DIGITAL AUTHORITARIANISM
THREATS TO U.S. DEMOCRACY

Shannon Dales daless1@mcmaster.ca
Rebecca Denyer denyerr@mcmaster.ca
Brenna Friesen friesb4@mcmaster.ca
Ryan Hart hartr11@mcmaster.ca
Rida Mohsin mohsir1@mcmaster.ca

POLICY OBJECTIVE

To identify and address digital authoritarian threats to the American liberal democracy at the individual, state, and corporate levels of society. A series of case studies will be used to highlight inadequate policy protection and intervention strategies for safeguarding American state institutions, corporations, law enforcement, and social media platforms.

WHAT IS DIGITAL AUTHORITARIANISM?

Digital authoritarianism is the "use of digital tools to surveil, repress, and manipulate domestic and foreign populations" (Polyakova and Meserole 2020).

A 2018 Freedom House study found that since 2017, 26 out of the 65 countries examined had experienced a significant decline in digital freedoms.

state level

Digital Threats to American Democratic State Institutions

In April 2015, a Chinese state-sponsored group breached the Office of Personnel Management's network and stole 21.5 million Americans' personally identifiable information. In June 2015, a Russian-based hacking group conducted a cyberattack against the Internal Revenue Service and stole $50 million worth in fraudulently filed tax returns. These are two examples of an increasing trend where authoritarian governments are hacking US democratic institutions to degrade Americans' trust in these institutions. Public trust in political institutions is vital to maintaining their legitimacy. Therefore, these institutions are ideal targets of sharp power exercises, a term describing authoritarian regimes' malign, stealthy exploitation of open democratic systems.

THE THREE LEVELS OF ANALYSIS

DIGITAL AUTHORITARIANISM

1. **STATE LEVEL**
   targeted or perpetrated by government-level officials
2. **CORPORATE LEVEL**
   targeted or perpetrated by corporations
3. **INDIVIDUAL LEVEL**
   targeted or perpetrated by individual citizens

corporate level

American Corporations' Compliance in Authoritarian Practices

American corporations have belligerently pursued capital accumulation at the expense of democratic values. This can be observed in Google's recent attempt to re-enter the Chinese market in Project Dragonfly, conforming company standards to meet CCP requirements on censorship and lending the firm's information infrastructure for use in state surveillance systems. With the precedent set, firms will continue to collaborate with authoritarian regimes, adjusting policy and infrastructure uses to state dictums. As the China Model Alternative for development becomes more legitimate due to American corporate assistance, the chasm between China's and America's spheres of influence will continue to grow.

state level

Digital Threats by Law Enforcement on Democratic Freedoms

The use of facial recognition technology (FRT) by U.S. law enforcement engages in digital authoritarian practices of mass surveillance and the erosion of democratic freedoms through its impact on citizen privacy and the increased surveillance of racialized communities. Recent studies have shown that FRT use by law enforcement is 100 times more likely to misidentify Black and Asian faces, leading to further profiling and surveilling of racialized Americans. Clearview AI's FRT has expanded into over 2,400 law enforcement agencies resulting in an increased reliance on mass identification phone apps and expanded imaging databases where the identity of over half of American adults are currently being stored.

corporate level

Facebook's Contribution to Authoritarian Practices

In 2020, Facebook removed many activists' posts while allowing hate groups to thrive on their platform. As a result, Facebook's content moderation practices pose a threat to democracy, as some individual posts that do not violate Facebook's content policies are removed, while other posts that do violate hate speech regulations are kept posted. The inconsistency of content moderation has led to a form of censorship, as certain voices are being silenced by Facebook while others are permitted on the platform. Thus, US lawmakers should work to halt Facebook's contribution to the rise of digital authoritarianism.

individual level

Online Harassment as a Threat to Democracy

Facebook and Twitter have fostered a toxic environment for women online, emboldening harassment and trolling campaigns. This has also made it harder for women in politics to strategically make use of such platforms, enabling political intimidation and suppressing their online voice. Online harassment is a growing barrier to entry for those considering a career in politics. Politicians are also unable to communicate with constituents efficiently due to harassers that flood comment sections and inboxes. Women in general are targeted at a higher rate and young women are more vulnerable in the escalation of online harassment towards attempted physical harm.

31.1K CYBERATTACKS

Cyber security incidents reported by United States federal government agencies in 2018

Source: Statista 2021

30 BRI MEMBER STATES

As of 2019, 30 of the 140 member states have already shifted towards the BeiDou System to more effectively integrate with China

Source: Pacific Forum 2019

117M AMERICANS

As of 2016, over 117 million American adults are listed in law enforcement facial recognition databases

Source: Georgetown University 2016

HATE SPEECH POSTS 32M

32 million posts removed by Facebook in the first half of 2020

Source: Council on Foreign Relations 2021

73% OF WOMEN

73% of women have already been exposed to or have experienced some form of online violence

Source: UNESCO 2015

POLICY RECOMMENDATIONS

1. Implement all outstanding recommendations from past information security reports, conduct annual audits of federal institutions' information security systems, and hold institutions accountable for subsequent implementation.
2. Restrict corporate collaboration with authoritarian regimes through multilateral norm-building efforts bringing corporations in-line with state values.
3. Halt the use of FRT federally until state-led policies are implemented on its use by law enforcement. State policies must include the regulation of everyday use of FRT by local officers as well as administrative permission requests and time-limits on the use of FRT data.
4. Implement fines for technology companies who fail to promptly remove hate speech and violent content and require platforms to report Americans' online violent speech to US authorities.
5. Implement quarantine AI moderation that analyzes content before it is uploaded and provides users with the option to hide potentially harmful content.

REFERENCES

Cheney, Clayton. 2019. "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism." Issues & Insights. Pacific Forum. https://www.pacforum.org/analysis/issues-insights-vol-19-wp8---chinas-digital-silk-road-strategic-technological-competition.
Gallagher, Ryan. 2018a. "Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal." The Intercept. August 1, 2018. https://theintercept.com/2018/08/01/google-china-search-engine-censorship/.
Garvie, Clare, Alvaro Bedoya and Jonathan Frankle. 2016. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." *Georgetown Law: Center on Privacy & Technology*. October 18, 2016. https://www.perpetuallineup.org.
Lopatto, Elizabeth. 2020. "Clearview AI CEO says 'over 2,400 police agencies' are using its facial recognition software." *The Verge*. August 26, 2020. https://www.theverge.com/2020/8/26/21402978/clearview-ai-ceo-interview-2400-police-agencies-facial-recognition.
Polyakova, Alina and Chris Meserole. 2020. "Exporting Digital Authoritarianism: The Russian and Chinese Models." *Brookings Institution*. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.
Shahbaz, Adrian. 2018. *The Rise of Digital Authoritarianism*. Freedom House: Freedom on the Net 2018. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.
Sherman, Justin. 2021. "Digital Authoritarianism and Implications for US National Security." The Cyber Defense Review 6 (1): 107–18. https://www.jstor.org/stable/26994115.
Vail, Hannah. 2017. "Cybersecurity Reform in the Wake of the OPM Breach Notes." Suffolk University Law Review 50 (1): 221–36. https://cpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/3/1172/files/2017/04/Vail_Note_FR-2.15.pdf.
van der Meer, Tom W. G. 2017. "Political Trust and the 'Crisis of Democracy.'" Oxford Research Encyclopedia of Politics, January, 1–21. doi: 10.1093/acrefore/9780190228637.013.77.
Walker, Christopher, and Jessica Ludwig. 2017. "From 'Soft Power' to 'Sharp Power': Rising Authoritarian Influence in the Democratic World." In Sharp Power: Rising Authoritarian Influence, by Juan Pablo Cardenal, Jacek Kucharczyk, Grigorij Mesežnikov, and Gabriela Pleschová. National Endowment for Democracy. https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-Rising-Authoritarian-Influence-Full-Report.pdf.
Ullmann, Stefanie, and Marcus Tomalin. 2020. "Quarantining online hate speech: technical and ethical perspectives." Ethics and Information Technology 22 (1): 69-80. doi: 10.1007/s10676-019-09516-z