Canada's Foreign Policy Objective: Combatting the Pillars of Digital Authoritarianism

Aleynor Aygor, Mehnaz Hossein, Shalin Nayak, Temi Reju

Issue Statement

Digital Authoritarianism (DA) constitutes the expansive misuse of digital tools by authoritarian regimes in ways that directly threaten the democratic fabric of Canadian society and that of our strategic allies.

Background

Some of the key avenues for DA have manifested through heightened surveillance, access to sensitive data, the intentional spread of disinformation (Cebul and Pickney 2021) and the denial of basic human rights (Dragu and Lupu 2021).

The literature suggests that the greater the development of these technologies, the greater the incentive for their misuse by governments. Further concerns about the misuse of these technologies point to their use in controlling political dissidents living outside an authoritarian regime's borders, interference in the democratic political processes of other states and the potential adoption of these techniques within democracies (Polyakova and Meserole 2019).

These concerns are not just limited to actions within authoritarian countries. Even liberal democratic nations like Canada are not immune to the draw of DA. Within the last decade, the use of DA tools like surveillance, tracking and artificial intelligence has become increasingly common among Western democracies. Many of the digital tools used by authoritarian leaders are also developed and sold by tech companies in the West. As technologies become more advanced, the lines between the legitimate and authoritarian uses of digital technologies begin to blur.

While digital authoritarianism poses a threat to human rights and foundational principles of democratic and open societies, it also raises additional concerns for Canada since digital foreign interference directed at democratic institutions and processes can threaten Canada's national security. Within the current securitization realm, we see digital authoritarianism as manifesting in three main ways: foreign electoral interference and espionage, transnational repression and disinformation. These areas of concern all involve some level of state and non-state interference within a sovereign Canada.

Foreign 'Electoral' Interference

As elections increasingly move online, the threat of interference by state and non-state actors to reach their immediate, medium, or long-term goals have increased. Foreign interference (FI) poses an emerging threat to Canada's democratic process (Carvin, 2021). Canada's CSIS Act defines foreign interference as, 'activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person' (CSIS Act, 1985). These activities can include undermining trust in Canada's democracy, institutions, social cohesiveness, national security and disrupting the rules-based international order. Canada's close ties to the United States, its status as a NATO and Five Eyes member and its socio-economic power makes it an attractive target (CSIS, 2021). Current geopolitical tensions,

especially after the Russian invasion of the Ukraine, presents an intensifying FI threat (Carbert, 2020).

Canada's Election Modernization Act (EMA), makes combatting FI one of its priorities. The creation of the Security and Intelligence Threats to Elections (SITE) Task Force brings together actors from CSE, CSIS, GAC and the RCMP to assess and respond to these FI threats. Canada is party to the G7 Rapid Response Mechanism (RRM), a G7 initiative to identify, prevent and respond to threats against G7 democracies and the Five-Country Ministerial. GAC houses the RRM's G7 RRM Coordination Unit that oversees information exchange and analysis (Government of Canada, 2019). The Five-Country Ministerial brings together the Five-Eyes, an intelligence alliance between Australia, Canada, New Zealand, the United Kingdom, and the U.S., to share transnational safety and security concerns (Public Safety Canada, 2021). Canada also took part in the 2021 Summit for Democracy hosted by the U.S. where it supported the 'Export Control and Human Rights Initiative' and was a part of the 'Surveillance Principles Initiative'.

With a looming FI threat to elections and Canada's democratic foundations, Canada must follow its Five Eyes partners and create multilateral digital governance frameworks and crack down on Chinese and Russian exports to combat possible FI such as banning Huawei from Canada's 5G network.

Disinformation

Other threats to Canada's democratic process include disinformation. Disinformation in a digital era utilizes digital tools to intentionally manipulate, degrade public deliberation, undermine norms, and weaken trust in public institutions within opposing states (Cyber Centre, 2022; Tenove et al., 2018; Yayboke & Brannen, 2020). The spread of false information poses a unique threat to democratic countries, specifically when autocratic regimes use disinformation as a political weapon to further their strategic agendas by undermining the political process in other countries (Yayboke & Brannen, 2020). Some of the commonly used disinformation techniques include claims of fake news, data scandals, and inaccurate information to restrict and manipulate the knowledge available to citizens in digital form (Tenove et al., 2018). This form of digital deception often weaponizes social media to impose certain ideologies and views on citizens around the world, resulting in digital authoritarianism (Jones, 2022).

While digital techniques are widely used by non-state actors, such as terrorist groups and extremist social movements, state actors [such as China or Russia] pose a particular risk to Canadian democracy. They have access to resources that can cause harm on a larger scale and therefore, the ability to broadcast long-lasting propaganda and disinformation campaigns in multiple languages (Tenove et al., 2018). This pillar emphasizes that disinformation campaigns can be harmful to democracy beyond electoral interference, as it also violates Canadians values rooted in the ruled-based international order, human rights, and FIAP.

The Canadian Centre for Cyber Security already offers guidance and resources related to disinformation on their website, and the country has launched a digital charter to protect the nation against disinformation that can undermine the integrity of elections and democratic institutions. During this launch, Justin Trudeau has discussed the role social media platforms play in countering disinformation and announced that such platforms will be held accountable with the digital charter. These measures suggest that Canada recognizes disinformation is a major threat to democracy and must ensure that foreign actors do not disrupt the country's democratic process through the spread of disinformation on cyber space.

[APG]

Transnational Repression

Finally, in committing transnational repression, foreign states effectively manipulate individuals and information in Canada, which threatens our democratic institutions and national sovereignty. Authoritarian states apply transnational repression techniques designed to intimidate, persecute, or coerce citizens living abroad. The proliferation of digital technology has provided these governments with new tools to suppress cross-border opposition. Common digital transnational repression tactics include hacking and phishing, account takeovers, troll and bot campaigns on social media, online threats, and disinformation campaigns.

These techniques are typically used against activists, human rights defenders or dissidents from other countries living in exile in Canada (Al-Jizawi et al., 2022). There is little to no support for individuals who are subject to transnational repression, and women are disproportionately targeted by this kind of harassment. Victims have also reported that authorities and law enforcement in Canada are not equipped to address the issues posed by transnational repression (Al-Jizawi et al., 2022).

Breach of privacy is a major risk of transnational repression, not only for those subject to state harassment, intimidation, or repression, but also other Canadians whose privacy may be infringed upon by these foreign state actors. Canada's *Privacy Act* protects individuals from the unlawful collection or use of personal information by the Canadian government, however, Canada does not have a policy framework that addresses transnational repression from foreign governments. The lack of a coordinated response to transnational repression jeopardizes Canada's status as a safe haven for vulnerable people, and Canada's cyber security may also be compromised by the same digital tools that authoritarian states use to oppress its citizens living abroad. In collaboration with Global Affairs Canada, Public Safety Canada and CSIS, Canada must actively work to reduce opportunities for states to engage in transnational repression and provide resources to support victims of transnational repression in Canada.

Models of DA

China and Russia are the most salient actors involved in developing and supplying the tools needed for governments to engage in digital authoritarianism. The Chinese model is based on strong partnerships between the state and the Chinese technology sector. Historically, this sector has supplied telecommunications hardware, advanced facial-recognition technology, and data analytics tools to a variety of governments with poor human rights records. Chinese technology companies are actively shaping the politics and policies of surveillance and monitoring technologies through forming high-level relationships with domestic governments and telecommunications firms (Cave et. al, 2019).

The Russian approach differs from the Chinese model and can be thought of as an ad-hoc strategy that leverages technical, legal, and administrative measures to monitor populations and suppress free access to the internet. Russia has also invested significant resources in information manipulation, which has been strategically deployed to destabilize and increase polarization in Western democracies. Russia's low-tech and low-cost model could be easier to replicate and more globally adaptable as emerging authoritarian regimes seek greater control over their populations (Polyakova and Meserole 2019).

The confluence of state and non-state actors involved in exporting digital authoritarianism poses a unique challenge for policymakers as mitigating this threat may require significant coordination between the public and private sectors.

[APG]

Recommendations

1. Disincentivize trade partners from exporting Chinese and Russian DA technology. Chinese DA technology is already being disseminated and used by strategic Canadian trade partners. As a two-pronged approach to combating DA, Canada must both tighten export regulations of these technologies and prevent partners from exporting undemocratic technology through including conditionalities and clauses within trade agreements and relationships.

2. Creation of a Five Eyes *Digital Authoritarianism Protocol (DAP).* To reconfirm its commitment to democracy, Canada should take initiative to host the 2022 Summit for Democracy and propose the creation of the Five Eyes DAP to create a multilateral agreement on what constitutes DA, reframe laws regarding DA and create agreements on how to combat DA and FI, thus building on the existing framework of the Five Eyes Alliance. DAP can also set a precedent for combating transnational repression by providing training for Canadian security agencies on how to respond to transnational repression. DAP can also stipulate the provision of funding and resources to support victims of transnational repression.

3. Formation of public-private partnerships to build digital infrastructure that serves as an affirmative alternative to the Chinese DA model. Utilizing the competitiveness of the Canadian private digital technology sector, technological infrastructure based on the principles of data transparency and responsible AI must be built out through public-private joint initiatives. This effort can address the technological demand for AI and surveillance technologies and serve as a viable alternative to the Chinese DA model globally.

4. Expand the scope of restrictions in Canada's *State Immunity Act* to include transnational repression. Canada's legislation provides certain exceptions to the principle of state immunity as long as it is consistent with the trends of restricting the scope of state immunity within the country. There is already an established precedent for criminalizing this type of foreign imposition as Canada has already made similar provisions in the past. In 2012, the *State Immunity Act* was amended to allow foreign actors who committed or supported acts of terrorism in Canada to be subject to punishment under sections 83.02, 83.04, 83.18 and 83.23 of the *Criminal Code*. Adding transnational repression to the scope of restrictions for state immunity would allow the both Canadian government and victims of transnational repression to pursue legal action against their perpetrators.

5. Develop a strategy to cultivate trust in democratic institutions in order to counter the spread of disinformation on cyber space. The process of rebuilding trust in public institutions and civic discourse cannot be achieved exclusively by providing resources on how to identify inaccurate, false, or unsustainable information. While offering cyber education is essential to building societal resilience to disinformation, providing credible information and finding ways to become more transparent with citizens on government communications will increase public resilience to disinformation. This approach requires collaboration between relevant departments and agencies such as Global Affairs Canada, Public Safety Canada, the Department of Justice, and stakeholder participation from other experts. The development of this strategy would serve as a fact check mechanism and help build institutional trust.

[APG]

About the Authors

Aleynor Aygor is a student in Wilfrid Laurier University's Master of International Public Policy program, based at the Balsillie School of International Affairs.

Mehnaz Hossein is a student in the University of Waterloo's Master of Arts in Global Governance program, based at the Balsillie School of International Affairs.

Shalin Nayak is a student in Wilfrid Laurier University's Master of International Public Policy program, based at the Balsillie School of International Affairs.

Temi Reju is a student in Wilfrid Laurier University's Master of International Public Policy program, based at the Balsillie School of International Affairs.

Acknowledgements

The authors would like to thank John Abraham, Naireen Khan and officials at Global Affairs Canada for all of their guidance and mentorship throughout the course of the fellowship program.

References

Al-Jizawi, N., Anstis, S., Barnett, S., Chan, S., Leonard, N., Senft, A., & Deibert., R. *Psychological and Emotional War: Digital Transnational Repression in Canada* (Research Report #151). The Citizen Lab, 2022. https://s3.amazonaws.com/tld-documents.llnassets.com/0034000/34289/citizen%20lab%20report.pdf

Bontcheva, K., Posetti, J.,Teyssou, D., Meyer, T., Gregory, S., Hanot, C., & Maynard, D. *Balancing Act: Countering Digital Disinformation while Respecting Freedom of Expression.* Broadband Commission for Sustainable Development, 2020. https://www.broadbandcommission.org/Documents/working-groups/FoE_Disinfo_Report.pdf

Canadian Centre for Cyber Security. "How to Identify Misinformation, Disinformation and Malinformation." Communications Security Establishment, 2022. https://cyber.gc.ca/sites/default/files/2022-02/ITSAP-00-300-How-To-Identify-Misinformation_e.pdf

Carvin, S. "The big lie: Is Canada's election 44 at risk from foreign interference?" Center for Innovation and Governance, 2021. https://www.cigionline.org/articles/the-big-lie-is-canadas-election-44-at-risk-from-foreign-interference/

Carbert, M. "Russia poses most immediate military threat to Canada, top general says." The Globe and Mail, 2020. https://www.theglobeandmail.com/politics/article-russia-poses-most-immediate-military-threat-to-canada-top-general/

Cave, D., Hoffman, S., Joske, A., Ryan, F., & Thomas, E. "Enabling & exporting digital authoritarianism." In *Mapping China's technology giants*: (2019) 8–15. Australian Strategic Policy Institute. http://www.jstor.org/stable/resrep23072.8

[APG]

Cebul, M., & Pinckney, J. "Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution." US Institute of Peace, 2021.

"Cyber Threats to Canada's democratic process." Communications Security Establishment, (2021). https://cyber.gc.ca/sites/default/files/2021-07/threat-to-democratic-process-2021-3-web-e.pdf

Dragu, T., & Lupu, Y. "Digital Authoritarianism and the Future of Human Rights." *International Organization* 75, no. 4 (2021): 991-1017. doi:10.1017/S0020818320000624

"Foreign interference threats to Canada's democratic process." Canadian Security Intelligence Service, 2021. https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/foreign-interference-threats-to-canada%27s-democratic-process.pdf

Government of Canada. *Canadian Security Intelligence Service Act*, 1985. https://laws-lois.justice.gc.ca/PDF/C-23.pdf

Polyakova, & Meserole, C. "Exporting digital authoritarianism: The Russian and Chinese models." In *Policy File*. The Brookings Institution, 2019.

Public Safety Canada. *Five-Country Ministerial*, 2021. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/fv-cntry-mnstrl-en.aspx

Schenkkan, N., & Linzer, I. *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression.* Freedom House, 2021. https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf

Tenove, C., Buffie, J., McKay, S., & Moscrop, D. *How Foreign Actors use Digital Techniques to Undermine Democracy.* Centre for the Study of Democratic Institutions, 2018. https://democracy2017.sites.olt.ubc.ca/files/2018/01/DigitalThreats_Report-FINAL.pdf

Yayboke, E.,& Brannen, S. *Promote and Build a Strategic Approach to Digital Authoritarianism.* Center for Strategic and International Studies, 2020. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/201015_Yayboke_Brannen_PromoteAndBuild_Brief.pdf

[APG]

[APG]