The authors consider the "transnational practices of the Eritrean government" with a focus on understanding practices that "have a negative effect on refugees' capacities for successful integration, and undermine Canadian sovereignty" (78). The authors base their research findings on 11 interviews conducted with Eritrean refugees, an Eritrean community activist, and Canadian law enforcement. This article contributes to the limited research that exists at the intersection of immigration, resettlement, and transnational authoritarian practices.

Highlights

- With transnationalism, states engage in activities to "control its citizens wherever they are by using law, economy, and social apparatuses" (79).
- This article builds on prior research into transnationalism and introduces "the new concept of *coercive transnational governance*" (79).
    - This term encapsulates "what is practiced outside of bilateral or multinational agreements without the knowledge of any other governments" and is a "form of governance used by dictatorial regimes to maintain political control and secure financial contributions by force from their citizens who settled in the Western world as refugees" (79).
- The authors describe how the Eritrean government engages in coercive transnational governance to control "the lives of its citizens outside the country by installing undercover representatives in every community event, gathering, or association, creating a 'climate of fear'" (79).
- The interviews reflected a continued fear of the Eritrean state, despite the interviewees residing in Canada. For example, "[a]ll participants believe that any activity they engage in Canada can negatively affect the fate of their family. They do not feel free or secure to reject or criticize the demands of the Eritrean consulate in Toronto, despite the protection they are provided by the Canadian government" (80).
- The authors noted that "[o]ne major barrier that all participants experienced during their settlement process was fear instilled by the Eritrean consulate, which effectively silenced the refugees' critical voices, because the consulate interfered and spied upon their activities and punished family members of any exiled person who spoke against the Eritrean government" (85).

Iran

Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran

Marcus Michaelsen

Michaelsen, Marcus. "Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran." *Surveillance & Society* 15, no. 3/4 (2017): 465-470. https://doi.org/10.24908/ss.v15i3/4.6635.

Crux

This article uses the case study of exiled activists in Iran to show how digital surveillance expands transnational repression (465). In particular, the author considers how digital media facilitates existing forms of transnational repression (such as controlling the circulation of information, political expression and freedom of association). In short, these practices show that authoritarian power is no longer territorially bounded (469).

Highlights

- The author begins by noting that surveillance has long been a part of authoritarian rule: "The institutionalized and systematic practices of information gathering under authoritarian rule are not only a means which enables repression and regime preservation but also a distinct form of power and control."
    - The author notes that we still know little, however, about "how authoritarian states use the affordances of digital technologies to extend their influence and control into the transnational realm" (465).
- The author observes that "[i]n response to the increasing role that online media and social networks play for political activism and the circulation of news and opinion, authoritarian states have built sophisticated systems of internet control" (see Deibert, above).
    - Methods have shifted towards "offensive approaches" that are "not only directed against domestic activists but target also opponents outside the country" (466).
- This article relies on interviews with exiled Iranian human rights activists and journalists to demonstrate just "how digital communication surveillance enables the regime to project power beyond borders." It describes how "Iran's security agencies rely on low-scale technical expertise and human information gathering to monitor political activity outside the country's territorial jurisdiction and to prepare retaliatory or pre-emptive measures" (466):
    - In response to the use of digital media in the 2009 protests, the Iranian government "enhanced its capacities for internet control." The article describes a number of techniques used in Iran by authorities to chill speech, e.g., airing "forced confessions of arrested social media users to highlight the regime's skills in cyber-policing", arresting social media users (467).
    - The Iranian regime also uses its capabilities in an international context to target Iranian exiles and diaspora organizations, human rights defenders, and journalists. This attribution to the Iranian state or state-sponsored actors is "[b]ased on inferences from malware code, infrastructure and target selection, a range of cyberattacks in countries of the Middle East, Europe and North America" (467).
    - Repressive tactics include online espionage and malware spearphishing which are part of a broader arsenal of repressive tactics directed against human rights defenders and journalists outside the country. Digital approaches are often combined with more traditional measures, such as pressure on relatives in the country and slander in state media. State authorities seek to compromise the ties of exiled activists into the country and to disable their 'voice'" (467).
    - The article documents how "in a series of intrusion attempts against social media and email accounts of activists in the diaspora, Iranian agents used information gathered online to coax their targets into opening malware files." They also attempted to break two factor authentication. The article describes several incidents in detail, such as the targeting of US-based journalist Negar Mortazavi (468).

- The author observes that "[c]onsidering the risks that people in Iran encounter when collaborating with outside activists, digital surveillance represents a clear threat to the dynamics of transnational exchange fostered by the internet and social media" (468).

Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State

Marcus Michaelsen

Michaelsen, Marcus. "Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State." *Globalizations* 15, no. 2 (2018): 248-264. https://doi.org/10.1080/14747731.2016.1263078.

Crux

While information communication technologies present opportunities to dissidents in exile, new technologies (digital media and social networks) also create new avenues for digital compromise that state actors can use. This article uses Iran as a case study to demonstrate how digital media facilitates transnational repression.

Highlights

- This article considers how digital communications open up new avenues for transnational repression. The author notes that "in an environment of intense transnational communication and information exchange, authoritarian regimes can monitor and respond to the activities of political exiles rapidly and on a large scale" (248).
    - At the same time, the author notes that traditional research on repression is primarily focused on what happens within the borders of a state and that the global reach of such activities "is rarely considered" (252).
- Of particular note, "[t]he networked character of online communication creates multiple points of exposure that state actors can exploit to penetrate and compromise the ties between exiled activists and people inside the country. At the same time, authorities are able to better identify and consequently punish claims to public attention which political exiles address either at domestic or international audiences in order to challenge the position of the regime" (249).
- Through interviews with Iranian journalists and human rights activists living outside Iran, this paper provides insight "into possible strategies, mechanisms, and triggers of repression by the Iranian state" (253). The author describes various Internet control measures adopted by the Iranian government after 2009 and describes some of the tactics against members of the Iranian community living in exile. For example:
    - The use of "personal information gleaned from social media sources in order to develop customized scenarios tricking the targets into revealing their passwords. Some activists got telephone calls in which the other party showed knowledge on their hobbies and social relations prior to sending them a related email with corrupted files. Others received fake messages from their email provider notifying of a suspicious sign-in attempt to the account and urging to change the passport. Files or links enclosed to these messages were again compromised with malware" (255-256).

    - There were also phishing attempts and “attempts to penetrate email and social media accounts were combined to more open threats and even direct contact of activists from members of the Iranian security apparatus” (256).
    - The Iranian regime “also uses established offline methods to threaten and coerce exiled activists”. For example, the government uses pending lawsuits to make return to Iran difficult or impossible and to serve as a form of additional pressure (256-257).
- These attacks are interpreted by activists “as a message from Iranian security agencies, signaling that they are being monitored. Although the attacks rarely interrupt their activities, they create pressure and additional costs, as activists are forced to consider their online behavior and protect their communications” (256).
- The author sees these activities by the Iranian state as an extension of transnational repression and an expansion of the influence of state authority abroad. In particular, it “can be analyzed as attempts to expand the security apparatus beyond borders. Online attacks, judicial harassment, and direct threats convey the impression that even though exiles have left the Iranian territory, they are still under the control of state authorities. The internet provides security agencies with a tool to monitor exiled dissidents closely and to come up with immediate responses to their activities” (257).
- In summary, the author notes that: “[m]onitoring, surveillance, and the penetration of online networks represent permanent and diffuse threats looming over activists in exile, facilitated by the significance that the Internet and social media have gained for their activities and in their daily routines. These measures not only demonstrate the reach of authoritarian power beyond borders, permeating the lives of exiles, but also threaten to expose contacts in the home country who risk to face persecution and imprisonment. With these measures, therefore, state authorities seek to undermine the networks and vitality of transnational horizontal voice” (260).

Silencing Across Borders: Transnational Repression and Digital Threats Against Exiled Activists from Egypt, Syria, and Iran

Marcus Michaelsen

Marcus Michaelsen. *Silencing Across Borders: Transnational Repression and Digital Threats Against Exiled Activists from Egypt, Syria, and Iran*. Hivos, February 2020. https://www.hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf.

Crux

This report considers how states use surveillance and smear campaigns, among other tactics, to “systematically disrupt cross-border information flows and curtail the opportunities of human rights defenders and journalists in exile” (4). The author relies on case studies from Egypt, Syria, and Iran. In addition to summarizing the voices and views of those subjected to transnational repression, this report provides a helpful review of relevant literature in this area.

Highlights

- This report is focused on "the more subtle and pervasive forms of transnational repression exerted against activists living outside their homeland" such as surveillance and smear campaigns (4).
- The author notes how authoritarian regimes can use "'toolkits' of transnational repression" to exert repression to silence activists living abroad through self-censorship and self-restraint (4). These toolkits allow the regime to "shield themselves from criticism and accountability are able to foster restraint" (4).
- The report reviews how "[d]igital technologies are essential components of all forms of this transnational repression. They refuse the costs of exerting political control while enabling regimes to monitor and respond to diaspora activism with greater scope and speed. Activists' reliance on digital platforms and social media creates multiple points of exposure" (4).
- Activists subjected to such forms of transnational repression experience various symptoms, such as "constant tension and stress." Their ties to their countries of origin are also undermined, which leads to the "dynamics, impact, and outreach" of their activism being altered (4).

Syria

The Long Reach of the *Mukhabarat*: Violence and Harassment Against Syrians Abroad and Their Relatives Back Home

Amnesty International

Amnesty International. *The Long Reach of the* Mukhabarat*: Violence and Harassment Against Syrians Abroad and Their Relatives Back Home*. Amnesty International, October 3, 2011. https://www.amnesty.org/en/documents/MDE24/057/2011/en/.

Crux

This report documents the cases of over thirty Syrian activists living in various countries that have faced different forms of intimidation from their country of origin because of their political activities.

Highlights

- This Amnesty International report documents how Syrian activists living abroad have been threatened and harassed by the Syrian regime: "Many have been filmed and orally intimidated while taking part in protests outside Syrian embassies, while some have been threatened, including with death threats, or physically attacked by individuals believed to be connected to the Syrian regime" (5).
- Some of the activists have told Amnesty International that "relatives living in Syria have been visited and questioned by the security forces about their activities abroad and, in several cases, have been detained and even tortured as an apparent consequence" (5).

Repression Across Borders: Homeland Response to Anti-Regime Mobilization Among Syrians in Sweden

Emma Lundgren Jorum

Lundgren Jorum, Emma. "Repression Across Borders: Homeland Response to Anti-Regime Mobilization Among Syrians in Sweden." *Diaspora Studies* 8, no. 2 (2015): 104-119. https://doi.org/10.1080/09739572.2015.1029711.

Crux

This article disputes the argument that repression can be "avoided through diaspora mobilization" (104). It uses the case study of Syrian diaspora activists in Sweden to show that "intelligence reports and threats against both activists abroad and their families in the state of origin … may continue to hamper and discourage mobilization abroad" (104). The article authors that "[t]ransterritorial repression is a problem not only for the individuals affected but also for the states where they reside, as citizens with roots in certain authoritarian states are effectively discouraged from exercising their constitutional rights" (116).

Highlights

- This article studies the "mobilization of the Syrian diaspora in Sweden" to understand the "Syrian regime response to anti-regime mobilization by nationals abroad" (104). As a result, it "seeks to contribute to the problematization of the relationship between territory and state and studies of domestic politics as played out in the transnational space" (104).
- The article notes several instances of the Syrian regime conducting operations in Sweden against Syrian nationals. For example:
    - In 2010, "a Syrian intelligence officer was expelled on suspicions of illegal intelligence activity at Syrians in Sweden" (108).
    - In addition to this, "[s]everal of the activists interviewed for this article have recounted their own experiences of travelling to Syria prior to the uprising and being withheld at the airport or the border and confronted with files containing information on things they had said and done while in Sweden" (108).
    - Further, "[t]he Swedish Security Services have continued to report on alleged cases of illegal intelligence activity directed towards Syrians in Sweden, most cases involving threats" (110).
- Since the start of the Syrian uprising, "a number of anti-regime activists have received anonymous threats which they believe to be initiated by the Syrian Embassy in Stockholm" (110). A journalist for Assyria TV (based in Sweden) "reports getting constant threats—including death threats—on Facebook and through text messages" (110).
- The article details numerous consequences for targets in Sweden (*e.g.*, having to relocate homes), while also noting that there are also consequences for relatives still living in Syria. Such consequences have included relatives being harassed, kidnapped, mistreated, and killed (111).
- The article notes how, as the Syrian case in Sweden shows, "not only activists but also states may 'go transnational'. Extending repression across borders, authoritarian states may impede mobilization by their nationals—or descendants of their nationals—abroad. Intelligence information collected on activism of nationals abroad and threats directed at these activists or

at family members still in the state of origin may effectively discourage mobilization in host states where mobilization would otherwise be perceived as unproblematic" (113).
- The article concludes that "leaving one's state of origin does not necessarily mean leaving that state's repressive capabilities behind." The repressive state "may extend part of its so-called domestic opportunity structure beyond its borders by engaging in repressive measures" (114).

Transnational Repression, Diaspora Mobilization, and the Case of the Arab Spring

Dana M. Moss

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

Crux

In this article, the author studies the tools utilized by authoritarian states to deter the diaspora and how such transnational repression undermined the mobilization of Syrian and Libyan diaspora in the United States and Britain before the Arab Spring. The author also identifies factors that enabled Syrians and Libyans to overcome transnationalism after the Arab Spring.

Highlights

- The article shows that authoritarian states' transnational repression prevented diaspora (Syrian & Libyans in the US and Britain) from anti-regime activism before the Arab Spring and identifies how this was overcome with the 2011 revolutions.
- In particular, "activists 'came out' when (1) violence at home changed their relatives' circumstances and upset repression's relational effects; (2) the sacrifices of vanguard activists expanded their objects of obligation, leading them to embrace cost sharing; and (3) the regimes were perceived as incapable of making good on their threats" (480).
- More recent academic literature on transnationalism has begun to study "how populations abroad become transnational political actors and mobilize for social change in the home country. States facilitate political transnationalism through top-down processes, such as by incorporating their diasporas as constituents with voting rights" (481).
- However, the article notes that "relatively little attention has been paid to diasporas' relations with authoritarian home countries" and thus "researchers have neglected to understand how these groups remain subject to repression's deterrent effects *after* emigration" (481).
    - This "transnational repression" means that "these populations cannot fully 'exit' from authoritarianism, and that those with domestic opportunities for protest remain constrained in the exercise of their rights, liberties, and 'voice'" (481).
- Through an analysis of the Syrian and Libyan diaspora, the author seeks to answer two questions: (1) how authoritarian regimes deter dissent outside their borders, and (2) under what conditions this can be overcome (481).
    - The article notes that transnational repression takes various forms, *e.g.*, "[t]he regimes conducted surveillance through informant networks, threatened dissidents, forced them into exile, held their relatives hostage at home, and in some cases harmed dissidents directly. These tactics instilled fear and mistrust between co-nationals, de-politicized their speech and social life, and rendered anti-regime activism a

high-risk activity. As a result, only a minority engaged in opposition activities abroad, and no public membership-based transnational advocacy organizations existed before 2011" (493).
    - The author argues that this research sheds some more light on "transnationalism, repression, and mobilization" (493). It shows "how populations simultaneously experience democracy and authoritarianism after emigration" (494). It also demonstrates how "significant escalations in violence can fuel transnational contention" (494).
    - Further, "[w]hile the precise methods of transnational repression will vary by factors that include the regime's degree of authoritarianism, its ideological orientation towards the diaspora, and its capacities for repression, even opaque threats can produce an 'internment of the psyche' … that deters collective action in democratic contexts" (494).

The Ties That Bind: Internet Communication Technologies, Networked Authoritarianism, and 'Voice' in the Syrian Diaspora

Dana M. Moss

Moss, Dana M. "The Ties That Bind: Internet Communication Technologies, Networked Authoritarianism, and 'Voice' in the Syrian Diaspora." *Globalizations* 15, no. 2 (2018): 265-282. https://doi.org/10.1080/14747731.2016.1263079.

Crux

This article studies how internet communication technologies (ICTs) globalize the authoritarian regime's repression methods of social control over the diaspora and how this impacts the diaspora's mobilization against the home-country regime ("*digitally-enabled transnational repression*"). The author conducted the analysis based on interviews with pro-revolution Syrian activists based in the US and Britain.

Highlights

- The article finds that "the presence and tactics of pro-regime agents online during the onset of Syria's 2011 uprising (i) eroded respondents' transnational ties and (ii) deterred many from using ICTs to contest the Assad regime" (265).
- It shows "how networked authoritarianism mitigates diaspora members' voices and tactics during periods of violent unrest, which is precisely when ICT-enabled activism can aid home-country movements in significant ways" (265).
- The author observes that "[g]overnment authorities incorporate [ICTs] into their repertoires of social control to better implement surveillance, censorship, propaganda, and crackdowns; authoritarian regimes also nationalize ICTs to control their uses and content" (265). Yet, "little research has been done on how ICTs *globalize* the reach of authoritarian regimes in ways that ensnare their nationals abroad, produce an acute sense of threat among the diaspora, and impact the expression of 'voice' after emigration" (266).
- This study seeks to answer a gap in the research by reviewing two questions: "first, how do authoritarian regimes and their agents use ICTs to counter dissent in the diaspora? Second,

what effects does digitally-enabled transnational repression have on regime opponents overseas?" (265).

- ICTs do not just provide a space for public debate, but can also expose the diaspora to new and additional dangers (276):
    - Since "ICTs are designed to facilitate transnational connectivity, they have correspondingly *globalized* the reach of state security apparatuses and their informers. In this way, 'networked authoritarianism'...places critics abroad on the radar of regimes and their agents. This is not a new phenomenon, but rather an extension of what Moss (2016) calls 'transnational repression'; this refers to the direct and indirect efforts by diasporas' home-country regimes including the Syrian regime, to surveil diaspora communities, threaten activists verbally and harm them physically, prevent them from returning home, and punish their family members and colleagues in the home country for real or suspected disloyalty" (269).
- Through interviews with diaspora, the author observes that "digitally-enabled transnational repression forced many respondents to cut their ICT-facilitated communications with family members at home. This contributed to network erosion…and the sorting of social media networks into those who were 'out' on behalf of the revolution and those who were not. Fears stoked by the regime's presence online also led respondents to self-censor their grievances and withhold publicizing their affiliation with the anti-regime cause. Overall, the regime's transnational reach via ICTs subjected populations residing thousands of miles from Syria to the deterrent effects of authoritarian state repression during the uprising's escalation in 2011" (276).
- The author observes that the effects of digital transnational repression are "not uniform" across all diaspora communities and have different impacts. Further, the "dynamics of ICT-mediated repression" change depending on the "conflict cycles" in the country of origin. Thus, where there are greater threats to regime survival domestically, "regimes are more likely to make their online presence known" (277). In addition to this, digital transnational repression is not just the responsibility of authoritarian states, but involves other third party actors (277).
- Going forward, the author notes that this study "suggests that direct and indirect regime surveillance, harassment, and the deployment of hackers and electronic armies will prevail as a dominant mode of transnational repression in the future because such methods allow regime representatives to easily deny their culpability. As quickly as activists innovate work-around and offensive online tactics, therefore, states can readily deploy resources and adherents to meet these challenges … As a result, activists, domestic law enforcement agencies and institutional defenders of free speech will continue facing significant obstacles in holding regimes accountable for repressive tactics deployed online" (278).

Uzbekistan

"Illiberal Spaces:" Uzbekistan's Extraterritorial Security Practices and the Spatial Politics of Contemporary Authoritarianism

David Lewis

Lewis, David. "'Illiberal Spaces:' Uzbekistan's Extraterritorial Security Practices and the Spatial Politics of Contemporary Authoritarianism." *The Journal of Nationalism and Ethnicity* 43, no 1. (2015): 140-159. https://doi.org/10.1080/00905992.2014.980796.

Crux

The author argues that spatial theory provides a "framework for exploring extraterritorial security practices to counter political opposition among migrant and exile communities." This article relies on Uzbekistan as a case study to illustrate and apply this theory.

Highlights

- This article focuses "on the role of state repression as a means of controlling space." While repression is usually territorially-bounded in academic literature, the author argues that "this clear delimitation of the domestic and the international, and the invocation of clear boundaries for mechanisms of repression is misleading when analyzing contemporary governments. In practice, transborder social and economic flows threaten the efficacy of state spatial controls. As a result, the spatial politics of authoritarian regimes frequently spill over into transnational spaces; in doing so, they challenge singular conceptualizations of sovereignty and encourage new understandings of the idea of 'state space'" (141).
- The author describes a history of extraterritorial security practices. While such practices existed in the 20th century, the article argues that they have more recently increased "as contemporary authoritarian states become more integrated into a global system of transnational economic flows and international migration" (141).
    - Thus, states are now moving from managing territorially-bounded space to managing the "'space of flows', the ever-shifting transnational spaces formed by travel, migration, and international financial structures" (141).
    - For example, "China, Eritrea, Rwanda, Iran, Libya, Kazakhstan, and Russia have all been accused of targeting their own citizens or co-ethnics abroad using surveillance and intelligence-gathering operations, physical attacks, or politically motivated extradition requests" (142).
- But, as the author notes, the issue of emigration has been overlooked by scholarship. For the most part, extraterritoriality research has focused on human rights and rule of law implications.
    - There are "wider theoretical and political implications of these practices in relation to our understanding of the contemporary authoritarian state. These policies force us to reconsider the spatial nature of the authoritarian state, which at once asserts hard boundaries and closed borders against external influence, while attempting to reproduce its own repressive discourses and practices in external jurisdictions" (142).
- The author explains that "[m]ass labor migration is the most obvious social phenomenon that produces new spaces that challenge the traditional territoriality of the nation-state. Migration results in a type of 'transnational space,' which is constructed through the 'interplay of the activities of international migrants and the control practices of states intent on disciplining or harnessing those activities" (143).
- While much of the literature focuses on host countries, the author argues that authoritarian regimes are "producing a 'state effect' far beyond their own frontiers, by exporting state coercion, and thus producing new understandings of state space through extraterritorial repressive actions" (143).

- Mass migration abroad produces additional challenges to the authoritarian regime, and thus "denying political opposition the space to operate freely outside the country's borders is a further logical step for any non-democratic regime" (144).
- The article focuses more narrowly on Uzbekistan as a case study. The regime views those living and working outside the country as "potential recruiting grounds for opposition movements … and has therefore sought to reproduce domestic spatial repressions in extraterritorial jurisdictions" (145).
    - Within the diaspora, the "Uzbek state also becomes an actor, using a range of mechanisms to infiltrate communities, to surveil dissidents, and to control certain modes of activity, thus adding a further constraint to the ways in which diasporic communities shape their presence in new locations" (146).
- The author details five extraterritorial security practices used by the Uzbek state: (1) the securitization of external spaces to Uzbekistan in a way that serve to "legitimize government security practices"; (2) conducting "extensive operations abroad, including surveillance, intelligence-gathering, and informal interventions; (3) use of a "range of mechanisms … to attempt to detain individuals abroad and restrict their movement"; (4) use of "a range of legal and extra-legal mechanisms to return individuals from other jurisdictions to face prosecution in Uzbekistan" and (5) "allegations that the Uzbek security forces have been involved in physical attacks and assassinations of Uzkbeks abroad" (146).
- These "activities create particular spatial effects that question notions of a fixed, bounded Uzbek state that manages repression only inside its own borders; instead they produce the sense of an extraterritorial state, reproducing its repressive mechanisms in a range of foreign jurisdictions" (146).

Uzbekistan: "We Will Find You, Anywhere": The Global Shadow of Uzbekistani Surveillance

Amnesty International

Amnesty International. *Uzbekistan: "We Will Find You, Anywhere": The Global Shadow of Uzbekistani Surveillance*. Amnesty International, March 3, 2017. https://www.amnesty.org/en/documents/eur62/5974/2017/en/.

Crux

The report highlights how the threat of surveillance by Uzbeki authorities "continues to exert its pressure on those who have fled" the country. It documents the experiences of seven Uzbeki people, both within the country and abroad, who have been impacted by unlawful government surveillance by Uzbeki authorities.

Highlights

- The report documents how surveillance by the Uzbekistan government "continues to exert its pressure on those who have fled. Because of the fear of surveillance, many refugees outside Uzbekistan are afraid to contact their families, fearing that even receiving a phone call from abroad could trigger harassment from *mahalla* (local neighborhood) committees or security services" (5).

- For example, one Uzbekistan refugee living in Sweden, explains how he fears that if he contacts friends and family in Uzbekistan they will be approached by authorities. The refugee describes an extensive system of surveillance, including mobile phones and landlines (15). Other interviewees describe a similar experience.
- Another interviewee, a journalist living in exile, describes having her email account hacked while she was living in Germany, which led to the exposure of her email communications (18).

Government Inquiries & Prosecutions

Australia

Inquiry Into the Issues Facing Diaspora Communities in Australia

Senate Standing Committee on Foreign Affairs and Trade

Senate Standing Committee on Foreign Affairs and Trade. *Inquiry Into the Issues Facing Diaspora Communities in Australia*. Government of Australia, 2020. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade/Diasporacommunities/Submissions.

Crux

A number of Australian individuals and organizations have provided submissions on a range of issues affecting the diaspora. This summary is not exhaustive, but focuses on issues related to foreign interference with the diaspora and digital transnational repression.

Highlights

- The Australian Security Intelligence Organization (ASIO) submitted that diaspora groups are "often the victims of foreign interference" and that some "foreign governments seek to interfere in diaspora communities to control or quash opposition or dissent deemed to be a threat to their government. Such interference has included threats of harm to individuals and/or their families, both in Australia and abroad." The ASIO claims to work actively to protect these communities from such interference.
- The President of the Uyghur Community, Alim Osman, submitted that there is "intimidation and harassment in Australia by local authorities in China. This typically takes the form of WeChat calls from family members back in China (often in the presence of local law enforcement personnel) warning Uyghurs in Australia not to say anything unfavorable to the Chinese government lest something happen to these family members."
- The Australian Uyghur Tangritagh Women's Association (AUTWA) also highlighted the repression of the Uyghur community in Australia. AUTWA noted that the Chinese Communist Party has been "increasing its oppression and control of Uyghurs at an alarming rate" and this has negatively impacted Uyghurs living in the diaspora. "Uyghurs and Turkic people living [sic] the diaspora have lost all forms of communication, and have also been harassed by phone calls and intimidation over social media."
- Responsible Technology Australia (RTA) provided a submission on the use of digital platforms to engage in "manipulation, abuse and/or the proliferation" of "false information for either

political or economic purposes." The submission focuses specifically on "the proliferation of hate speech and misinformation, opening risks for foreign interference, and the potential for radicalisation and violence." RTA observed that the "manipulation of diaspora communities" could most clearly be seen in relation to China's attempt to "stoke division within Chinese-Australian communities." RTA noted that the Chinese government and other Chinese-sympathetic organizations use digital platforms to "drive wedges between diaspora communities and the wider public in Australia."

- The Falun Dafa Association of Australia submitted that one of the Chinese Communist Party's tactics for repressing the Falun Gong/Falun Dafa community in Australia was engaging in "fraudulent email campaigns." This involved the "sending of malicious emails, purporting to be from local Falun Gong practitioners."
- The report noted that this methodology had been used since 2010 in relation to all three levels of government bodies in Australia:
    - "The senders of these emails often claim to be local Falun Gong practitioners and make bizarre and sometimes insulting claims against elected representatives. In other cases, the emails portray practitioners as threatening, intolerant and otherwise undeserving of sympathy or respect. These, and similar fraudulent emails sent to officials, NGOs, journalists and human rights groups around the world have been traced back to IP addresses in China."
    - The organization—which included examples of such emails in its submission—noted that the email campaigns had succeeded in arousing and spreading distrust.

Canada

Evidence Presented to the Canadian Special Committee on Canada-China Relations

Special Committee on Canada-China Relations

Special Committee on Canada-China Relations. *Evidence.* Special Committee on Canada-China Relations, January to August 2020. https://www.ourcommons.ca/DocumentViewer/en/43-1/CACN/meeting-10/evidence#Int-10923409.

Crux

A number of witnesses spoke to the Senate Committee regarding repression by Chinese and Hong Kong authorities. The following summaries focus on extraterritorial repression, and particularly where there is a digital aspect to that repression. Because of the focus on *digital* transnational repression, it is not a complete summary of all relevant testimony regarding transnational repression, which is evidently widespread and deeply impactful on the diaspora.

Highlights

- Cherie Wong, Executive Director of Alliance Canada Hong Kong, provided evidence to the Senate committee on August 11, 2020 (1110 ff):

    - Wong testified that, since the start of the Hong Kong democratic movement, she has "received death and rape threats." In the days leading up to a protest she co-led on Parliament Hill which took place on 1 October 2019, they "started receiving online threats." At protests, they were "verbally and physically assaulted, threatened and harassed." During the protest, their pictures were taken and "many of us had our private information maliciously published" (1110).
- Annie Boyajian, Director of Advocacy at Freedom House, provided evidence to the Senate committee on August 13, 2020 (1235 ff):
    - Boyajian observed that repression in Hong Kong directly affects the lives of individuals living in Canada. She noted, for example, that "advocates across Canada are increasingly facing threats, intimidation and harassment for their work on human rights in China" with many incidents happening in schools and universities in Canada and the U.S. (1235).
    - She noted that the security law applies not only to those in Hong Kong, but also applies to "actions undertaken outside the region by people who are not even permanent residents of the region. This means that anyone in Canada speaking out again [sic] repression in Hong Kong could face arrest" (1240).
    - She referred to a few specific cases of individuals living outside Hong Kong who are at risk of arrest for activities performed outside the region. She also noted that "[r]epression in Hong Kong also impacts the information available to CAnadians, the products and services they purchase and the news and entertainment they consume." She noted that many voices have been silenced by the ongoing repression in Hong Kong, with scholars "scared into silence." Further "[p]olitical groups and advocacy coalitions have disbanded, removing reports and materials from the web, deleting social media accounts and changing phone numbers and email addresses" (1240).
- Samuel M. Chu, Founding and Managing Director of the Hong Kong Democracy Council, provided evidence to the Senate committee on August 13, 2020 (1245 ff):
    - An arrest warrant was issued for Chu by the Hong Kong authorities in July. This was despite the fact that Chu is an overseas activist (1245). Chu noted that you do not have to be physically present in Hong Kong to face legal repercussions: "Simply tweeting or re-tweeting someone else's tweet could earn you an arrest warrant and a prison sentence" (1245).
- Cheuk Kwan appeared in front of the Senate Committee on behalf of the Toronto Association for Democracy in China on August 13, 2020 (1130 ff):
    - Kwan laid out how Chinese activities had infiltrated and impacted civil society in Canada. He then set out a series of recommendations for Canadian government in responding to this transnational repression. Among other recommendations, he submitted that the Canadian government has to be "vigilant against cyber-attacks and theft of intellectual property from [Canadian] corporations and research institutions." He also suggested a "national hotline" for coordinating and reporting on harassment by China in Canada (1130).

National Security and Intelligence Committee of Parliamentarians: Annual Report 2020

National Security and Intelligence Committee of Parliamentarians

National Security and Intelligence Committee of Parliamentarians. *National Security and Intelligence Committee of Parliamentarians: Annual Report 2020*. NSICP. April 12, 2021. https://nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/annual_report_2020_public_en.pdf.

Crux

In this annual report, the National Security and Intelligence Committee of Parliamentarians address national security threats against Canada. It considers the cyber surveillance of dissidents in Canada as a national security threat.

Highlights

- The most significant threats to Canada's national security include terrorism, espionage and foriegn interference, malicious cyber activities, major organized crime, and weapons of mass destruction.
- Cyber threats have been characterized by the committee as a significant risk to national security. Such threats affect government systems, critical infrastructure providers, the private sector, and Canadians.
- Cyber threat actors range from low-sophistication cyber criminals to highly capable state-sponsored actors.
- State-sponsored cyber surveillance targeting dissidents and individuals in Canada has also been considered by the Committee as a national security concern.
- The murder of Saudi dissident Jamal Khashoggi in 2018 is an example of states using digital threats to target activists and dissidents in exile.

United States

Tools of Transnational Repression: How Autocrats Punish Dissent Overseas

Commission on Security and Cooperation in Europe, 116 Congress (1st Session)

Commission on Security and Cooperation in Europe. *Tools of Transnational Repression: How Autocrats Punish Dissent Overseas*. 116 Congress (1st Session), 2019. https://www.govinfo.gov/content/pkg/CHRG-116hhrg37829/html/CHRG-116hhrg37829.htm.

Crux

An expert panel was convened to study how states project repressive force beyond their borders. While the discussion was heavily centered on the abuse of INTERPOL, a number of experts made relevant observations regarding how transnational repression has been facilitated through the use of digital tools.

Highlights

- The Co-Chairman of the CSCE, Hon. Roger F. Wicker, made the following opening observations:
    - The United States assembled an expert panel to study how "states project repressive force beyond their borders to silence dissenters, human rights defenders, journalists, and other perceived enemies overseas."

    - He noted that autocratic states have a range of tools at their disposal: "Some schemes rely on 21st century technologies to hack, surveil, and intimidate targets, while others use blunter tactics, such as extortion, abduction, and assassination." He observed that this practice of "transnational repression" is a "wholesale assault on the rule of law internationally" and "requires the attention of all democratic nations."
    - He noted that the Helsinki Commission is taking action to "address these assaults on the rule of law." Along with Chairman Alcee Hastings, they are preparing to introduce bipartisan legislation in the House and Senate to tackle INTERPOL abuse by autocrats.
- Alexander Cooley, professor at Columbia University and author of "Dictators Without Borders: Power and Money in Central Asia," appeared before the panel:
    - He noted that the "rise of new digital and information technologies, including social media, offers new tools to authoritarians to extend their control of the information space. Without leaving their own territorial borders, dictators can now target the communications and social media profiles of exiles abroad, disrupt online platforms, and damage anti-government websites, and intimidate outspoken regime critics within electronic messages and the collection of their personal information."
    - In his prepared statement, he also provided more remarks regarding characteristics and features of present-day transnational repression. He noted a number of recent features: the global backlash against democratization; globalization and the creation of new diaspora communities, which are facilitated by cheap international transportation and communication solutions; and the rise of new digital and information technologies. On the latter point, he noted that this technology offers "new tools to the security services of authoritarians to monitor, survey and infiltrate beyond borders." While information technology was initially seen as facilitating free speech, he noted that "authoritarians have responded by extending their control of the information space beyond their territorial borders and into transnational spaces used for anti-regime activities."
- Nate Schenkkan, Director for Special Research at Freedom House, made the following comments before the panel. He made a number of recommendations regarding how the US should address transnational repression:
    - He observed that research by Yossi Shain in "The Frontier of Loyalty" sets out a three-part test for why states engage in persecution of exiles: the perception of the threat posed by exiles, the available options and kills for suppression through coercion, and a cost-benefit calculation for using coercion. In response to transnational repression, we can "blunt the tools of transnational repression."
    - More specifically, "[a]nother tool of transnational repression to be blunted is commercially available spyware." He noted the commentary by Special Rapporteur David Kaye calling for tighter regulation and new guidance from the US Department of State regarding exports of commercial surveillance technology. However, he recommended that "this guidance must be translated into mandatory regulations governing these exports, including those that carry penalties for violations. We cannot rely on industry to self-regulate in this area."
    - He also recommended supporting the targeted diaspora, such as through the Uighur Human Rights Policy Act. He also recommended that Congress "pursue legislation to support all vulnerable diaspora communities in the United States, including by providing additional resources to strengthen the ability of the FBI and appropriate US law enforcement to counter transnational repression campaigns. It should make

resources available to educate local law enforcement and immigration authorities in parts of the country where there are high concentrations of vulnerable diaspora."
    - He also suggested that the US "raise the cost of engaging in transnational repression. On the diplomatic front, we should make a consistent practice of issuing private, and where necessary public, protests to diplomats and consular officials who abuse their positions to intimidate, threaten, or undermine the rights and freedoms of exiles and members of diasporas in the United States." Further, people should be sanctioned under the Global Magnitsky Act or under other authorities.

Department of Justice: China-Based Executive at U.S. Telecommunications Company Charged with Disrupting Video Meetings Commemorating Tiananmen Square Massacre

Department of Justice

Department of Justice. *China-Based Executives at U.S. Telecommunications Company Charged With Disrupting Video Meetings Commemorating Tiananmen Square Massacre.* 2020. https://www.justice.gov/opa/pr/china-based-executive-us-telecommunications-company-charged-disrupting-video-meetings.

Crux

- A complaint and arrest warrant were unsealed charging Xinjiang Jin (aka Julien Jin) with conspiracy to commit interstate harassment and unlawful conspiracy to transfer a means of identification.
- He works for a US-based telecommunications company and was based in the People's Republic of China. He allegedly participated in a scheme to disrupt meetings in May and June 2020, that were held to commemorate the Tiananmen Square massacre.
- The commemoration meetings were conducted by videoconferencing and organized and hosted by U.S.-based individuals.

Congressional-Executive Commission on China: Annual Report 2020

Congressional-Executive Commission on China, 116th Congress

Congressional-Executive Commission on China. *Annual Report 2020*. 116th Congress (2nd Session), 2020. https://www.cecc.gov/sites/chinacommission.house.gov/files/documents/2020%20ANNUAL%20REPORT%20FINAL%201223.pdf.

Crux

Chapter seven on "Human Rights Violations in the U.S. and Globally" discusses both the harassment and intimidation of Uyghurs in the US as well as the surveillance and harassment of students from China and Hong Kong in the US (pp. 154-156).

Highlights

- Uyghur individuals in the US have reported threats and intimidation through phone and social media, and both direct and implied threats to family members still inside China.
    - The intimidation and harassment of Uyghurs in the US was conducted either anonymously or by identified members of the Chinese government.
    - This has had a chilling effect on Uyghurs in the US who wish to speak about repression in Xinjiang and violates their right to freedom of expression and association.
    - The Chinese government often harasses Uyghurs in the US by forcing close family members to convey sensitive personal and financial information.
        - Example: In 2018, Chinese authorities detained the mother of a Uyghur-American, Ferkat Jawdat, in a Xinjiang mass internment camp, prompting Jawdat to speak out about her plight. He next heard from her over a year later, in a May 2019 phone call, when she said she had been released from the camp, and asked him to cease his advocacy. Her pleas continued in the months afterward, during which a Chinese official contacted Jawdat and tried to convince him to return to Xinjiang, telling him that his actions made little difference since ‘‘China is a powerful country.”
    - A June 2017 classified directive from Xinjiang’s Political and Legal Affairs Commission obtained by the International Consortium of Investigative Journalists provides information gathered by Chinese embassies and consulates on thousands of individuals from Xinjiang who have obtained foreign citizenship or reside abroad.
- The Chinese government surveils and intimidates students from mainland China and Hong Kong studying at universities in the US via government-supervised student organizations, social media surveillance and harassment, and state-controlled media intimidation of students who publicly express political views objectionable to the Communist Party.
    - The atmosphere of suspicion has had a documented chilling effect on the freedom of expression of students from these localities studying in the US.
        - Example: In July 2019, Wuhan police detained Chinese national Luo Daiqing while he was visiting during a break from his studies at the University of Minnesota. Court documents state that Luo had used his Twitter account to post ‘‘more than 40 comments denigrating a national leader’s image and indecent pictures,’’ an apparent reference to images posted by Luo that appear to mock Chinese President Xi Jinping. A court in China sentenced him to six months’ imprisonment on the charge of ‘‘picking quarrels and provoking trouble.’’
        - Example II: Individuals claiming to be Yale University students targeted Hong Kong pro-democracy activist Nathan Law for online harassment, including death threats, after he arrived at Yale in the fall of 2019 to pursue a graduate degree. Official media such as the Global Times amplified the harassment campaign with articles in Chinese and in English, reporting disparagingly on Law’s decision to attend Yale.

Bibliography

Adamson, Fiona B. “Non-State Authoritarianism and Diaspora Politics.” *Global Networks* 20, no. 1 (2020): 150-169. https://doi.org/10.1111/glob.12246.

Adamson, Fiona B. and Gerasimos Tsourapas. *At Home and Abroad: Coercion-by-Proxy as a Tool of Transnational Repression*. Freedom House, 2020. https://freedomhouse.org/report/special-report/2020/home-and-abroad-coercion-proxy-tool-transnational-repression.

Al Jazeera. “Zoom Says it Acted on Tiananmen Accounts after China Demand.” *Al Jazeera*, June 11, 2020. https://www.aljazeera.com/news/2020/06/zoom-acted-tiananmen-accounts-china-demand-200612024129555.html.

Al Jazeera. “China: Spies, Lies and Blackmail: How China Controls Its Citizens Inside and Outside the Country Where No Criticism or Dissent is Allowed.” *Al Jazeera*, April 5, 2018. https://www.aljazeera.com/programmes/101east/2018/04/china-spies-lies-blackmail-180404145244034.html?xif=.

Alexander, Geoffrey, Matt Brooks, Masashi Crete-Nishihata, Etienne Maynier, John Scott-Railton, and Ron Deibert. *Familiar Feeling: A Malware Campaign Targeting the Tibetan Diaspora Resurfaces.* Citizen Lab, University of Toronto, August 8, 2018. https://citizenlab.ca/2018/08/familiar-feeling-a-malware-campaign-targeting-the-tibetan-diaspora-resurfaces/.

Amnesty International. *Amnesty International Among Targets of NSO-powered Campaign.* Amnesty International, August 1, 2018. https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.

Amnesty International. *Uzbekistan: “We Will Find You, Anywhere”: The Global Shadow of Uzbekistani Surveillance*. Amnesty International, March 3, 2017. https://www.amnesty.org/en/documents/eur62/5974/2017/en/.

Amnesty International. *The Long Reach of the* Mukhabarat*: Violence and Harassment Against Syrians Abroad and Their Relatives Back Home*. Amnesty International, October 3, 2011. https://www.amnesty.org/en/documents/MDE24/057/2011/en/.

Arab News. *Iranian Regime Using Dutch Server to Spy on Dissidents: Investigation*. Arab News, February 19, 2021. https://www.arabnews.com/node/1811671/middle-east.

Azerbaijan Internet Watch. “Activist’s YouTube Channel Down.” *Azerbaijan Internet Watch*, December 5, 2019. https://www.az-netwatch.org/news/activists-youtube-channel-down/.

Berhane, Aaron and Vappu Tyyskä. “Coercive Transnational Governance and Its Impact on the Settlement Process of Eritrean Refugees in Canada.” *Refuge: Canada’s Journal on Refugees/Refuge* 33, no. 2 (2017): 78-87. https://doi.org/10.7202/1043065ar.

BR24. “Lined Up in the Sights of Vietnamese Hackers.” *BR24*, October 7, 2020. https://web.br.de/interaktiv/ocean-lotus/en/.

Brooks, Matt, Jakub Dalek, and Masashi Crete-Nishihata. *Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns.* Citizen Lab, University of Toronto, April 18, 2016. https://citizenlab.ca/2016/04/between-hong-kong-and-burma/

Burton, Charles. “China Threatens and Intimidates People Within Canada as Ottawa Remains Silent.” *The Toronto Star*, September 8, 2020. https://www.thestar.com/opinion/contributors/2020/09/08/china-threatens-and-intimidates-people-within-canada-as-ottawa-remains-silent.html.

Canadian Coalition on Human Rights in China & Amnesty International Canada. *Harassment & Intimidation of Individuals in Canada Working on China-Related Human Rights Concerns.* Canadian Coalition on Human Rights in China & Amnesty International, 2020. https://www.amnesty.ca/sites/default/files/Canadian%20Coalition%20on%20Human%20Rights%20in%20China%20-%20Harassment%20Report%20Update%20-%20Final%20Version.pdf.

Certfa Lab. *Fake Interview: The New Activity of Charming Kitten.* Certfa Lab, January 30, 2020. https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/.

Chase, Steven. “Victims Recount Foreign State-Sponsored Harassment.” *The Globe and Mail*, November 27, 2020.

Chaudhary, Ali R. and Dana M. Moss. “Suppressing Transnationalism: Bringing Constraints Into the Study of Transnational Political Action.” *Comparative Migration Studies* 7, no. 9 (2019). https://doi.org/10.1186/s40878-019-0112-z.

Check Point. *Of Kittens and Princes: Latest Updates on Two Iranian Espionage Operations*. Check Point, February 2021. https://blog.checkpoint.com/2021/02/08/of-kittens-and-princes-the-latest-updates-on-two-iranian-espionage-operations/.

Commission on Security and Cooperation in Europe. *Tools of Transnational Repression: How Autocrats Punish Dissent Overseas*. 116 Congress (1st Session), 2020. https://www.govinfo.gov/content/pkg/CHRG-116hhrg37829/html/CHRG-116hhrg37829.htm.

Committee to Protect Journalists. “Palestinian journalist Muath Hamed Questioned in Spain by Alleged Israeli Intelligence Agent.” *Committee to Protect Journalists,* April 15, 2021. https://cpj.org/2021/04/palestinian-journalist-muath-hamed-questioned-in-spain-by-alleged-israeli-intelligence-agent/.

Congressional-Executive Commission on China. *Annual Report 2020*. 116th Congress (2nd Session),

2020. https://www.cecc.gov/sites/chinacommission.house.gov/files/documents/2020%20ANNUAL%20REPORT%20FINAL%201223.pdf.

Crete-Nishihata, Masashi, Jakub Dalek, Etienne Maynier, and John Scott-Railton. *Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community*. Citizen Lab, University of Toronto, January 30, 2018. https://citizenlab.ca/2018/01/spying-on-a-budget-inside-a-phishing-operation-with-targets-in-the-tibetan-community/

Dalek, Jakub, Masashi Crete-Nishihata, and John Scott-Railton. *Shifting Tactics: Tracking Changes in Years-Long Espionage Campaign Against Tibetans.* Citizen Lab, University of Toronto, March 10, 2016. https://citizenlab.ca/2016/03/shifting-tactics/

Dalmasso, Emanuela, Adele Del Sordi, Marlies Glasius, Nicole Hirt, Marcus Michaelsen, Abdulkader S. Mohammad, and Dana Moss. "Intervention: Extraterritorial Authoritarian Power." *Political Geography* (2017): 1-10. https://doi.org/10.1016/j.polgeo.2017.07.003.

Dearden, Lizzie. "Human Rights Activist Launches Legal Claim Against Saudi Arabia For 'Hacking Phone' in UK." *The Independent UK*, May 29, 2019. https://www.independent.co.uk/news/uk/home-news/saudi-arabia-spying-phones-ghanem-dosari-uk-spyware-pegasus-a8935331.html.

Deibert, Ronald. "Authoritarianism Goes Global: Cyberspace Under Siege." *Journal of Democracy* 26, no. 3 (2015): 64-78. https://doi.org/10.1353/jod.2015.0051.

Department of Justice. *China-Based Executives at U.S. Telecommunications Company Charged With Disrupting Video Meetings Commemorating Tiananmen Square Massacre.* 2020. https://www.justice.gov/opa/pr/china-based-executive-us-telecommunications-company-charged-disrupting-video-meetings.

Dvilyanski, Mike and Nathaniel Gleicher. *Taking Action Against Hackers in China*. Facebook, March 24, 2021. https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/.

Dvilyanski, Mike and David Agranovich. *Taking Action Against Hackers in Palestine*. Facebook, April 21, 2021. https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/.

Mike Dvilyanski and David Agranovich. *Taking Action Against Hackers in Palestine*. Facebook, April 21, 2021. https://about.fb.com/news/2021/04/taking-action-against-hackers-in-palestine/.

Galperin, Eva, Cooper Quintin, Morgan Marquis-Boire, and Claudio Guarnieri. *I Got a Letter From the Government the Other Day: Unveiling Campaign of Intimidation, Kidnapping and Malware in Kazakhstan.* The Electronic Frontier Foundation (EFF), August 2016. https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf.

Gilbert, David. "Chinese Police Are Making Threatening Video Calls to Dissidents Abroad." *Vice News*, July 14, 2020.

https://www.vice.com/en_us/article/jgxdv7/chinese-police-are-video-calling-citizens-abroad-with-threats-not-to-criticize-beijing.

Glasius, Marlies. "Extraterritorial Authoritarian Practices: A Framework." *Globalizations* 15, no. 2 (2018): 179-197. https://doi.org/10.1080/14747731.2017.1403781.

Green, Geff and Eleanor Grace Lockley. "Surveillance Without Borders: The Case of Karen Refugees in Sheffield." In *Emerging Trends in ICT Security*. Edited by Babak Akhgar and Hamid R. Arabnia (Waltham, MA: Elsevier, 2014), 519-533. https://doi.org/10.1016/B978-0-12-411474-6.00032-3.

Gulf Center For Human Rights. "Bahrain: Human rights defenders in exile threatened, along with their families, while ongoing court cases continue against other defenders." *Gulf Center For Human Rights*, March 11, 2017. https://www.gc4hr.org/news/view/1511.

Hamilton, Clive. "Beijing's Assault on Privacy Goes Global." *The Globe and Mail*, September 8, 2020. https://www.theglobeandmail.com/opinion/article-beijings-assault-on-privacy-goes-worldwide/.

Human Rights Watch. *China's Global Threat to Human Rights.* Human Rights Watch, 2020. https://www.hrw.org/world-report/2020/country-chapters/global.

Human Rights Watch. *Egypt: Escalating Reprisals, Arrests of Critics' Families*. Human Rights Watch, February 19, 2021. https://www.hrw.org/news/2021/02/19/egypt-escalating-reprisals-arrests-critics-families.

Kajjo, Sirwan. *Secondary Targets: When You Can't Punish a Journalist, Family Will Do Just Fine*. VOA News, undated. https://projects.voanews.com/press-freedom/secondary-targets/.

Kleemola, Katie, Masashi Crete-Nishihata, Adam Senft, and Irene Poetranto. *Targeted Malware Attacks against NGO Linked to Attacks on Burmese Government Websites.* Citizen Lab, University of Toronto, October 16, 2015. https://citizenlab.ca/2015/10/targeted-attacks-ngo-burma/.

Kleemola, Katie, Masashi Crete-Nishihata, and John Scott-Railton. *Targeted Attacks against Tibetan and Hong Kong Groups Exploiting CVE-2014-4114.* Citizen Lab, University of Toronto, June 15, 2015. https://citizenlab.ca/2015/06/targeted-attacks-against-tibetan-and-hong-kong-groups-exploiting-cve-2014-4114/

Kleemola, Katie, Masashi Crete-Nishihata, and John Scott-Railton. *Tibetan Uprising Day Malware Attacks.* Citizen Lab, University of Toronto. March 10, 2015. https://citizenlab.ca/2015/03/tibetan-uprising-day-malware-attacks/.

Knight, Ben. "UK Malware Used Against Bahraini Activists." *DW*, May 9, 2012. https://www.dw.com/en/uk-malware-used-against-bahraini-activists/a-16219440.

Knockel, Jeffrey, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert. *We Chat, They Watch: How International Users Unwittingly Build Up WeChat's Chinese*

Censorship Apparatus. Citizen Lab, University of Toronto, May 7, 2020. https://citizenlab.ca/2020/05/we-chat-they-watch/.

Lake, Eli. "The Dark Side of Israel's Cold Peace With Saudi Arabia: The Saudis Are Using Israeli-made Cyberweapons to Monitor and Intimidate Dissidents Abroad." *Bloomberg*, June 3, 2019. https://www.bloomberg.com/opinion/articles/2019-06-03/israel-s-cold-peace-with-saudi-arabia-has-a-dark-side.

Lewis, David. "'Illiberal Spaces:' Uzbekistan's Extraterritorial Security Practices and the Spatial Politics of Contemporary Authoritarianism." *The Journal of Nationalism and Ethnicity* 43, no 1. (2015): 140-159. https://doi.org/10.1080/00905992.2014.980796.

Linzer, Isabel. *Digital Technology Helps Governments Target Critics Across Borders*. Slate, February 24, 2021. https://slate.com/technology/2021/02/paul-rusesabagina-rwanda-trial-digital-technology-critics-abroad.html.

Lundgren Jorum, Emma. "Repression Across Borders: Homeland Response to Anti-Regime Mobilization Among Syrians in Sweden." *Diaspora Studies* 8, no. 2 (2015): 104-119. https://doi.org/10.1080/09739572.2015.1029711.

Marczak, Bill, Adam Hulcoop, Etienne Maynier, Bahr Abdul Razzak, Masashi Crete-Nishihata, John Scott-Railton, and Ron Deibert. *Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits*. Citizen Lab, University of Toronto, September 24, 2019. https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/.

Marczak, Bill, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert. *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*. Citizen Lab, University of Toronto, October 1, 2018. https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/.

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. Citizen Lab, University of Toronto, September 18, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Marczak, Bill, John Scott-Railton, and Ron Deibert. *NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident.* Citizen Lab, University of Toronto, July 31, 2018. https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/.

Marczak, Bill, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert. *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware*. Citizen Lab, University of Toronto, December 6, 2017.

https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/.

Marczak, Bill and John Scott-Railton. *The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender.* Citizen Lab, University of Toronto, August 24, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Marczak, Bill, John Scott-Railton, and Sarah McKune. *Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware*. Citizen Lab, University of Toronto, March 9, 2015. https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton. *Hacking Team and the Targeting of Ethiopian Journalists*. Citizen Lab, February 12, 2014. https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/.

Marcus Michaelsen. *Silencing Across Borders: Transnational Repression and Digital Threats Against Exiled Activists from Egypt, Syria, and Iran*. Hivos, February 2020. https://www.hivos.org/assets/2020/02/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf.

Michaelsen, Marcus. *The Digital Transnational Repression Toolkit, and Its Silencing Effects*. Freedom House, 2020. https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects.

Marczak, Bill, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert. *The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit*. Citizen Lab, University of Toronto, December 20, 2020. https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/.

Michaelsen, Marcus. "Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State." *Globalizations* 15, no. 2 (2018): 248-264. https://doi.org/10.1080/14747731.2016.1263078.

Michaelsen, Marcus. "Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran." *Surveillance & Society* 15, no. 3/4 (2017): 465-470. https://doi.org/10.24908/ss.v15i3/4.6635.

Mohyeldin, Ayman M. "No One Is Safe: How Saudi Arabia Makes Dissidents Disappear." *Vanity Fair*, July 29, 2019. https://www.vanityfair.com/news/2019/07/how-saudi-arabia-makes-dissidents-disappear.

Moss, Dana M. *The Importance of Defending Diaspora Activism for Democracy and Human Rights*. Freedom House, 2020. https://freedomhouse.org/report/special-report/2020/importance-defending-diaspora-activism-democracy-and-human-rights.

Moss, Dana M. “The Ties That Bind: Internet Communication Technologies, Networked Authoritarianism, and ‘Voice’ in the Syrian Diaspora.” *Globalizations* 15, no. 2 (2018): 265-282. https://doi.org/10.1080/14747731.2016.1263079.

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

Mozur, Paul and Nicole Perlroth. “China’s Software Stalked Uighurs Earlier and More Widely, Researchers Learn.” *The New York Times*, July 1, 2020. https://www.nytimes.com/2020/07/01/technology/china-uighurs-hackers-malware-hackers-smartphones.html.

Mustafa, Naheed. “Life in the digital life of the Syrian War.” *Open Canada*, October 18, 2016. https://www.opencanada.org/features/life-digital-shadow-syrian-war/.

National Security and Intelligence Committee of Parliamentarians. *National Security and Intelligence Committee of Parliamentarians: Annual Report 2020*. NSICP, April 12, 2021. https://nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/annual_report_2020_public_en.pdf.

Öztürk, Ahmet Erdi and Hakkı Taş. “The Repertoire of Extraterritorial Repression: Diasporas and Home States.” *Migration Letters* 17, no. 1 (2020): 59-69. https://doi.org/10.33182/ml.v17i1.853.

Regalado, Daniel, Nart Villeneuve, and John Scott-Railton. *Behind the Syrian Conflict’s Digital Frontlines.* Fire Eye, February, 2015. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf.

Satter, Raphael and Christopher Bing. “Exclusive: Iran-Linked Hackers Pose as Journalists in Email Scam.” *Reuters*, February 5, 2020. https://www.reuters.com/article/us-iran-hackers-exclusive-idUSKBN1ZZ1MS.

Schenkkan, Nate and Isabel Linzer. *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression*. Freedom House, February 2021. https://freedomhouse.org/report/transnational-repression.

Scott-Railton, John, Bahr Abdul Razzak, Adam Hulcoop, Matt Brooks, and Katie Kleemola. *Group5: Syria and the Iranian Connection.* Citizen Lab, University of Toronto, August 2, 2016. https://citizenlab.ca/2016/08/group5-syria/.

Scott-Railton, John and Katie Kleemola. *London Calling: Two-Factor Authentication Phishing From Iran.* Citizen Lab, University of Toronto, August 27, 2015. https://citizenlab.ca/2015/08/iran_two_factor_phishing/.

Senate Standing Committee on Foreign Affairs and Trade. *Inquiry Into the Issues Facing Diaspora Communities in Australia*. Government of Australia, 2020.

https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade/Diasporacommunities/Submissions.

Snowdon, Wallis. "Edmonton Software Engineer Says Iranian Regime Attempted to Make Him Their Spy." *CBC News*, August 27, 2020. https://www.cbc.ca/news/canada/edmonton/edmonton-software-engineer-arrest-iranian-regime-informant-1.5700744.

Special Committee on Canada-China Relations. *Evidence.* Special Committee on Canada-China Relations, January to August 2020. https://www.ourcommons.ca/DocumentViewer/en/43-1/CACN/meeting-10/evidence#Int-10923409.

Tidy, Joe. "'I Was a Victim of the WhatsApp Hack'." *BBC News*, October 31, 2019. https://www.bbc.com/news/technology-50249859.

Tsourapas, Gerasimos. "Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-Optation in World Politics." *International Studies Review* (2020): 1-29. https://doi.org/10.1093/isr/viaa061.

Tsourapas, Gerasimos. *A Tightening Grip Abroad: Authoritarian Regimes Target Their Emigrant and Diaspora Communities.* Migration Policy, 2019. https://www.migrationpolicy.org/article/authoritarian-regimes-target-their-emigrant-and-diaspora-communities.

Wang, Yaqiu. "Why Some Chinese Immigrants Living in Canada Live in Silent Fear." *The Globe and Mail*, February 25, 2019. https://www.theglobeandmail.com/opinion/article-why-some-chinese-immigrants-living-in-canada-live-in-silent-fear/.

Zetter, Kim. "Bahraini Activists Hacked by Their Government Go After UK Spyware Maker." *Wired*, October 13, 2014. https://www.wired.com/2014/10/bahraini-activists-go-after-spyware-source/.