DIGITAL AUTHORITARIANISM: PATHWAYS, TRENDS, SOLUTIONS.

Author: Jessica Brandt

Prepared for the Montreal Institute for Genocide and Human Rights Studies

Sept 2022

EMBASSY OF THE UNITED STATES
Ottawa, Canada

Université Concordia University
MONTREAL INSTITUTE FOR GENOCIDE AND HUMAN RIGHTS STUDIES

About the author

Jessica Brandt is policy director for the Artificial Intelligence and Emerging Technology Initiative at the Brookings Institution and a fellow in the Foreign Policy program's Strobe Talbott Center for Security, Strategy, and Technology. Her research interests and recent publications focus on foreign interference, disinformation, digital authoritarianism and the implications of emerging technologies for liberal democracies. Her work has been widely published and quoted in the Washington Post, Associated Press, BBC, NPR, Bloomberg, Vox, Slate, and Wired, among others.

About the Montreal Institute for Genocide and Human Rights Studies

The Montreal Institute for Genocide and Human Rights Studies (MIGS) at Concordia University is Canada's leading think tank working at the intersection of human rights, conflict and emerging technologies. The institute serves as a leadership and ideas incubator that convenes stakeholders with the goal of developing better policies to protect human rights.

Acknowledgements

MIGS would like to thank the U.S. Embassy in Ottawa for the support of this project, which led to the publication of this publication.

Introduction

Authoritarian governments leverage digital technologies to repress the rights and freedoms of their citizens at home, silence dissent among diasporas and other individuals beyond their borders, and to interfere in democratic governments, processes and institutions abroad. China and Russia export surveillance technologies to less-than-wholly free regimes in Africa, South America, and the Middle East. These practices are referred to as digital authoritarianism and have widespread effects on democracy, security, and human rights around the world.

This paper aims to increase understanding of the various pathways through which authoritarian regimes use digital tools to shore up their grip on power at home, weaken democratic governments and institutions that they perceive as threatening to their interests, undermine liberal norms related to privacy and free expression, and replace those norms with illiberal ones. It also outlines approaches that liberal democratic governments can take to push back on digital authoritarianism – approaches rooted in their values.

Methodology

The following white paper is based on a review of academic literature, policy papers and authoritative media reports on digital authoritarianism. The paper also includes the main findings of the digital roundtable discussions and podcast interviews organized and hosted by the MIGS throughout June 2021 and June 2022

The roundtable discussion and podcast interviews featured the following experts:

- Yinka Adegoke, Reporter, Rest of World.
- Noura Aljizawi, Security Researcher, Citizen Lab, University of Toronto.
- Siena Anstis, Senior Legal Advisor, Citizen Lab, University of Toronto.
- Felicia Anthonio, #KeepItOn Campaign Manager, Access Now.
- Jessica Brandt, Policy Director, Artificial Intelligence and Emerging Technology Initiative, and Fellow in Foreign Policy, Brookings Institution.
- Ron Deibert, Director, Citizen Lab, University of Toronto.
- Eileen Donahoe, Executive Director of the Global Digital Policy Incubator (GDPI) at Stanford University, FSI/Cyber Policy Center.
- Rachelle Faust, Assistant Program Officer, International Forum for Democratic Studies, International Forum for Democratic Studies.
- Steven Feldstein, Senior Fellow, Democracy, Conflict, and Governance Program, Carnegie Endowment for International Peace.
- Dr. Sheena Greitens, Associate Professor, LBJ School, and Faculty Fellow, Clements Center for National Security.
- Peter Guest, Enterprise Editor, Rest of the World.

- David Kaye, Clinical Professor of Law at the University of California, Irvine, and former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.
- Andrea Kendall-Taylor, Senior Fellow and Director, Transatlantic Security Program, Center for a New American Security.
- Kyle Matthews, Executive Director, Montreal Institute for Genocide and Human Rights Studies, Concordia University.
- Margaret McCuaig-Johnston, Senior Fellow in the Institute for Science, Society and Policy, University of Ottawa.
- Chris Meserole, Research Director, Artificial Intelligence and Emerging Technology Initiative, and Fellow in Foreign Policy, Brookings Institution.
- Paul Mozur, Correspondent, The New York Times.
- Suzanne Nossel, Chief Executive Officer, PEN America.
- Alina Polyakova, President and CEO, Center for European Policy Analysis.
- Sophie Richardson, China Director, Human Rights Watch.
- Ainikki Riikonen, Research Assistant for the Technology and National Security Program at the Center for a New American Security.
- Amin Sabeti, Executive Director, Digital Impact Lab.
- Kevin Sheives, Associate Director, International Forum for Democratic Studies.
- Caitlin Thompson, Reporter, Coda Story.
- Inga Kristina Trauthig, Research Manager and Senior Research Fellow, Center for Media Engagement, University of Texas.
- Christopher Walker, Vice President for Studies and Analysis at the National Endowment for Democracy, National Endowment for Democracy.
- Burhan Wazir, Managing Editor, Coda Story.

Understanding the Problem

At the end of the Cold War, liberal democracy appeared triumphant -- global norms had shifted in favor of respect for the political and human rights of citizens and the viability of dictatorship was discredited. In this context, the emergence of digital technologies was viewed with optimism. Analysts believed that they would support democratic freedoms by facilitating greater access to information and that they would enable rights advocates, opposition figures, and other civil society leaders to organize and build new connections across communities.[1]

But it is now increasingly clear that these technologies are offering rulers fresh methods for preserving their power. Mass surveillance and censorship allow autocrats to tighten their grip on power at home by exercising strict, effective, and in the case of China, near-totalizing social

[1] Andrea Kendall-Taylor, "Russia and Iran's Digital Authoritarian Playbook," MIGS, November 18, 2021, https://www.youtube.com/watch?v=2T1aOpJeH6M See also: Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs* 99 (2020): 103.

control. Cyber-enabled transnational repression enables autocrats to prevent and deter critics from shedding light on their illiberal practices or otherwise organizing against their interests. The export of these technologies undermines democratic norms that support rights to expression and privacy, which creates space for autocrats to replace those norms with their own illiberal ones. Meanwhile, information operations enable autocrats to weaken democratic competitors – by denting their ability to build and wield soft power, and by fracturing them from within.

Errol Yayboke and Samuel Brannen define this challenge as "the use of the Internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties."[2] Chris Meserole and Alina Polyakova define it as "the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations."[3]

Authoritarian governments -- which over the past fifteen years have become increasingly personalist in character -- use these tools primarily as a means of ensuring the consolidation of their power and home and to eliminate or undermine potential challenges to their legitimacy.[4] The Chinese government's vision for the role of the surveillance state is informed, for example, by Beijing's "comprehensive national security concept," which aims first and foremost to preserve the leadership role of the Chinese Communist Party and of Xi himself.[5] For Russia and Iran, the dynamics are similar. Putin deploys information campaigns abroad to destabilize competitors as a means of compensating for Russia's relative weakness and cementing his own authority. As Ariane Tabatabai has documented, Iranian leadership views these tools as "a means to prevent dissent at home and to ensure regime survival."[6]

Recent research has shown that authoritarian regimes that use digital technologies for repression have become more durable. The use of digital repression reduces the likelihood that such a regime faces internal protest or sustained mobilization efforts, which represent perhaps the most significant threat to dictatorships today. It also enables strongmen to harden their tactics offline. Regimes that increase their use of digital repression tend to increase their use of violent means of crushing dissent "in real life," including torture and the killing of opponents.

---

[2] Erol Yayboke, "Promote and Build: A Strategic Approach to Digital Authoritarianism" (Center for Strategic & International Studies, October 15, 2020), https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism.

[3] Chris Meserole and Alina Polyakova, "Exporting digital authoritarianism : The Russian and Chinese models" (The Brookings Institution, August 2019), https://www.brookings.edu/research/exporting-digital-authoritarianism/.

[4] Torrey Taussig, "The Rise of Personalist Rule" (The Brookings Institution, March 23, 2017), https://www.brookings.edu/blog/order-from-chaos/2017/03/23/the-rise-of-personalist-rule/.

[5] Sheena Chestnut Greitens, "Prepared Testimony before the Senate Armed Services Committee Hearing on "The United States' Strategic Competition with China"," (United States Senate Committee on Armed Services, June 8, 2021), https://www.armed-services.senate.gov/imo/media/doc/06.08%20Greitens%20Testimony.pdf.

[6] Ariane M. Tabatabai, "Iran's Authoritarian Playbook" (Alliance for Securing Democracy, 2020), https://securingdemocracy.gmfus.org/wp-content/uploads/2020/09/Irans_Authoritarian_Playbook.pdf.

Perhaps for these reasons, where digital repression is highest, leaders survive in office longer than in places where digital repression is less significant.[7]

Ultimately, these activities have consequential, detrimental effects on the rights and freedoms of millions of individuals around the world – from citizens living under repressive regimes, including China's Orwellian surveillance state, to those who live in weakly democratic countries that appear susceptible to backsliding. Even in consolidated democracies, academics, journalists, and activists have been bullied or otherwise stifled by the long arm of transnational repression. These societies have faced ongoing cyber and information operations that target a wide range of political events and institutions, making it harder for them to govern themselves.

Pathways of Digital Authoritarianism

Digital authoritarian activity takes place through at least four, overlapping and mutually reinforcing channels: mass surveillance; cyber-operations; censorship; and information operations. The examples highlighted below represent but a sampling of the full range of tactics and strategies strongmen have employed, with a focus on those highlighted by experts during the recent series of roundtable discussions organized by the Montreal Institute for Genocide and Human Rights Studies.

Mass surveillance

In China, digital technologies are enabling Beijing to push the boundaries of social and political control. As Paul Mozur and Aaron Krolik have documented, "Chinese authorities are knitting together old and state-of-the-art technologies — phone scanners, facial-recognition cameras, face and fingerprint databases and many others — into sweeping tools for authoritarian control."[8] Ubiquitous surveillance cameras within China, married with facial recognition algorithms that are embedded with ethnicity detection capabilities, threaten to encode power imbalances into government decision making. Authorities use phone trackers to extract private information and link a user's digital presence with his or her physical movements.[9] And they collect DNA samples, voice prints and iris scans in order to build comprehensive profiles on individuals that are accessible across levels of government.[10] The Chinese government has

[7] Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs* 99 (2020): 103.

[8] Paul Mozur and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers," *The New York Times*, December 18, 2019, sec. Technology, https://www.nytimes.com/2019/12/17/technology/china-surveillance.html.

[9] Isabelle Qian et al., "Four Takeaways From a Times Investigation Into China's Expanding Surveillance State," *The New York Times*, June 21, 2022, sec. World, https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html.

[10] Qian et al.

exported surveillance systems to more than 80 countries around the world, raising concerns about democratic backsliding and the rights of individuals there.[11]

Cyber operations

Numerous illiberal regimes – China, Iran, Russia, Rwanda, Saudi Arabia – have deployed digital tools to silence, harass, or threaten dissidents and activists far beyond their borders, making it harder for rights advocates to continue their work in safety. Repressive governments target the computers and mobile devices, as well as social media and email accounts, of civil society leaders, seeking access to confidential communications and contacts.[12] As Noura Aljizawi and Siena Antis have noted, "Such activity may have several goals, such as uncovering and gaining access to an activist's network, unearthing information to incriminate or track and locate activists to detain or kidnap them, or chilling speech."[13] Likewise, regime-backed hacking groups have disrupted the operation of media and opposition websites based abroad with defacements and Distributed Denial of Service (DDoS) attacks, also to suppress dissent. Meanwhile, the Facebook pages of civil society leaders have been taken down after being targeted by massive false reports that they violated the platform's terms of service.[14]

Strongmen and their proxies have also frequently deployed cyber operations against government institutions, businesses, and media organizations. One goal of this activity is to punish entities perceived to threaten regime interests. Russia, for example, has targeted the Organization for the Prevention of Chemical Weapons, responsible for investigating the poisoning of Russian dissident Sergei Skripal and chemical attacks on Syrian civilians; the Organization for Security and Cooperation in Europe's Monitoring group in Ukraine, responsible for tracking Russian activity in the Donbass region; and the Integrity-initiative, a UK-based think tank that exposes Russian disinformation operations; among many others.[15] Moscow has stolen and weaponized information by strategically releasing it to the public in order to shape political events in France, the United States, United Kingdom, and elsewhere. The Kremlin has also used cyber operations to disrupt organizations that are essential to the functioning of democracy, including legislatures (such as the German Bundestag and UK Parliament) and political parties (in Estonia, France, and Germany).[16]

---

[11] Sheena Chestnut Greitens, "Dealing with Demand for China's Global Surveillance Exports" (The Brookings Institution, April 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200428_china_surveillance_greitens_v3.pdf.

[12] Marcus Michaelsen, "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#footnoteref1_uwy39td.

[13] Noura Aljizawi and Siena Anstis, "The Effects of Digital Transnational Repression and the Responsibility of Host States," *Lawfare*, May 27, 2022, https://www.lawfareblog.com/effects-digital-transnational-repression-and-responsibility-host-states.

[14] Ibid.

[15] Jessica Brandt and Torrey Taussig, "Europe's Authoritarian Challenge," *The Washington Quarterly* 42, no. 4 (October 2, 2019): 133–53, https://doi.org/10.1080/0163660X.2019.1693099.

[16] Ibid.

Censorship

Around the world, repressive governments shut off connectivity or block applications or technologies as a means of enacting information control within their borders, thereby tightening their grasp on power. According to a recent study by Freedom House, this trend is on the rise: last year officials in at least 20 countries suspended internet access; in 21 countries, leaders blocked access to social media platforms.[17] Meanwhile, a growing number of governments are forcing internet service providers to slow, or "throttle" their services during tense political junctures, infringing on expression, preventing journalists from sharing valuable documentation of developments with the public, and stifling the free flow of information.[18] In Turkey, Russia, and elsewhere, governments have imposed problematic legal obligations on platforms to remove offending content. And the Chinese government, for example, uses AI to screen video footage for images of objects like tanks and candles that could be associated with protest messages -- a feat made possible by technology, as video was previously difficult to monitor because it required too much manpower.[19]

Information operations

For autocrats, information isn't just a threat to be tightly controlled at home, but a weapon to be wielded abroad. Numerous illiberal governments use information manipulation tactics – from bots to trolls to a network of sympathetic voices -- to advance their goals. Russia and China both invest large sums in state media apparatuses that operate online in multiple languages, spreading their preferred narratives around the world. Both work through local influencers to try to make their information campaigns appear to be authentic advocacy, posing challenges for government and private sector defenders within target societies.[20] Russia, China, and Iran use malinformation – factually accurate information stripped of context for the purpose of deception -- to try to shape perceptions of politicized events in their favor, recognizing that it can be just as damaging as outright disinformation but much harder to fact check or otherwise moderate.[21] On issues including the origins of COVID, the human rights of Uighurs in Xinjiang, the invasion of Ukraine and the Skripal poisoning, Moscow and Beijing have exploited search engine results to surface propaganda denying culpability, questioning extant evidence, and promoting alternative theories of events.[22] On issues such as race, policing, gun violence, and democratic

---

[17] Adrian Shahbaz and Allie Funk, "The Global Drive to Control Big Tech" (Freedom House, 2022), https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.

[18] Samuel Woodhams, "The Rise of Internet Throttling: A Hidden Threat to Media Development" (Center for International Media Assistance, May 20, 2020), https://www.cima.ned.org/publication/the-rise-of-bandwidth-throttling-a-hidden-threat-to-media-development/.

[19] Paul Mozur, "The Great Firewall: China's model of digital control," MIGS, September 14, 2021, https://www.youtube.com/watch?v=IMDYzAsomGA

[20] Jessica Brandt, "How Autocrats Manipulate Online Information: Putin's and Xi's Playbooks," *The Washington Quarterly* 44, no. 3 (July 3, 2021): 127–54, https://doi.org/10.1080/0163660X.2021.1970902.

[21] Jessica Brandt and Bret Schafer, "Using the Truth to Tell a Lie: Authoritarian COVID-19 Vaccine Malinformation Strategies," *Power 3.0*, May 6, 2021, https://www.power3point0.org/2021/05/06/using-the-truth-to-tell-a-lie-authoritarian-covid-19-vaccine-mal-information-strategies.

[22] Jessica Brandt et al., "Winning the Web: How Beijing Exploits Search Results to Shape Xinjiang and COVID-19," *The Brookings Institution*, May 2022, https://www.brookings.edu/research/winning-the-web-how-beijing-exploits-

practice, both Russia and China regularly use whataboutism to draw false equivalence with their illiberal practices.

Trends

Recognizing that there are gaps in its ability to connect various sources of data in order to make maximum use of what it has collected, the Chinese government is actively working to close what it has deemed "information islands." This means scaling up and integrating various systems, working to make them interoperable at the local level, with the goal of having them ultimately be seamlessly connected at the national level.[23] This has two implications. First, to the extent that such platforms will improve Beijing's ability to better integrate data across stovepipes, they seem likely to sharpen the Chinese government's capacity to conduct digital repression at home. Second, to the extent that these data integration platforms spread globally, they could have a detrimental effect on governance trends worldwide.[24]

There is growing evidence that coordination between Russia and China is increasing. Earlier this year, Putin and Xi released a joint statement highlighting their shared belief "that any attempts to limit their sovereign right to regulate national segments of the Internet and ensure their security are unacceptable," and their intent to "deepen bilateral cooperation in international information security" and shared interest in development new norms of conduct for states on the subject.[25] As Björn Alexander Düben has noted, Russia and China have "extensively 'exchanged experiences' in coordinating state control of mass media and training domestic security personnel, and they have actively cooperated in tightening internet censorship and implementing ever-more-refined surveillance technologies on their territories."[26]

---

search-results-to-shape-views-of-xinjiang-and-covid-19/ ; Jessica Brandt and Valerie Wirtschafter, "The Surprising Performance of Kremlin Propaganda on Google News," *The Brookings Institution*, March 1, 2022, sec. TechStream, https://www.brookings.edu/techstream/the-surprising-performance-of-kremlin-propaganda-on-google-news/ ; Elen Aghekyan and Bret Schafer, "Deep in the Data Void: China's COVID-19 Disinformation Dominates Search Engine Results," *Alliance for Securing Democracy*, October 5, 2021, https://securingdemocracy.gmfus.org/data-void-china-covid-disinformation/ .

[23] Sheena Chestnut Greitens, "Internal Security & Grand Strategy: China's Approach to National Security under Xi Jinping," January 28, 2021, https://www.uscc.gov/sites/default/files/2021-01/Sheena_Chestnut_Greitens_Testimony.pdf ; Sheena Chestnut Greitens, "The Great Firewall: China's Model of Digital Control," Montreal Institute for Genocide and Human Rights Studies, September 14, 2021, https://www.youtube.com/watch?v=MOTuY7I2uuQ ; Huirong Chen and Sheena Chestnut Greitens, "Information Capacity and Social Order: The Local Politics of Information Integration in China," *Governance* 35, no. 2 (2022): 497–523, https://doi.org/10.1111/gove.12592.

[24] Chen and Greitens, "Information Capacity and Social Order."

[25] "Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development," Press Release, February 4, 2022, http://en.kremlin.ru/supplement/5770.

[26] Björn Alexander Düben, "Entente of the Autocrats: Examining the Domestic Drivers of China-Russia Alignment | Part 2: The Centrality of Regime Security," *The London School of Economics and Political Science* (blog), June 15, 2021, https://blogs.lse.ac.uk/cff/2021/06/15/entente-of-the-autocrats-examining-the-domestic-drivers-of-china-russia-alignment-part-2-the-centrality-of-regime-security/.

Meanwhile it is clear that China has been drawing from Russia's information manipulation playbook, even as it develops several of its own unique plays.[27] Like Russia, China increasingly makes coordinated use of multiple, at times conflicting conspiracy theories to cast doubt on official versions of highly politicized events – for example, the origins of the COVID pandemic, which is a salient subject to Beijing, as it endeavors to deflect blame for its own, early mishandling of the crisis. Also like Russia, China increasingly uses whataboutism to paint the United States and other liberal democracies as hypocritical, particularly on issues related to race and democratic performance. In the information space it is less clear that coordination is explicit or formal, but Russia and China's respective activities are nevertheless having a compounding effect.[28]

Russia and China's alignment goes beyond advancing a shared vision for internet governance and deploying similar disinformation tactics aimed at overlapping targets. There is also evidence of coordination among their respective technology sectors. Russia's NTech Lab, for example (one of the country's leading developers of AI and facial recognition technology) has worked with China's Dahua technology (which manufactures video surveillance) to jointly produce a wearable camera with facial recognition capabilities. This kind of coordination could help both parties accelerate the development of surveillance models that may ultimately be replicated elsewhere.[29]

Autocrats increasingly point to technology regulation within liberal societies as justification for repressive policies of their own. For example, Germany´s Network Enforcement Act (NetzDG) -- which obligated social media platforms to swiftly take down illegal content or face stiff financial penalties, raising concerns from rights advocates – has influenced laws in 25 other countries, most of them flawed democracies or authoritarian states without rule of law or protections on expression.[30]

Recommendations

There are many constraints on the ability of and perhaps few opportunities for liberal societies to alter the uses of technology within authoritarian regimes, but there are some measures that could shape the trajectory of digital authoritarianism. For lawmakers within liberal democratic societies these include:

---

[27] Jessica Brandt and Bret Schafer, "How China's 'Wolf Warrior' Diplomats Use and Abuse Twitter," *The Brookings Institution*, October 28, 2020, https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/ ; Brandt, "Playbooks of Putin and Xi."

[28] Brandt, "Playbooks of Putin and Xi."

[29] Jeff Cirillo et al., "The Future of the Digital Order" (Center for a New American Security, November 2021), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-HTI-Nov-2021-finalb.pdf?mc_cid=8dd16fe4c4&mc_eid=d7531df096.

[30] Jacob Mchangama and Natalie Alkiviadou, "The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship - Act Two" (Justitia, 2020), https://justitia-int.org/wp-content/uploads/2020/09/Analyse_Cross-fertilizing-Online-Censorship-The-Global-Impact-of-Germanys-Network-Enforcement-Act-Part-two_Final-1.pdf.

- **Expanding and modernizing legislation to help ensure that entities within democratic societies aren't enabling human rights abuses elsewhere.** This could include imposing sanctions on businesses and entities that give surveillance technology training and equipment to authoritarian regimes that are implicated in human rights abuses. It could also include implementing or using legislation that prevents companies within democratic societies from investing in companies that are building AI tools for repression. The United States in particular could use the Global Magnitsky Act to sanction foreign individuals who are implicated in rights abuses using technology.

- **Strengthening the political and legal frameworks that govern how surveillance technologies are used, recognizing that these technologies are lowering the costs of leaders' efforts to consolidate power within fragile democracies.** This could include building the capacity of civil society groups – including activists and watchdog organizations– to push back on and build resilience against worrying trends within weak democracies looking to adopt some of these technologies.

- **Before implementing new technology regulations, anticipating the ways that authoritarian states seeking stricter information control at home will copy and abuse legislation within liberal societies to advance their own illiberal goals.** Where possible, lawmakers should draft legislation in ways designed to make it harder for autocrats to do so.

- **Seizing the initiative in the information space, harnessing truthful messaging to push back on authoritarian advances.** This should include efforts to expose autocrats' failures and false promises, as the United States and its partners did ahead of and during the Ukraine crisis, when they quickly declassified information documenting Putin's preparations for a false flag operation that would enable him to justify his invasion with lies, and when they provided ongoing information about Russian troop death numbers likely to raise the ire of the Russian population.[31]

- **Standing behind companies that face pressure from authoritarian governments to take repressive actions**, both rhetorically, and by imposing tangible costs on regimes that do so.

- **Enacting strong privacy legislation** that: affords government limited ability to access personal data (only in circumstances prescribed by law, subject to judicial authorization, and on a time limited basis); requires companies to disclose how they use an individual's data, identify what third parties may have access to it, and what those third parties can

[31] Jessica Brandt, Zack Cooper, Bradley Hanley, and Laura Rosenberg, "Linking Values and Strategy: How Democracies Can Offset Autocratic Advances," Alliance for Securing Democracy, October 30, 2020. https://securingdemocracy.gmfus.org/wp-content/uploads/2020/10/Linking-Values-and-Strategy.pdf

use it for; and obligates companies to quickly notify users if their information is compromised.[32]

- **Prioritizing engagement in standards-setting bodies and with international technical organizations that shape the rules and norms of the future Internet** and other technologies to ensure that the decisions they make support the rights and freedoms of individuals worldwide. This should include coordination with like-minded governments.[33]

Other actors within liberal societies have a role to play as well:

- **Major western social media platforms should provide greater transparency around their content moderation decisions.** This should include providing clear and comprehensive information about the specific requests they have received from governments, how they have responded, and on what basis their decisions were made. This should also include providing processes for appeal, recognizing that content moderation can be a tool that governments use to suppress speech.

- **Technology companies should fully live up to their existing obligations under the UN Guiding Principles on Business and Human Rights**, which require firms to assess whether their business practices may cause or contribute to adverse human rights impacts and to address any such findings.[34] On an ongoing basis, they should monitor how their tools are used by governments and be prepared to act when there is documented evidence of abuse.

- **Companies and governments that undertake public-private surveillance partnerships should**, **"incorporate specific agreements reflecting principles of transparency**, rules-respecting procurement, accountability, oversight, legality, necessity and proportionality, and redress," as Privacy International has proposed and Steven Feldstein has echoed.[35]

- **Industry could establish global standards for appropriate applications of facial recognition technology** that respects human rights and the rule of law, based on

[32] "Policy Recommendations: Internet Freedom," Freedom House, n.d., https://freedomhouse.org/policy-recommendations/internet-freedom.
[33] Lindsay Gorman, "The U.S. Needs to Get in the Standards Game—With Like-Minded Democracies," *Lawfare*, April 2, 2020, https://www.lawfareblog.com/us-needs-get-standards-game%E2%80%94-minded-democracies.
[34] "Guiding Principles on Business and Human Rights" (United Nations, 2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.
[35] Steve Feldstein, "The Global Struggle over AI Surveillance" (National Endowment for Democracy, June 7, 2022), https://www.ned.org/wp-content/uploads/2022/06/Global-Struggle-Over-AI-Surveillance-Feldstein.pdf ; "Safeguards for Public-Private Surveillance Partnerships," Privacy International, n.d., https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships.

principles of fairness, transparency, accountability, nondiscrimination, notice and consent, and lawful surveillance.[36]

- **Academic institutions conducting scientific research – and in particular, research related to sensitive, potentially dual use technologies or other high risk technology applications - should implement due diligence measures** to ensure that they are not inadvertently partnering with entities that are implicated in digital repression.

- **Civil society groups should continue to conduct research on the contours and implications of intrusive surveillance technologies.** This should include technical analyses to identify human rights risks of emerging technologies.[37]

By taking these steps, democratic societies can push back on various forms of digital authoritarianism to limit their detrimental effects, and in so doing, help advance the political and human rights of millions of people around the world.

[36] Lindsay Gorman and Matt Schrader, "U.S. Firms Are Helping Build China's Orwellian State – Foreign Policy," *Foreign Policy*, March 19, 2019, https://foreignpolicy.com/2019/03/19/962492-orwell-china-socialcredit-surveillance/.
[37] "Policy Recommendations."

RESOURCES

Combating Digital Authoritarianism Project panel discussions

MIGS. "#RightsCon 2021: Spotlight on digital authoritarianism." *YouTube,* June 8, 2021, https://www.youtube.com/watch?v=xE43Dwe0UGA&list=PLdSO17Wd8O7hHAX2f7-K7-tHN1x_jatOp&index=3

MIGS. "#RightsCity: Confronting digital authoritarianism." *YouTube*, June15, 2021, https://www.youtube.com/watch?v=bpAuLf283hY&list=PLdSO17Wd8O7hHAX2f7-K7-tHN1x_jatOp&index=4

MIGS. "The Great Firewall China's model of digital control." *YouTube*, September 14, 2021, https://www.youtube.com/watch?v=IMDYzAsomGA&list=PLdSO17Wd8O7hHAX2f7-K7-tHN1x_jatOp&index=3&t=6s

MIGS. "Digital Authoritarianism Without Borders." *YouTube,* October 19, 2021, https://www.youtube.com/watch?v=cnWL5kEIUVU&list=PLdSO17Wd8O7hHAX2f7-K7-tHN1x_jatOp&index=2&t=6s

MIGS. "Russia and Iran's Digital Authoritarian Playbook." *YouTube,* November 18, 2021, https://www.youtube.com/watch?v=2T1aOpJeH6M&list=PLdSO17Wd8O7hHAX2f7-K7-tHN1x_jatOp&index=6

MIGS. "What next? US-Canadian relationship to confront digital authoritarianism." *YouTube*, June 18, 2022, https://www.youtube.com/watch?v=yzv56nr2V-I&list=PLdSO17Wd8O7hHAX2f7-K7-tHN1x_jatOp&index=8&t=4s

Combating Digital Authoritarianism Podcast interviews

MIGS, host. "Discussing Sharp Power with Kevin Sheives and Rachelle Faust." Human Rights Talks, MIGS, April 14, 2022. https://podcasts.apple.com/us/podcast/human-rights-talks-discussing-sharp-power-with-kevin/id1483243995?i=1000557610647.

MIGS, host. "Internet Shutdowns and #KeepItOn with Felicia Anthonio." Human Rights Talks, MIGS, June 3, 2022. https://podcasts.apple.com/us/podcast/internet-shutdowns-and-keepiton-with-felicia-anthonio/id1483243995?i=1000565119447.

MIGS. "Digital Authoritarianism with Caitlin Thompson." Human Rights Talks, MIGS, May 24, 2022. https://podcasts.apple.com/us/podcast/digital-authoritarianism-with-caitlin-thompson-coda/id1483243995?i=1000563526578.

MIGS, host. "Peter Guest on internet shutdowns." Human Rights Talks, MIGS, May 11, 2022. https://podcasts.apple.com/us/podcast/peter-guest-on-internet-shutdowns/id1483243995?i=1000560528672.

MIGS Articles

Marie Lamensch. “In Latin America, Youthful Branding Meets Authoritarian Populism,” Marie Lamensch, *Centre for International Governance Innovation*, 21 March, 2022. https://www.cigionline.org/articles/in-latin-america-youthful-branding-meets-authoritarian-populism/

Kyle Matthews and Lauren Salim. “Why Canadians need to take digital disinformation seriously,” *The Hill Times*, March 29, 2021. https://www.hilltimes.com/2021/03/29/why-canadians-need-to-take-digital-disinformation-seriously/291091

Kyle Matthews. “Will Canada Finally Take a Stand Against China’s Totalitarian Use of Tech?”, *The Macdonald-Laurier Institute*, 3 February 2022. https://macdonaldlaurier.ca/will-canada-finally-take-stand-chinas-totalitarian-use-tech-kyle-matthews-inside-policy/

Marie Lamensch. “Authoritarianism Has Been Reinvented for the Digital Age,” Cent*re for International Governance Innovation*, 9 July 2021, https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/

Marie Lamensch. “The Cost of an Internet Shutdown”, Marie Lamensch, *Centre for International Governance Innovation*, March 9, 2021. https://www.cigionline.org/articles/cost-internet-shutdown/

Kyle Matthews and George Tsagaroulis. “Why Canada must confront the rise of digital authoritarianism,” *OpenCanada.org,* November 18, 2020. https://opencanada.org/why-canada-must-confront-the-rise-of-digital-authoritarianism/