Digital Repression

Edited by Chris Ogden and Olivia Hagen

Published by Global Policy Journal at Smashwords

Cover Image: https://www.pexels.com/photo/abstract-colorful-background-of-night-star-4021521/ via Pexels.com

Citation: Ogden, C. and Hagen, O. Eds. (2023) Digital Repression. Durham: Global Policy.

ENDORSEMENTS

Digital Repression is an excellent introduction to a complex topic that concerns citizens, political and social activist, and political decision makers alike. The book merits a wide readership and deserves to be a standard read in advanced school and undergraduate social science and ITeducation.

Bettina Koch, Professor of Political Science, Virginia Polytechnic Institute & State University, Visiting Professor, TU Darmstadt.

Within little more than a decade, the internet in general, and social media in particular, has gone from being a vehicle for liberation and empowerment to becoming a cesspit of misinformation, hate-speech and political manipulation. This ebook expertly analyses the origins and nature of this negative journey, and what policy makers can do to restrain or reverse it.

Duncan Green, Professor in Practice at London School of Economics and Political Science and Strategic Advisor, Oxfam.

CONTENTS

Introduction: Digital Repression: Causes, Consequences and Policy Responses

Chris Ogden and Olivia Hagen

In April 2022, a report by the investigative news outlet Inside Story revealed that financial journalist and editor Thanasis Koukakis had been targeted by "Predator" spyware (Mildebrath 2022b). Manufactured by Cytrox, the spyware infects a target's cellphone by delivering a one-time "phishing" link, enabling the operator to monitor every aspect of the target's cellphone (Marczak et al. 2021). Google and CitizenLab have asserted that the spyware has been primarily bought by government-backed actors (Lecigne and Resell 2022). Subsequent to the initial report, another news outlet, Reporters United, revealed that the Greek National Intelligence Service (EYP) had been monitoring Koukakis from June to August 2020; however, Koukakis was only made aware of this surveillance by CitizenLab in March 2022.

The hack had been undertaken with authorisation from prosecutor Vasiliki Vlachou, who oversees matters regarding the EYP, and has ties to other high-ranking government officials. Although the Greek government was cleared in an investigation regarding the wiretap (Mildebrath 2022b), days later it was made public that the EYP and Vlachou had authorised a wiretap of Nikos Androulakis, a member of the European Parliament and leader of the Greek opposition party Pasok. After reports implicated several more high-ranking officials, the Secretary-General to the Prime Minister, Grigoris Dimitriadis, and the EYP Director, Panagiotis Kontoleon, resigned. In November 2022, it was then revealed that more than thirty people had been victims of state-sanctioned mobile spyware. The Greek Prime Minister Kyriakos Mitsotakis has denied these accusations, which have been subsequently investigated by various prosecutors, including the European Parliament (Reuters 2022a).

The "Greek Watergate" is not an isolated incident. Following reports from CitizenLab, Amnesty International and eighteen other media organisations in the summer of

2021, it was uncovered that 50,000 persons within the EU have been targeted by spyware (In 't Veld 2022, 3). The Greece investigation became part of a more extensive European Parliament inquiry into the use of spyware by other EU countries, including Spain, Poland, Hungary and Cyprus. It has been reported that all EU Member States have acquired one or more commercial spyware products and that the NSO group sold its products to 14 Member States (Ibid, 4-5)

Such spyware, and its ever-widening use, is emblematic of the contemporary prevalence of digital repression as a way to monitor, control and coerce forms of political and social opposition. Specifically, technologies such a Predator and "Pegasus" (Gurijala 2021) have been linked to the murder of Saudi Arabian journalist Jamal Khashoggi and various human rights abuses (Mildebrath 2022a, 1). These tools are highly invasive, allowing operators total access to files, messages, metadata and communications of the person they target, all from a distance and without alerting the victim. The material obtained can then be used in order to intimidate, discredit and manipulate the victims (In 't Veld 2022, 3). The abuses perpetrated by spyware are not only gross violations of the right to privacy and civil liberties but also undermine democracy and democratic institutions, which are the cornerstones of the legal order in Europe and the western world (Liger and Gutheil 2022, 8-9).

The utilisation of spyware is part of a global trend involving the deployment of modern internet and communication technologies (ICTs) - the internet, computer, mobile phone, and social media (Diamond 2010, 70) – for purposes of social control and repression. For example, following nationwide protests in response to the murder of Mahsa Amini, the Iranian government shut down the internet and disrupted services to Instagram and Whatsapp (Nast 2022). In 2020, in Thailand, where the internet is severely restricted, authorities arrested and harassed internet users and pro-democracy leaders who criticised the monarchy (Freedom House 2021). Since 2016, the Chinese Communist Party has used facial recognition and emotion detection cameras, smart checkpoints and phone monitoring software (Roche and

Leibold 2022) in order to surveil, oppress and arrest ethnic Uighurs in Xinjiang province (Human Rights Watch 2019). At the most extreme, in 2020 29 countries carried out a total 155 internal internet shutdowns, 109 of which were done by India, including for the whole year in the Kashmir region (KIO 2021).

Digital Repression as a Global Trans-Political Phenomenon

Steven Feldstein defines digital repression as ‘the use of information and communications technology to surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state´ (Feldstein 2021, 25), which enhances a state´s ability to carry out ‟traditional″ modes of repression. Such a definition allows for the investigation of digital repression in a range of regime types, from authoritarian regimes to democracies, so as to better comprehend how governments employ repressive digital tactics and for what purposes. As shown by the essays in this volume, this definition will help interested readers to better understand how digital repression is manifesting in different parts of the world and vitally underscores that it is a global phenomenon that now requires global policy responses.

The rise of digital repression arrived with the spread of ICTs and social media in the early 2000s. It was initially believed that these technologies would help end the tyrannical reign of autocrats around the world. Earlier research offered a theory of "liberation technology", arguing that ICTs were powerful tools which would empower citizens to collectively mobilise against their repressive rulers (Gohdes 2020; Weidmann and Rød 2019). Such normative arguments as per the internet's positive potential exploded after the Arab Spring, when social media helped empower activists to coordinate protests which helped topple regimes in Libya, Egypt and Tunisia. So-called "cyberoptimists" argued that they have the ability to disrupt authoritarian regimes, facilitate popular protest, contribute to regime reforms and transitions, and even spread democracy across the globe.

However, it also became clear that these new technologies, whilst giving voice to activists around the globe, also served to ‘supercharge long-standing authoritarian survival tactics´ (Kendall-Taylor, Frantz, and Wright 2020). As such, aspiring "digital dictators" began using technology to control, manipulate, surveil and repress their citizens to sustain their political authority (Feldstein 2021, 23-24). China is furthermore exporting the technologies underpinning its massive online censorship and surveillance system. Such "algorithmic authoritarianism" includes the selling of intelligent monitoring systems and facial recognition technology; the training of local media elites and government officials concerning new media or information management; and dozens of countries buying telecom infrastructure, internet and mobile networking equipment installed by Chinese companies (Shahbaz 2018).

Such dangers are also evident within mature democracies. Coupled with business models that harvest and monetise personal data, the dominance of companies such as Facebook and Google are incompatible with the right to privacy, and 'pose a serious risk to a range of other rights, from freedom of expression and opinion, to freedom of thought and the right to non-discrimination' (Amnesty International 2019). In April 2021, investigators revealed that Facebook officials' repeatedly allowed world leaders and politicians to use its platform to deceive the public or harass opponents despite being alerted to evidence of the wrongdoing' (Wong 2021). This practice included in India, where fake accounts were allowed to inflate the popularity of leaders (months after Facebook was alerted to the problem), as well as across Europe, Asia and the Americas (Wong and Ellis-Petersen 2021). Such a confluence has led to declining internet freedom from 2010 to 2018, as the rise of "digital authoritarianism" that is eroding global freedoms of speech, the press, assembly and petition (Shahbaz 2018).

Argument & Structure

The contributors to this serialised e-book argue that ICTs are tools which can be used for both virtuous and wicked purposes. As such, its essays investigate different

dimensions of digital repression in order to understand how and why governments employ repressive digital tactics. While autocrats more widely employ digital repression, it is paramount to understand that democracies also use repressive digital tactics for various reasons. By looking at a range of regime types, this volume increases policymakers' and researchers' understanding of the topic, and underlines the threat that digital repression poses to internet freedom and democracy around the globe.

Written by a group of the world's leading academic and policy experts, this forensic exposition of "digital repression" proceeds along four core themes. The first underscores how different digital techniques are used in digital oppression, how they differ in outcomes, and why some states employ digital repression. The second theme then probes who is responsible for the rise of digital repression and the role that states and private companies have in spreading its usage. In turn, the third theme highlights the consequences of digital repression and its dangers, before the final theme synthesises these perspectives to offer effective and practical policy responses for all key global stakeholders.

Dr Chris Ogden is Senior Lecturer / Associate Professor in Asian Security and Asian Affairs in the School of International Relations at the University of St Andrews, Scotland. His research interests concern the global rise of India and China, great power politics, shifting world orders, authoritarianism, the Asian Century, Hindu nationalism, and the interplay between national identity, security and domestic politics in South Asia (primarily India) and East Asia (primarily China). Chris' latest book concerns The Authoritarian Century: China's Rise and the Demise of the Liberal International Order (Bristol UP) and he was also the Series Consultant for the 2023 BBC Documentary Series, India: The Modi Question. For more information, see http://chris-ogden.org

Olivia Mills Hagen is currently in her final year of an MA (Hons.) in International Relations at the University of St Andrews and an intern for Global Policy Online. Before university, she decided to do her National Service and spent a year in Northern Norway in the Norwegian Army's Artillery Battalion. During her time at St Andrews, Olivia has been the director of the Lumsden Leadership Summit, a platform that invites successful and inspiring women to speak to inspire the student body and help them become the next generation of leaders. As the director, she focused the summit on sustainability and invited women whose diverse careers shared sustainability as the common denominator. Her

academic research is centered on the intricate and multifaceted phenomenon of digital repression, as well as international development, foreign policy of India and China and force and statecraft.

Photo by Sora Shimazaki

References

Amnesty International. 2019 "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights". Amnesty International. 21 November 2019. https://www.amnesty.org/en/documents/pol30/1404/2019/en/

Diamond, Larry. 2010. "Liberation Technology." Journal of Democracy 21 (3): 69–83. https://doi.org/10.1353/jod.0.0190.

Feldstein, Steven. 2021. The Rise of Digital Repression How Technology Is Reshaping Power, Politics, and Resistance. Oxford: Oxford University Press USA - OSO.

Frantz, Erica, Andrea Kendall-Taylor, and Joseph Wright. 2020. "Digital Repression in Autocracies Users Working Paper SERIES 2020:27 the VARIETIES of DEMOCRACY INSTITUTE." https://www.v-dem.net/media/publications/digital-repression17mar.pdf

Freedom House. 2021. "Thailand: Freedom on the Net 2021 Country Report." Freedom House. 2021. https://freedomhouse.org/country/thailand/freedom-net/2021

Gohdes, Anita R. 2020. "Repression Technology: Internet Accessibility and State Violence." American Journal of Political Science 8 (10). https://doi.org/10.1111/ajps.12509

Gurijala, Bhanukiran. 2021. "What is Pegasus? A Cybersecurity Expert Exaplians How the Spyware Invades Phones and What it Does When it Gets In". The Conversation. August 9, 2021. https://theconversation.com/what-is-pegasus-a-cybersecurity-expert-explains-how-the-spyware-invades-phones-and-what-it-does-when-it-gets-in-165382

Human Rights Watch. 2019. "China's Algorithms of Repression." Human Rights Watch. May 1, 2019. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

In 't Veld, Sophie. 2022. "Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware." Www.europarl.europa.eu. European Parliament. https://www.europarl.europa.eu/committees/en/pega-findings/product-details/20221114CAN67684

KIO. 2021. "Internet Shutdowns Report: Shattered Dreams and Lost Opportunities: A Year in the Fight to #KeepItOn." KeepItOn. 3 March, 2021. https://www.accessnow.org/keepiton-report-a-year-in-the-fight/

Lecigne, Clement, and Christian Resell. 2022. "Protecting Android Users from 0-Day Attacks." Google. May 19, 2022. https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/

Liger, Quentin, and Mirja Gutheil. 2022. "The Use of Pegasus and Equivalent Surveillance Spyware - the Existing Legal Framework in EU Member States for the Acquisition and Use of Pegasus and Equivalent Surveillance Spyware" Www.europarl.europa.eu. https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740151

Marczak, Bill, John Scott-Railton, Bahra Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Bredan, and Ronald Deibert. 2021. "Pegasus vs. Predator: Dissident's

Doubly-Infected IPhone Reveals Cytrox Mercenary Spyware - the Citizen Lab.″ Citizenlab.ca. December 16, 2021. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

Mildebrath, Hendrik. 2022a. ‟Europe´s PegasusGate.″ European Parliament. https://doi.org/10.1007/s11590-022-01905-6.

———. 2022b. ‟Greece´s Predatorgate: The Latest Chapter in Europe´s Spyware Scandal?″ Www.europarl.europa.eu. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)733637

Nast, Condé. 2022. ‟Iran´s Internet Shutdown Hides a Deadly Crackdown.″ Wired UK. September 23, 2022. https://www.wired.co.uk/article/iran-protests-2022-internet-shutdown-whatsapp

Reuters. 2022a. ‟EU Parliament to Help Probe ‛Inexcusable´ Spying on Greek Member.″ Reuters, August 17, 2022, sec. Europe. https://www.reuters.com/world/europe/eu-parliament-help-probe-inexcusable-spying-greek-member-2022-08-17/

———. 2022b. ‟Greece to Ban Sale of Spyware amid Wiretapping Scandal.″ Reuters, November 7, 2022, sec. Europe. https://www.reuters.com/world/europe/greece-ban-sale-spyware-amid-wiretapping-scandal-2022-11-07/

Roche, Gerald, and James Leibold. 2022. ‟State Racism and Surveillance in Xinjiang (People´s Republic of China).″ The Political Quarterly 93 (3)

Shahbaz, Adrian. 2018. ‟Freedom on the Net 2018: The Rise of Digital Authoritarianism.″ Freedom House. October, 2018. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Weidmann, Nils B., and Espen Geelmuyden Rød. 2019. The Internet and Political Protest in Autocracies. Oxford University Press. https://doi.org/10.1093/oso/9780190918309.001.0001

Wong, Julia Carrie. 2021. "How Facebook Let Fake Engagement Distort Global Politics: a Whistleblower's Account." The Guardian. 12 April, 2021. https://www.theguardian.com/technology/2021/apr/12/facebook-fake-engagement-whistleblower-sophie-zhang

Wong, Julia Carrie and Hannah Ellis-Petersen. 2021. "Facebook Planned to Remove Fake Accounts in India – Until it Realized a BJP Politician was Involved." The Guardian. 15 April, 2021. https://www.theguardian.com/technology/2021/apr/15/facebook-india-bjp-fake-accounts

1. Understanding the Incentives Driving Digital Repression

Steven Feldstein

There is a growing recognition that digital technologies can threaten democracy and human rights, empower autocratic regimes, facilitate censorship, and abet surveillance. Yet, researchers and policymakers frequently misunderstand what constitutes digital repression and what factors drive its spread. After laying out constitutive elements of digital repression and describing general trends about digital repression´s relationship to regime type, I will discuss three common inaccuracies related to drivers of technological repression.

Digital repression exhibits a strong relationship with regime type. Regimes that are more authoritarian are more likely to deploy digital repression tools, from mass surveillance and biometrics to online censorship and internet shutdowns (Feldstein 2021). As Figure 1 shows, highly authoritarian countries – such as China, Iran, and North Korea – have elevated levels of digital repression. Conversely, strong liberal democracies, particularly governments in northern Europe, register lower levels of digital repression.

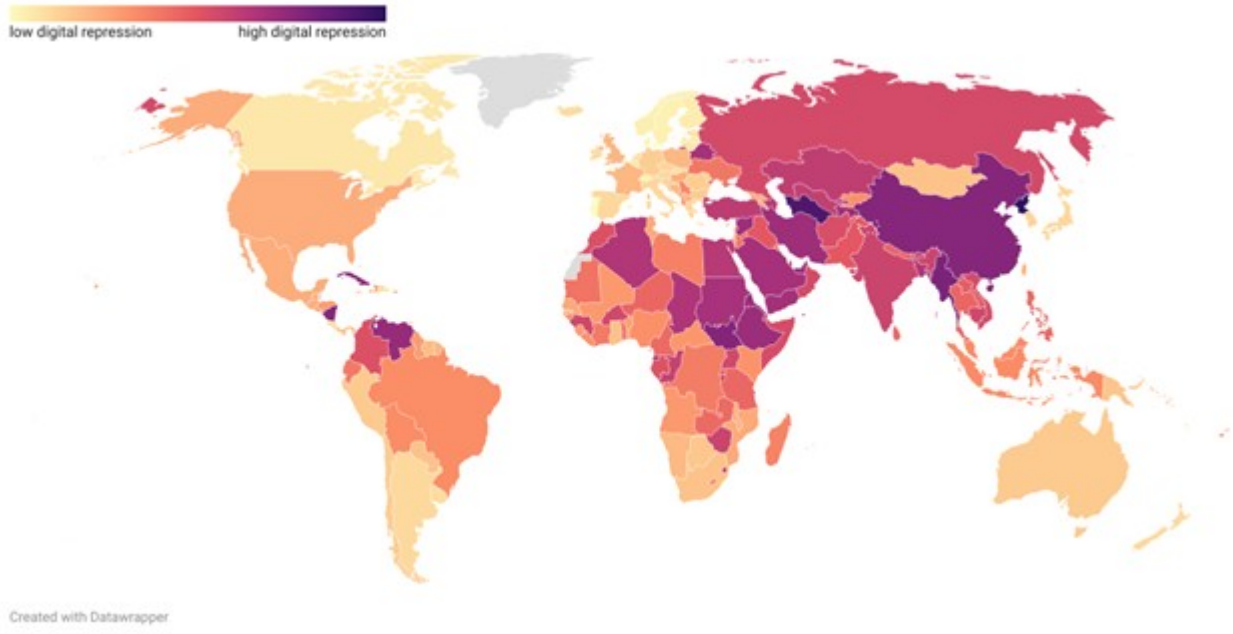

Figure 1. Global prevalence of digital repression in 2021 (Feldstein, Steven. 2022. "Digital Repression Index (updated 2021 data)". Mendeley Data, V3, doi: 10.17632/5dnfmtgbfs.3)

Digital repression strategies are not uniform; they vary across countries and regime types. Strategies deployed by authoritarian and democratic states differ based on a range of factors: administrative capacity, political norms, resource availability, and regime context. Authoritarian states often rely upon sophisticated digital strategies to control the flow of information and prevent citizens from accessing or publishing content critical of government policies. Experts cite China as a case-study in digital repression. Chinese authorities have established a "great fire wall" that filters content coming in and out of the country, banned foreign internet platforms such as Google and Facebook, and constructed a vast surveillance apparatus combining online monitoring with physical devices (Roberts 2018). China, however, is unique. No other authoritarian regime has attained China's level of digital repression. In Russia, for example, while there is a growing amount of online censorship and an emerging surveillance apparatus, it still contains permissive elements: YouTube remains accessible to Russian citizens; government officials and ordinary citizens rely on Telegram for communication (Soldatov and Borogan 2022). As Leonid Kovachich and Andrei Kolesnikov (2021) write, "there are vast gaps between the Russian government's aspirations and its actual ability to harness digital tools such as facial recognition software using artificial intelligence, or China's nascent social credit system".

Digital repression tactics are not limited to authoritarian governments; democracies also deploy these tactics. Particularly among weaker democracies, governments frequently use digital repression tools to support their political objectives. In India, for instance, Prime Minister Narendra Modi's administration has pressed platforms to suppress content that is critical of the government and has authorized police units to raid internet companies that express disagreement with the government's policies (Iyengar 2023). India also has an "emergent surveillance regime" that includes AI-enabled facial recognition technology and even drones that have been "mainstreamed into public life without statutory basis or the consent of the surveilled" (Mahapatra 2021).

While most people have an intuitive sense of what digital repression encompasses, its underlying causes and possible responses remain debated. Policymakers and experts tend to mischaracterize several aspects in this regard.

First, policymakers often describe digital repression as a problem largely driven by China. They emphasize that the Chinese state is "working to export its high-tech tools and authoritarian principles throughout the globe" (Committee on Foreign Relations 2020) and is advancing an "alternate vision to digital freedom" that is a core part of its strategy to "reshape and lead a new global order" (Special Competitive Studies Project 2022). To be sure, China's diffusion of digital technology is shaping data governance and leading to negative policy outcomes. China influences global norms through "parallel modeling" – demonstrating the benefits of censorship and surveillance tools and thereby making their use more attractive to other countries (Repnikova 2022). China is attempting to sway the technical standards process in favor of Chinese technologies and infrastructure to reinforce its core foreign policy objectives (Teleanu 2021). The Chinese government also subsidizes advanced technological exports, assuming that countries which build out their technical needs using Chinese equipment are more likely to use Chinese standards and products for future needs (Feldstein 2022a).

Yet on their own, these factors do not render China the primary or exclusive driver of digital repression worldwide. For one, Chinese companies are not the only suppliers of repressive digital tools to autocratic leaders. They face stiff competition from firms based in democracies (in the spyware surveillance sector, for example, companies based in Europe, Israel, and the United States, exhibit far more sales than Chinese firms). There is also scant evidence that China is leveraging the export of repressive technology in pursuit of a grand strategy to establish an alternate governance model (Weiss 2019). In my research, government officials highlighted the low cost of Chinese technology as the most compelling reason to acquire products from Chinese firms (Feldstein 2021).

Second, experts often treat digital technology as an "independent variable" or an "exogenous shock" – relying heavily on supply-side explanations to account for the presence of technological repression (Drezner 2019). Rather than scrutinize political

motivations or incentives for why regimes seek intrusive technologies in the first place, experts focus heavily on technological acquisition factors. But overlooking regime dynamics means that analysts are only getting half the picture when it comes to understanding the drivers of digital repression. As Matthew Erie and Thomas Streinz (2021) write, "The digital authoritarianism thesis tends to assume that authoritarians are interchangeable and that China's data governance approach can be exported". The reality is more complicated. Many factors determine whether a country will deploy certain digital techniques over others. In Brazil, for instance, there is an established tradition of protecting free expression, meaning that authoritarian censorship strategies – such as filtering content or blocking websites – would face public backlash. In substitute, political parties and politicians (such as former President Jair Bolsonaro) have deployed disinformation strategies. In the run-up to the 2022 election and the subsequent attacks on Brazil's federal government buildings, disinformation played a prominent role, with false claims about "corruption, Covid, deforestation, and even cannibalism" circulating widely (Horton and Gragnani 2022).

Third, experts place considerable emphasis on export controls as a means to curb digital repression, contending that if democracies stem the supply of digital technologies this will mitigate surveillance or censorship concerns (Polyakova and Meserole 2019). However, it is nearly impossible to stop the diffusion of general use technologies once these innovations have been commercialized. As Audrey Cronin notes in her book Power to the People, at the close of the twentieth century, the United States made a conscious decision to shift from "closed technological development". where states largely control access to major technological innovations, to "open development", where innovations are driven by the commercial sector. Devices like smartphones would not exist "without US-government funded programs that created key components, including the microchips, touchscreens, and voice activation systems" (Cronin 2019). But the downside of the open technological revolution is that a wide group of countries – authoritarian and democratic – and even non-governmental actors, can access these same technologies to design

repressive systems, whether filtering online content, surveilling private communications and data, or distorting political narratives.

In order for policymakers to come up with practical and effective solutions to counter digital repression, it is essential they have an accurate understanding about its characteristics. The global prevalence of digital repression is not simply a function of Chinese technological exports. Supply-side factors are insufficient to explain why governments choose to acquire digital tools. And stringent export controls on their own will do little to curb the spread of digital repression. Instead, policymakers should look at regime incentives, political interests, and resource capacity to better understand why regimes acquire and deploy repressive technologies.

Steven Feldstein is a senior fellow at the Carnegie Endowment for International Peace in the Democracy, Conflict, and Governance Program. His research focuses on technology and politics, U.S. foreign policy, international relations, and the global context for democracy and human rights. Feldstein is the author of The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance (2021), which is the recipient of the 2023 Grawemeyer Award for Ideas Improving World Order.

References

Committee on Foreign Relations, United States Senate. 2020. "The New Big Brother: China and Digital Authoritarianism." https://www.govinfo.gov/content/pkg/CPRT-116SPRT42356/pdf/CPRT-116SPRT42356.pdf

Cronin, Audrey Kurth. 2019. Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists. Oxford University Press

Drezner, Daniel. 2019. "Technological Change and International Relations." International Relations, 33(2), pp. 286-303

Feldstein, Steven. 2021. The Rise of Digital Repression How Technology Is Reshaping Power, Politics, and Resistance. Oxford University Press

Feldstein, Steven. 2022a. ‟China′s High-Tech Surveillance Drives Oppression of Uyghurs.″
Bulletin of the Atomic Scientists. https://thebulletin.org/2022/10/chinas-high-tech-surveillance-drives-oppression-of-uyghurs/

Feldstein, Steven. 2022b. ‟Digital Repression Index (updated 2021 data).″ Mendeley Data, V3, doi: 10.17632/5dnfmtgbfs.3

Horton, Jake and Juliana Gragnani. 2022. ‟Brazil Election: Accusations and Misinformation on the Campaign Trail.″ BBC
News. https://www.bbc.com/news/63374100.
Iyengar, Rishi. 2023. ‟Modi is Muzzling Big Tech.″ Foreign
Policy. https://foreignpolicy.com/2023/01/27/modi-big-tech-india-bbc-documentary-twitter/

Kovachich, Leonid and Andrei Kolesnikov. 2021. ‟Digital Authoritarianism with Russian Characteristics?″ Carnegie Endowment for International
Peace. https://carnegiemoscow.org/2021/04/21/digital-authoritarianism-with-russian-characteristics-pub-84346

Mahapatra, Sangeeta. 2021. Digital Surveillance and the threat to Civil Liberties in India. German Institute for Global and Area Studies. https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india

Ong, Jonathan and Jason Cabañes. 2018. ‟Architects of Networked Disinformation.″ Newton Tech4Dev Network. https://doi.org/10.7275/2cq4-5396

Polyakova, Alina and Chris Meserole. 2019. "Exporting Digital Authoritarianism. The Russian and Chinese Models." Brookings. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

Repnikova, Maria. 2022. Chinese Soft Power. Cambridge University Press

Roberts, Margaret E. 2018. Censored: Distraction and Diversion Inside China's Great Firewall. Princeton University Press

Soldatov, Andrei and Irinia Borogan. 2022. "The New Iron Curtain." Center for European Policy Analysis. https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/.

Special Competitive Studies Project. 2022. "Defending Digital Freedom and the Competition for the Future of the Global Order." https://www.scsp.ai/wp-content/uploads/2022/12/FP-IPR-FOR-RELEASE.pdf

Teleanu, Sorina. 2021. "The Geopolitics of Digital Standards: China's Role in Standard-Setting

Organizations." DiploFoundation. https://www.diplomacy.edu/resource/report-the-geopolitics-of-digital-standards-chinas-role-in-standard-setting-organisations/

Weiss, Jessica Chen. 2019. "A World Safe for Autocracy? China's Rise and the Future of Global Politics," Foreign Affairs 98: 93–94

2. Why do some states employ digital repression and not others?

Erica Frantz and Andrea Kendall–Taylor

Digital tools—namely the Internet, social media, and Artificial Intelligence (AI)—are supercharging government efforts to repress citizens and maintain political control. There are a variety of forms that such digital repression can take, ranging from simple tactics, such as Internet shutdowns, to more sophisticated techniques, such as disinformation campaigns to discredit opponents. Although the term digital repression is most often associated with notions of today´s increasingly savvy autocrats, governments of all stripes are deploying digital tools for repressive purposes. Indeed, the data show that both democracies and autocracies have increased their use of digital repression (Frantz, Kendall-Taylor, and Wright 2020). Digital repression is therefore a global phenomenon, as this book makes clear. Yet, what explains why some states use digital repression more than others? Though research in this field is nascent, here we explore the role of three factors: regime type, digital capacity, and levels of wealth. We also highlight how digital repression is making autocracies more durable, while raising the risks of democratic decay in new and/or weak democracies.

Regime type

Digital repression is in many ways like traditional repression. The goal of both is to increase the costs of disloyalty and to help leaders identify their opponents and restrict their ability to mobilize in ways that run counter to the government´s interests. Because authoritarian regimes repress more than their democratic counterparts, it is unsurprising that digital repression is higher in autocracies than democracies (Feldstein 2021). As of 2019, it was North Korea, Turkmenistan, Eritrea, and the People´s Republic of China (PRC) that relied most on digital repression (Frantz and Kendall-Taylor 2021). In fact, regime type is one of the strongest predictors of the

extent to which a government will use digital repression: as democracy levels increase, levels of digital repression decline.

Digital repression is a more attractive tool for autocratic governments than democratic ones because the former have fewer constraints on their ability to apply it and are less likely to face backlash for doing so. Consistent with this insight, Feldstein (2021) finds that as a country´s repression of civil liberties increases, so too does its use of digital repression. This suggests that governments are more likely to see digital repression as an attractive tactic when they expect to face limited public criticism or collective action against the government in response.

In addition to explaining differences in the level of digital repression across countries, regime type also sheds light on the types of digital repression that governments are most likely to use. Democracies (as of 2019) were most likely to rely on social media monitoring, followed by social media censorship, though their reliance on even these tools is far lower than in authoritarian regimes (Frantz and Kendall-Taylor 2021). Today´s democracies rely least on shutting down or filtering the Internet or social media than on other digital tools. Dictatorships (as of 2019) relied most on social media monitoring, followed by Internet filtering. They too relied least on shutting down the Internet or social media.

Digital Capacity

In theory, a state´s digital capacity should affect the extent of digital repression it uses. The People´s Republic of China (PRC), for example, is on the cutting edge of digital repression. The government has developed significant capacity to monitor, manipulate, and control its citizens through digital means. In the case of the PRC, high levels of digital capacity enable high levels of digital repression. Yet, digital capacity is not always a clear predictor of a government´s use of digital repression. Many governments excel at cyber security or content moderation, for example, but choose not to use such capacity to surveil citizens or track political opponents.

Conversely, some governments lack the ability to apply digital repression in a sophisticated fashion, and therefore opt to rely on rudimentary tactics instead, such as shutting down the Internet. Likely for these reasons, the data show that autocratic governments employ more digital repression, on average, than their levels of digital capacity would suggest, while the opposite is true of democracies (Frantz, Kendall-Taylor, and Wright 2020).

Importantly, less capable states can acquire more sophisticated tools, such as surveillance software, from more capable states. Indeed, the ability to import digital repression is one of the factors that sets this type of repression apart from its more traditional forms. In the past, cultivating an effective repressive apparatus with widespread boots-on-the-ground surveillance capacity entailed recruiting, training, and arming thousands of loyal cadres. With digital tools, however, this sort of extensive manpower is no longer necessary to surveil and monitor citizens. Governments can simply import the capacity to digitally repress by buying desired technologies and training a small number of individuals in how to use them. In the digital age, developing an effective repressive apparatus is no longer restricted to a handful of competent dictatorships, suggesting that the repressive capabilities of today´s authoritarians are likely to expand in the years to come.

Levels of wealth

Levels of wealth are another factor that helps explain a country´s reliance on digital repression, albeit only in democracies. The data show that as democracies grow richer, their use of digital repression declines (Frantz and Kendall-Taylor 2021). This is likely because wealthier democracies tend to have firmer mechanisms of accountability and more robust democratic institutions in place, lessening incidences of such repression.

In terms of digital capacity, levels of wealth are tightly linked to a country´s capacity for digital repression, regardless of whether it is authoritarian or democratic. This

suggests that in democracies, as states grow richer, they obtain greater digital capacity but use digital repression less. In dictatorships, however, wealth is associated with greater digital capacity but not with changes in reliance on digital repression. Future research is needed to better understand the ways in which changes in levels of development influence government decisions to adopt digital tools and use them for repressive purposes.

It is worth noting that a state's military spending is positively correlated with its use of AI-based surveillance systems (Feldstein, 2019a). Though this does not mean states with high military spending are using such systems for repression, among the fifty states with the highest military spending, 80 percent use AI-based surveillance technology.

The implications of digital repression

Digital repression serves numerous functions for the governments that deploy it. In addition to helping governments monitor and identify their opponents, new technologies allow governments to keep tabs on other government officials in ways that enable them to root out underperforming members that can reduce citizen dissatisfaction with government performance, gain greater information about ordinary citizens in ways that improve their ability to respond to and/or address sources of discontent before they escalate, and more effectively control and manipulate their information environments. Digital tools also blur the lines between cooptation and repression, enabling governments to fine-tune their use of reward and refusal in ways that encourage compliance with government objectives.

For these reasons, there is good reason to expect that digital repression will confer survival benefits for the governments that use it. More specifically, research on autocracies shows that digitally repressive autocrats face a lower risk of protests than those autocrats who rely less heavily on these tools (Frantz, Kendall-Taylor, and Wright 2020). Digital repression not only decreases the likelihood that a protest

will occur but also reduces the chances that a government will face large, sustained mobilization efforts, such as the ‘red shirt´ protests in Thailand in 2010 or the anti-Mubarak and antimilitary protests in Egypt in 2011.

Autocracies lower risk of protest may be a product of the fact that digital tools are supercharging traditional methods of control. In particular, dictatorships that increase their use of digital repression also tend to increase their use of violent forms of repression ‘in real life´, particularly torture and the killing of opponents (Frantz, Kendall-Taylor, and Wright, 2020). By providing dictatorships with more information about their opponents, digital repression enables regimes to use violence more precisely and efficiently. This is advantageous given the potential for indiscriminate government violence to trigger political backlash. In this way, digital repression allows autocracies to reap the benefits of repression while reducing the costs of doing so.

As autocracies have learned to finetune their use of digital tools, they have become a more formidable threat to democracy. Our research shows that that digital repression is making authoritarian regimes more durable (Frantz, Kendall-Taylor, and Wright 2020). Between 2000 and 2017, of the 91 dictatorships that had survived in power more than one year, 37 collapsed; those that avoided collapse had significantly higher levels of digital repression, on average, than those that fell.

Finally, although less is known about the implications of digital repression for democracies, there are indicators that it may be facilitating backsliding in environments where democracy is already fragile. New technologies are particularly dangerous for weak democracies because so many are dual use: technology can enhance government efficiency and provide the capacity to address challenges such as crime and terrorism, but—regardless of the intentions with which governments initially acquire such technology—it can also be used to muzzle and restrict the activities of political opponents. Greitens (2020), for example, shows that high crime rates are a key factors explaining which countries are most likely to adopt the PRC´s

digital tools. Whether these technologies are applied in ways that violate human rights depends on domestic factors and weak and/or fragile democracies have fewer constraints on the ability to repurpose these technologies for repressive purposes.

Conclusion

The strong relationship between regime type and levels of digital repression suggests that components of democracy—for example the strength of a country's legal system, courts, and civil society organizations that can shine light on government abuses—are key to mitigating the negative uses of digital tools. Future research is needed, however, to better understand the specific laws or legal frameworks that would effectively limit abuses, especially in new or fragile democracies that acquire digital tools for legitimate reasons such countering crime or terrorism. Likewise, the ease with which governments can import the capacity for digital repression underscores the importance of the United States and its democratic allies modernizing and expanding legislation to help ensure that democratic entities are not enabling digital human rights abuses. Though our understanding of why some countries digitally repress more than others is limited, this discussion highlights key areas that can already be pursued to reduce its spread.

Andrea Kendall-Taylor is a Senior Fellow and Director of the Transatlantic Security Program at the Center for a New American Security.

Erica Frantz is an Associate Professor of Political Science at Michigan State University. She is an expert on authoritarian politics, particularly themes related to democratization, backsliding, conflict, and development.

References

Feldstein, Steven. 2021. The Rise of Digital Repression How Technology Is Reshaping Power, Politics, and Resistance. Oxford: Oxford University Press USA – OSO

Frantz, Erica, and Andrea Kendall-Taylor. 2021. "Digitized Autocracy Literature Review: Final Report." DRG Center Working Paper, U.S. Agency for International Development. https://pdf.usaid.gov/pdf_docs/PA00XV9R.pdf

Frantz, Erica, Andrea Kendall-Taylor, and Joseph Wright. 2020. "Digital Repression in Autocracies Users Working Paper." V-DEM Institute. https://www.v-dem.net/media/publications/digital-repression17mar.pdf

Frenkel, Sheera. 2015. "These Two Companies Are Helping Governments Spy on Their Citizens." BuzzFeed News, August 24, 2015. https://bit.ly/2lQM5B8.

Greitens, Sheena Chestnut. 2020. "Dealing with Demand for China's Global Surveillance Exports." Brookings.edu. Brookings. https://www.brookings.edu/research/dealing-with-demand-for-chinas-global-surveillance-exports/

3. Is digital transnational repression "spreading" among states?

Marcus Michaelsen

The Iranian regime has gone to great lengths to silence Masih Alinejad. In summer 2022, a man armed with a loaded assault rifle was arrested outside Alinejad´s house in Brooklyn, New York. Together with two other members of an Eastern European criminal organization known for its ties to Iran, he had conspired to murder the outspoken Iranian-American women´s rights activist. Only a year earlier, US law enforcement agencies had broken up a plot to kidnap Alinejad and forcibly return her to Iran, where she likely would have faced execution after a show trial (Weiser and Thrush 2023). For the past decade, Alinejad´s relatives in Iran have been put under relentless pressure. Her brother was sentenced to eight years in prison and her sister forced to disown her on state television. Her parents have stopped talking to her, pressured and brainwashed by the regime (Alinejad 2018). Programmes on state television portrayed Alinejad alternately as a drug addict, a prostitute, rape victim, or foreign agent.

These attacks were prepared by and embedded in a barrage of digital threats. Ever since Masih Alinejad started the Facebook campaign 'My Stealthy Freedom´, in 2014, which collected photos and videos of Iranian women without the mandatory headscarf, she became a target for online harassment and other threats. "The day I post something on the page of the campaign, I will get 300 similar comments. 'Death to Masih Alinejad´, they write with different identities", she told me in an interview in 2015. "They also leave a lot of other insulting and vulgar comments. I don´t fear these threats, but they nevertheless leave an impression on my thoughts. It´s a lot of pressure." Around the same year, in one of the numerous digital attacks directed against Alinejad, Iranian regime agents hacked into the Facebook profile of a young relative in Tehran to reach out and trick her into revealing the passwords of her own accounts.

With her persistent campaigning against the compulsory dress code and other restrictions on women´s freedoms under the Islamic Republic, Masih Alinejad clearly became a thorn in the eye of the regime. When the "Woman, Life, Freedom" protests erupted inside Iran in September 2022, Alinejad seemed vindicated for having endured almost the entire range of known methods of transnational repression. Her case exemplifies how digital technologies have allowed diaspora activists to mobilize for and participate in political struggles in their country of origin. Yet, it also shows how authoritarian regimes use these same technologies to intimidate and threaten dissidents in exile.

As assertive autocratic rulers extend coercion across borders, digital threats are a key instrument in their toolkit. These regimes use surveillance, malware attacks, online harassment, defamation and disinformation campaigns to monitor, undermine and suppress activism in the diaspora (Michaelsen 2020b). Digital transnational repression enables state agents to reach far into foreign territories - and into the personal lives and political activities of targeted exiles (Al-Jizawi et al. 2022). Moreover, digital attacks are often closely connected to other methods of transnational repression which range from threats against home-country families to assassinations (Schenkkan and Linzer 2021).

The repertoire of digital transnational repression is as broad as the array of states using it. Governments in countries like Egypt, Iran and Vietnam are behind wide-ranging phishing campaigns that seek to infiltrate the communications of exiles. They use tailored messages to trick their targets into opening files compromised with malware, steal their credentials and expose domestic counterparts (Amnesty International 2018, 2021). Chinese agents regularly call members of the Uyghur diaspora via WhatsApp and other messengers from their parents´ home as a means of intimidation (Jardine and Hall 2021). The Azerbaijani regime has relied on coordinated inauthentic Facebook profiles to attack exiled journalists (Wong and Harding 2021). Many other governments, too, use paid trolls and artificial social

media accounts to shape online narratives and mute critical voices (Jones 2022; Monaco and Nyst 2018).

For campaigns of targeted surveillance, governments purchase sophisticated spyware on a thriving, but obscure market of surveillance technologies (Deibert 2022). The rulers of Saudi Arabia, the United Arab Emirates and Rwanda, among others, have used the notorious Pegasus spyware, sold by the Israeli NSO Group, to hack into the smartphones of opponents abroad (Marczak et al. 2018). The powerful tool infects digital devices without a single click, giving operatives access to phone calls, personal files, emails, chats and geolocation data. The gruesome murder of exiled journalist Jamal Khashoggi in the Saudi consulate in Istanbul was likely prepared by Pegasus infiltrations in his close circle, if not his own device (Office of the High Commissioner for Human Rights 2019).

Women activists and journalists are particularly exposed to threats that instrumentalize their gender to intimidate and discourage them from speaking out. Rape threats, misogynistic hate speech and harassment from regime actors are often picked up and amplified by loyal supporters. Intimate photos, fake or real, are dumped online to smear women´s reputation. In the Gulf region, for instance, such material was spread on social media, after the phones of several high-profile women journalists got infected with spyware (Solon 2021).

Given the central role of digital communication in all aspects of professional and personal life, digital transnational repression can have deep, and often disturbing impacts. The targets of social media harassment or intrusive surveillance operations report mental stress, paranoia and social isolation (Al-Jizawi et al. 2022). Uncertain about digital spying from regime agents, they reduce contacts to families and friends; for fear of a possible backlash, they engage in self-censorship (Michaelsen 2020a).

Spreading along the ties that link migrants to their homeland and exposing them, once again, to the arbitrary control of regime agents, digital transnational repression

clearly is a manifestation of globalizing authoritarianism. At the same time, the tools and practices of digital repression are also spreading from one country to another, in constellations of actors that stretch across democratic and autocratic, state and non-state divides (Glasius and Michaelsen 2018). Leading perpetrators, like China and Russia, export technology and know-how for pervasive surveillance and information controls (Weber 2019). Authoritarian states are learning from one another how to control social-media-fueled protests.

With the commodification of surveillance, data exploitation and influence operations, private companies cater to the needs of unaccountable and oppressive power holders. Oblivious to the vulnerabilities of users outside their main markets, big tech platforms often fail to provide appropriate protections and remedies to those targeted by digital repression. And finally, the securitization of digital space is also driven by the practices of Western democracies in anti-terror policies or migration controls (Bauman et al. 2014; Molnar 2020). Such entanglements need to be taken into account in any response to digital repression that seeks to defend civil society's continued ability to use digital tools to freely exchange, organize and mobilize.

Marcus Michaelsen is a Senior Researcher for the Citizen Lab in a project on gender-based digital transnational repression. His research encompasses digital technologies, human rights activism and authoritarian politics, whilst his ongoing work centres around digital transnational repression. Between December 2019 and February 2022, Michaelsen was a senior post-doctoral researcher in the Law, Science, Technology and Society (LSTS) research group at Vrije Universiteit Brussel.

References

Alinejad, Masih. 2018. "My Sister Disowned Me on State TV." The New York Times. 31 July 2018. https://www.nytimes.com/2018/07/31/opinion/iran-hijab-feminist.html

Al-Jizawi, Noura et al. 2022. "Psychological and Emotional War: Digital Transnational Repression in Canada". Citizen Lab. https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada

Amnesty International. 2018. "When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users." https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough

———. 2021. "Click and Bait: Vietnamese Human Rights Defenders Targeted with Spyware Attacks." https://www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-targeted-with-spyware-attacks

Bauman, Zygmunt et al. 2014. "After Snowden: Rethinking the Impact of Surveillance." International Political Sociology 8(2): 121–44

Deibert, Ronald J. 2022. "The Autocrat in Your IPhone." Foreign Affairs (January/February 2023). https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert

Glasius, Marlies, and Marcus Michaelsen. 2018. "Illiberal and Authoritarian Practices in the Digital Sphere." International Journal of Communication 12(0): 3795–3813

Jardine, Bradley, and Natalie Hall. 2021. "'Your Family Will Suffer'. How China Is Hacking, Surveilling, and Intimidating Uyghurs in Liberal Democracies." Uyghur Human Rights Project (UHRP) / Oxus Society for Central Asian Affairs. https://uhrp.org/report/your-family-will-suffer-how-china-is-hacking-surveilling-and-intimidating-uyghurs-in-liberal-democracies

Jones, Marc Owen. 2022. Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media. London: Hurst Publishers

Marczak, Bill et al. 2018. "HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." Citizen Lab. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries

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

———. 2020b. "The Digital Transnational Repression Toolkit, and Its Silencing Effects." Freedom House. https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects (November 12, 2021)

Molnar, Petra. 2020. "Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up." European Digital Rights (EDRi). https://edri.org/our-work/technological-testing-grounds-border-tech-is-experimenting-with-peoples-lives

Monaco, Nicolas, and Carly Nyst. 2018. "State-Sponsored Trolling. How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns." Institute for the Future. https://www.iftf.org/statesponsoredtrolling

Office of the High Commissioner for Human Rights. 2019. "Khashoggi Killing: UN Human Rights Expert Says Saudi Arabia Is Responsible for 'Premeditated Execution.'" https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24713.

Schenkkan, Nate, and Isabel Linzer. 2021. "Out of Sight, Not Out of Reach." Freedom House. https://freedomhouse.org/report/transnational-repression

Solon, Olivia. 2021. "'I Will Not Be Silenced': Women Targeted in Hack-and-Leak Attacks Speak out about Spyware." NBC News. 1 August 2021. https://www.nbcnews.com/tech/social-media/i-will-not-be-silenced-women-targeted-hack-leak-attacks-n1275540

Weber, Valentin. 2019. "The Worldwide Web of Chinese and Russian Information Controls." University of Oxford, Centre for Technology and Global Affairs

Weiser, Benjamin, and Glenn Thrush. 2023. "Justice Dept. Announces More Arrests in Plot to Kill Iranian Writer." The New York Times. 27 January 2023. https://www.nytimes.com/2023/01/27/us/politics/masih-alinejad-doj-assassination-plot.html

Wong, Julia Carrie, and Luke Harding. 2021. "'Facebook Isn't Interested in Countries like Ours': Azerbaijan Troll Network Returns Months after Ban." The Guardian. 13 April 2021. https://www.theguardian.com/technology/2021/apr/13/facebook-azerbaijan-ilham-aliyev

4. China's Role in Global Digital Repression

Xiao Qiang

Chinese Digital Authoritarianism

China is the largest and most powerful one-party state in human history, and it also has some of the most developed and sophisticated digital technologies in the world. It contributes to global digital repression through its domestic censorship and control of tech companies, exporting surveillance technologies and efforts to shape the international order and international rules.

The Chinese government uses digital technology, especially artificial intelligence, to establish a mass surveillance system in the country in the name of building a "safe society", "smart cities", and "smart policing". Government agencies use facial recognition, biometrics, surveillance cameras, and big data analytics to quickly profile and classify individuals, track activity, predict activity, and take preemptive action against any perceived threats to state power (Hillman and McCalpin 2019).

China's technology companies are among the world's largest and most innovative and can exert increasing levels of influence over industries and governments around the world. China's tech giants, whatever their ownership structure, are domestic monopolies that are tightly integrated with the Chinese Communist Party (CCP). Over 70% of private enterprises in China have party organizations and branches (Martina 2017). These companies also often pursue commercial interests that align with Chinese diplomatic goals.

Internationally, China has promoted the concept of "cyber sovereignty" to legitimize censorship, surveillance and localized control of data (Mok 2022). In the name of "cyber sovereignty," CCP has used the national "Cross-Border Data Security Gateway" (aka "Great Firewall") (Yang 2021) to massively block foreign social media

platforms that offer unfiltered services in China. Exclude foreign tech companies, including Google, Twitter, Facebook, etc; replace them with local versions of search (Baidu), entertainment (Tencent), e-commerce (Alibaba), social media (Weibo) and text messaging (WeChat). It provides a market platform for Chinese digital companies to compete unfairly against foreign tech companies (Shirk et al. 2016).

The Cyberspace Administration of China has continuously expanded the list of banned websites using strict cybersecurity laws. Companies must abide by stringent censorship regulations and need to conduct self-censorship to avoid government penalties. At the same time, all companies operating in China, including foreign companies, are required to store information, including personal data, in data centers or servers in China (Wagner 2017).

Exportation of Surveillance Technology

China has become a leading exporter of surveillance technology, including closed-circuit television (CCTV) systems, facial recognition technology, and data analytics software (Romaniuk and Burgers 2018). These technologies are being used by governments around the world to monitor their citizens, including countries with a history of human rights abuses. Chinese companies exported surveillance technology to at least 63 countries. (Feldstein 2019) Chinese security monitoring equipment companies Hikvision, Dahua, and Meiya Pico, all of which have close ties to the Chinese government, have expanded their databases and improved their systems due to overseas development.

China has formed alliances with other authoritarian regimes around the world, including Russia, Iran, and North Korea, to advance its digital repression efforts. For example, China and Russia have signed agreements to cooperate on the development of their respective digital monitoring and censorship systems and to share information on online censorship and surveillance (Tsydenova and Balmforth 2019). China regularly conducts large-scale training programs for foreign officials to

respond to public opinion, control civil society, and enforce Chinese-style internet surveillance policies. (Cook et al. 2022).

Investment in Digital Infrastructure

China has invested heavily in the development of digital infrastructure in other countries, including telecommunications networks and data centres. This has enabled the country to expand its influence and presence in the digital world, and to increase its ability to monitor and control online content in other countries.

In recent years, China has been aggressively promoting its "Digital Silk Road", which is the code name for fiber optic cables, mobile networks, satellite relay stations, data centres and smart cities built by global Chinese technology companies. This effort has accumulated more than $17 billion in loans and investments, including funding for global telecom networks, e-commerce, mobile payment systems, and big data projects. China has specifically courted North Africa and the Middle East as part of its technology push (Xiao 2021).

The International Cyber Policy Center of the Australian Strategic Policy Institute has created a public database (ASPI 2021) to map the global expansion of 12 major Chinese technology companies. The surveying map of the project shows that 12 Chinese high-tech companies are involved in: 75 "smart city" or "public safety solutions" projects, most of which are in Europe, South America and Africa; 52 5G plans, covering 34 countries; 56 submarine optical cables, 31 leased optical cables and 17 terrestrial optical cables; 202 data centres and 305 telecommunications and information communication technology (ICT) projects are spread all over the world. These infrastructure constructions not only bring huge economic opportunities for Chinese high-tech companies, but also provide opportunities for China to obtain huge overseas data, and even provide technical means for some illiberal regime to monitor their own people.

Influence on International Organizations

China has also been working to shape international norms and standards related to the regulation of the internet, including through international organizations such as the United Nations. Chinese diplomats, along with companies, have also been using their influence at the International Telecommunication Union (ITU) to advance their own interests in the digital economy. This includes promoting the adoption of Chinese-made technologies in developing countries, such as Huawei´s 5G equipment, and advocating for these technologies to be included in international standards (Ryugen and Akiyama 2020).

In recent years, China has become more and more aggressive in order to improve its influence in international technical standards. In 2021, the telecoms group Huawei, together with state-run companies China Unicom and China Telecom, and the country´s Ministry of Industry and Information Technology (MIIT), jointly proposed a new standard for core network technology called "New IP" at the UN´s International Telecommunication Union (ITU) (Gross and Murgia 2020). While the proposal claims to enable cutting-edge technologies such as holograms and self-driving cars, in reality, the proposal to reshape the internet also embeds digital repression into the very fabric that underpins the web. This enables the state to have far greater control over internet services than in the past.

Conclusion

Now the world is entering the era of artificial intelligence. This technology can be a force for good as a predictive tool, analytical tool, or automated decision-making tool; it can also be used for surveillance, censorship and information manipulation (Xiao 2019). The rise and global expansion of digital repression in China is reshaping the balance of power between democracies and autocracies. The international community must work together to address China´s digital repression and promote greater online freedom and privacy.

Xiao Qiang 强 is a Research Scientist at the School of Information and the Founder and Editor-in-Chief of China Digital Times, a bi-lingual China news website. A theoretical physicist by training, Xiao Qiang studied at the University of Science and Technology of China and entered the PhD program (1986-1989) in Astrophysics at the University of Notre Dame. He became a full time human rights activist after the Tiananmen Massacre in 1989. Xiao was the Executive Director of the New York-based NGO Human Rights in China from 1991 to 2002. Since 2003, Xiao has taught classes Digital Activism, Internet Freedom and Blogging in China at both the School of Information and the Graduate School of Journalism, University of California at Berkeley. His current research focuses on state censorship, propaganda and disinformation, as well as emerging AI-driven mass surveillance and social control in China.

Xiao is a recipient of the MacArthur Fellowship in 2001. In January 2015, Xiao was named to Foreign Policy magazine's Pacific Power Index, a list of "50 people shaping the future of the U.S.-China relationship." He was named on the list "for taking on China's Great Firewall of censorship."

References

ASPI's International Cyber Policy Centre. 2021. "Mapping China's Tech Giants." ASPI's International Cyber Policy Centre. June 2021. https://chinatechmap.aspi.org.au/#/homepage

Cook, Sarah, Angeli Datt, Ellie Young, and BC Han. 2022. "BEIJING'S GLOBAL MEDIA INFLUENCE - Authoritarian Expansion and the Power of Democratic Resilience." https://freedomhouse.org/sites/default/files/2022-09/BGMI_final_digital_090722.pdf

Feldstein, Steven. 2019. "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Gross, Anna, and Madhumita Murgia. 2020. "China and Huawei Propose Reinvention of the Internet." Www.ft.com, March 27, 2020. https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2

Hillman, Jonathan, and Maesea Mccalpin. 2019. "Watching Huawei's 'Safe Cities' Middle East Program." CSIS Briefs. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030_HillmanMcCalpin_HuaweiSafeCity_layout_v4.pdf

Martina, Michael. 2017. "Exclusive: In China, the Party's Push for Influence inside Foreign Firms Stirs Fears." U.S., August 24, 2017. https://www.reuters.com/article/us-china-congress-companies/exclusive-in-china-the-partys-push-for-influence-inside-foreign-firms-stirs-fears-idUSKCN1B40JU

Mok, Charles. 2022. "China and Russia Want to Rule the Global Internet." The Diplomat, February 22, 2022. https://thediplomat.com/2022/02/china-and-russia-want-to-rule-the-global-internet/

Romaniuk, Scott N., and Tobias Burgers. 2018. "How China's AI Technology Exports Are Seeding Surveillance Societies Globally." The Diplomat, October 18, 2018. https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/

Ryugen, Hideaki, and Hiroyuki Akiyama. 2020. "China Leads the Way on Global Standards for 5G and Beyon." Financial Times, August 4, 2020. https://www.ft.com/content/858d81bd-c42c-404d-b30d-0be32a097f1c

Shirk, Susan, Bethany Allen-Ebrahimian, and Emily Parker. 2016. "It's Official: Washington Thinks Chinese Internet Censorship Is a 'Trade Barrier.'" Foreign Policy, April 14, 2016. https://foreignpolicy.com/2016/04/14/chinese-censorship-trade-barrier-great-firewall-ustr-business-trade-internet/

Tsydenova, Nadezhda, and Tom Balmforth. 2019. "Russia and China to Sign Treaty on Combating Illegal Online Content." Reuters, October 8, 2019, sec. Internet News. https://www.reuters.com/article/us-russia-china-internet/russia-and-china-to-sign-treaty-on-combating-illegal-online-content-idUSKBN1WN1E7

Wagner, Jack. 2017. "China's Cybersecurity Law: What You Need to Know." The Diplomat, June 2017. https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

Xiao, Qiang. 2019. "The Road to Digital Unfreedom: President Xi's Surveillance State." Journal of Democracy, January. https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/

———. 2021. "Chinese Digital Authoritarianism and Its Global Impact." Project on Middle East Political Science (POEMPS). August 4, 2021. https://pomeps.org/chinese-digital-authoritarianism-and-its-global-impact

Yang, Zeyi. 2021. "China's Cyber Regulation Acknowledges the Great Firewall - Protocol." Protocol. November 18, 2021. https://www.protocol.com/china/vpns-out-new-cyber-regulation

5. From the Unwitting to the Unscrupulous: Private Sector Complicity in Digital Repression

Adrian Shahbaz

Technology companies have extended states′ capacity for digital repression. Around the world, governments have developed methods for coopting and even coercing internet firms into complying with abusive policies. Authorities have also procured new surveillance technologies from firms that have too often displayed disregard for business and human rights principles. This chapter outlines how different industry players range from unwitting to unscrupulous agents of state repression.

Authoritarian intermediaries

Governments, led by the United States, had long pursued a laissez-faire approach to regulating the internet. However, driven by real and perceived online harms and, in some cases, a desire for regime control, an increasing number of states have passed legislation that imposes requirements on telecommunication firms, social media companies, and other internet intermediaries (Shahbaz and Funk 2021). Cybercrime, data protection, and antiterrorism laws can be controversial in democratic contexts; in autocracies, similar provisions are regularly used to pressure companies into compliance with human rights violations.

Telecommunications companies and internet service providers (ISPs) consistently face demands to censor nonviolent political, social, and religious content, including independent journalism or materials related to marginalized populations. Most countries also require firms to retain data about their users, share it with law enforcement, and allow for lawful interception of electronic communications or to monitor their users. A 2009 cybercrime law obliges ISPs in Iran to filter thousands of nonviolent political, social, and religious websites that threaten the Islamic regime. Authorities have banned major foreign social media and communication platforms that have been crucial to documenting violence against nonviolent protesters

(Alterman and Alimardani 2022). In Myanmar, the military ordered ISPs to shut down internet service entirely during a 2021 coup. Largescale crackdowns on freedom of expression and access to information, combined with rising pressure to cooperate with surveillance agencies, led the Norwegian ISP Telenor to exit the market in the following year (Dunant 2022).

Search engines, social media, app stores, and other digital platforms routinely come under pressure to remove content. The Turkish government banned access to Twitter in 2014 for refusing to take down accounts and tweets that allegedly violated local laws, including "an account accusing a former minister of corruption". Although Twitter successfully challenged the ban in court, the company has faced numerous bans and ultimately resorted to restricting posts for users based within the country (Ozbilgin and Coskun 2014; Gadde 2014). Vietnamese authorities used a similar tactic to coerce Facebook to take down anti-government posts in 2020. (Pearson 2020) Like ISPs, platforms receive requests from courts and executive agencies to hand over user data. Requests to platforms have expanded dramatically over the years; Google's transparency report noted an increase from 27,625 requests in 2010 to 174,569 in only the first half of 2022 (Google 2022).

Compliance with an illegitimate request can bring devastating consequences. For example, Yahoo cooperated with Chinese authorities in 2004 to identify a local journalist who used an anonymous email address to contact overseas human rights groups, leading to his imprisonment on a 10-year term (The New York Times 2007). Over the years, many multinational companies have closed their China-based operations as the country has ramped up its regulatory pressure against technology firms (Lin 2021). Their exit may leave space for firms with a more dubious commitment to human rights. A Wall Street Journal investigation found that employees at Huawei, a Chinese telecommunications firm, assisted Ugandan and Zambian authorities to repress local opposition figures and journalists (Parkinson et al. 2019)

Merchants of digital repression

While internet intermediaries can be complicit in rights violations in the course of offering information and communication services, surveillance companies play a more direct role in enabling state repression. States have long outsourced security and even military operations to the private sector. Today´s merchants of digital repression primarily market their products to law enforcement and intelligence agencies, as well as a variety of state and commercial actors. Two industries – facial recognition technology (FRT) and spyware – have particularly alarming consequences for human rights in the digital age.

FRT systems analyze video and images against a database of photos to identify people in real-time or asynchronously. While inconsistencies in the technology can compound existing discrimination and lead to mistaken arrests, as it has in the United States, the effectiveness of FRT also presents a significant danger (Hill 2020). For example, police in Moscow used FRT to detain several activists and journalists in June 2022 because they were deemed to constitute "potential protesters". (Current Time 2022). In 2011, members of the persecuted Falun Gong group sued Cisco, a US-based multinational, for allegedly facilitating human rights abuses after the leak of an internal corporate presentation regarding possible projects in Beijing (Reitman 2011). More recently, the US government condemned Hikvision, a Chinese company, for enabling mass repression and serious human rights violations against the Uyghur and other minority populations in the Xinjiang region of China (Bateman 2022).

Several spyware companies have come under scrutiny for their dubious ethical practices and, in some cases, alleged unlawful practices. For over a decade, Citizen Lab and other groups have documented abuse by purveyors of targeted interception technology. Hacking Team, an Italian firm, claimed to have a system for vetting clients and restricting their use of the company´s spyware products if found to engaging in human rights violations. Nonetheless, investigative researchers found the company´s imprints on the devices of journalists and political activists in over 20

countries, and a leaked client list revealed contracts with the security agencies of several autocratic regimes, including Egypt, Saudi Arabia, and Sudan (Kopfstein 2014; Greenberg 2015).

The scrutiny has resulted in limited accountability. One bombshell investigation found a list of over 50,000 phone numbers believed to have been targeted by Pegasus, a product of the Israel-based NSO Group (Kirchgaessner et al. 2021). Researchers have identified at least 180 journalists in the database (Rueckert 2021). In 2021, the US Commerce Department added the NSO Group and three Israeli, Russian, and Singaporean companies to a blacklist in response to their "malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad" (U.S. Department of Commerce 2021). Nonetheless, countless spyware firms remain in operation around the globe, and few governments have regulations in place that limit their use by law enforcement and security services (Mazzetti et al. 2022)

Addressing supply and demand

The private sector is a crucial intermediary between states and citizens in the 21st century. In line with the United Nations Guiding Principles on Business and Human Rights, technology companies should evaluate and mitigate any human rights risks related to their business, particularly when operating in countries that lack the rule of law and respect for human rights. Firms should develop internal processes for pushing back against illegitimate government requests and map out scenarios in which they would decide to exit problematic markets entirely (Arun 2022). Researchers and investigative reporters play a powerful role in raising awareness of companies' errant practices, and policymakers should respond with legislation that constrains opportunities for abuse by both the private sector and state agencies. Ultimately, the best defense against digital repression remains robust democratic institutions.

Adrian Shahbaz is vice president for research and analysis at Freedom House. He oversees the organization's portfolio of annual publications and special reports, including Freedom in the World, Freedom on the Net and Nations in Transit, as well as new streams of work on transnational repression, Beijing's global media influence, and election integrity in the digital age. Adrian previously served as Freedom House's director for technology and democracy and has authored or coauthored several internet freedom analyses, including Countering an Authoritarian Overhaul of the Internet (2022), The Global Drive to Control Big Tech (2021), The Pandemic's Digital Shadow (2020), The Crisis of Social Media (2019), and The Rise of Digital Authoritarianism (2018). Prior to joining Freedom House, he worked as a researcher at the UN Department of Political Affairs, the European Parliament, and the Organization for Security and Co-operation in Europe (OSCE). He holds a master's degree from the London School of Economics.

References

Alterman, Jon B. and Mahsa Alimardani. 2022. "Protest, Social Media, and Censorship in Iran." Center for Strategic and International Studies. 18 October, 2022. https://www.csis.org/analysis/protest-social-media-and-censorship-iran

Arun, Chinmayi. 2022. "The Exit Option." Centre for International Governance Innovation. 13 June, 2022. https://www.cigionline.org/articles/the-exit-option/

Bateman, Jon. 2022. "U.S. Sanctions on Hikvision Would Dangerously Escalate China Tech Tensions." Carnegie Endowment for International Peace. May 6, 2022. https://carnegieendowment.org/2022/05/06/u.s.-sanctions-on-hikvision-would-dangerously-escalate-china-tech-tensions-pub-87089

Current Time. 2022. "Dozens arrested in Moscow via facial-recognition system on Russia Day." RFE/RL. 13 June, 2022. https://www.rferl.org/a/moscow-police-detain-dozens-using-facial-recognition-system/31896070.html

Dunant, Ben. 2022. "Companies Quitting Myanmar Provide Hollow Victories Against Junta." Foreign Policy. 27 September, 2022. https://foreignpolicy.com/2022/09/27/western-companies-leaving-myanmar-totalenergies-telenor-human-rights/

Gadde, Vijaya. 2014. "Challenging the access ban in Turkey." Twitter Blog. 26 March 2014. https://blog.twitter.com/en_us/a/2014/challenging-the-access-ban-in-turkey.
Google. 2022. "Global requests for user information." Google Transparency Report. https://transparencyreport.google.com/user-data/overview?hl=en.

Greenberg, Andy. 2015. "Hacking Team breach shows a global spying firm run amok." WIRED. 6 July, 2015. https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/

Harwell, Drew. 2022. "Clearview AI to stop selling facial recognition tool to private firms." The Washington Post. 9 May, 2022. https://www.washingtonpost.com/technology/2022/05/09/clearview-illinois-court-settlement/

Hill, Kashmir. 2020. "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match." The New York Times. 29 December, 2020. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

Kirchgaessner, Stephanie, Paul Lewis, David Pegg, Nina Lakhani, and Michael Safi. 2021. "Revealed: leak uncovers global cyber-surveillance." The Guardian. 18 July, 2021. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Kopfstein, Janus. 2014. "Hackers without borders." The New Yorker. 10 March, 2014. https://www.newyorker.com/tech/annals-of-technology/hackers-without-borders

Lin, Liza. 2021. "Yahoo Pulls Out of China, Ending Tumultuous Two-Decade Relationship." The Wall Street Journal. 2 November, 2021. https://www.wsj.com/articles/yahoo-pulls-out-of-china-ending-tumultuous-two-decade-relationship-11635848926

Mazzetti, Mark, Ronen Bergman, and Matina Stevis-Gridneff. 2022. "How the Global Spyware Industry Spiraled Out of Control." The New York Times. 8 December, 2022. https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html

Ozbilgin, Ozge and Orhan Coskun. 2014. "Turkey lifts Twitter ban after court ruling." Reuters. 3 April, 2014. https://www.reuters.com/article/us-turkey-twitter/turkey-lifts-twitter-ban-after-court-ruling-idUSBREA320E120140403

Parkinson, Joe, Nicholas Bariyo, and Josh Chin. 2019. "Huawei Technicians Helped African Governments Spy on Political Opponents." The Wall Street Journal. 15 August, 2019. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

Pearson, James. 2020. "Exclusive: Facebook agreed to censor posts after Vietnam slowed traffic – sources." Reuters. 21 April, 2020. https://www.reuters.com/article/us-vietnam-facebook-exclusive/exclusive-facebook-agreed-to-censor-posts-after-vietnam-slowed-traffic-sources-idUSKCN2232JX

Reitman, Rainey. 2011. "Cisco and abuses of human rights in China: part 1." Electronic Frontier Foundation. 22 August, 2011. https://www.eff.org/deeplinks/2011/08/cisco-and-abuses-human-rights-china-part-1

Rueckert, Phineas. 2021. "Pegasus: The new global weapon for silencing journalists." Forbidden Stories. 18 July, 2021. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

Shahbaz, Adrian and Allie Funk. 2021. "The Global Drive to Control Big Tech." Freedom on the Net 2021. Freedom House. https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech

The New York Times, 2007. "Yahoo chief apologizes to Chinese dissidents' relatives." The New York Times. 7 November 7, 2007. https://www.nytimes.com/2007/11/07/business/worldbusiness/07iht-yahoo.1.8226586.html

U.S. Department of Commerce. "Commerce adds NSO group and other foreign companies to entity list for malicious cyber activities." 3 November, 2021. https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

6. When democracies employ repressive technology, what are the repercussions?

Jessica Brandt

Anti-democratic leaders employ repressive technologies to tighten their grip on power at home, silence critics beyond their borders, and interfere in democratic states and institutions abroad, with damaging consequences for the rights of millions of people worldwide (Brandt 2022b). But authoritarian governments are not alone in harnessing digital technologies to accomplish their objectives. Democratic governments have used facial recognition systems, biometric identification and predictive policing for law enforcement purposes. They have also used them for national security purposes, to monitor potential threats. Some have used commercial spyware to achieve political aims -- targeting journalists, activists, opposition politicians, government officials and business executives.

When democracies employ repressive technologies, they undermine the civil and human rights of the individuals and communities they target. They weaken the rule of law. By silencing journalists and opposition leaders, they damage the vibrant and open information environment on which democracy depends. In using repressive technologies, democratic governments undermine the credibility of their institutions and of democratic systems more broadly, making it easier for authoritarian governments to advance critiques rooted in "whataboutism", the practice of responding to an accusation by making a counteraccusation or raising a different issue (Merriam-Webster n.d.). They also make it harder for democratic governments to push back on authoritarian uses of repressive technologies – against their own citizens, and against diaspora populations living within democratic societies. In short, when democracies employ repressive technology, they become less democratic themselves and worsen their position in the emerging geopolitical competition between democracies and their authoritarian challengers.

The state of play

Much has been written about uses of digital technology by autocrats to surveil, repress, and manipulate domestic and foreign populations, often for the purposes of consolidating power or undermining challenges to their legitimacy (Polyakova and Meserole 2022; Brandt 2022b). Although they do so less frequently, given normative and institutional constraints, democracies have employed repressive technologies too – sometimes for law enforcement or national security purposes; others to preserve their grip on power (Feldstein 2023). In Greece, for example, intelligence services appear to have used spyware to monitor an opposition leader, investigative journalists, and a foreign national working for a global corporation (Markham and Emmanouilidou 2022; Stevis-gridneff 2023). In Indonesia, police may have used commercial spyware to persecute LGBTQ communities and religious minorities (Feldstein 2023; Yaron 2020). In Mexico, dozens of lawyers, human rights defenders, opposition politicians, anti-corruption advocates, and investigative journalists have been targeted by spyware sold to that country´s government (Ahmed and Perlroth 2017; Kirchgaessner 2022; Sheridan 2021). These are far from the only cases: at least 27 other democratic governments worldwide have acquired commercial spyware tools (Feldstein 2023). Meanwhile, law enforcement agencies in at least eleven European countries are using biometric recognition systems for investigations (Ragazzi et al., 2021).

Democratic societies have also been responsible for the spread of repressive technology to abusive regimes around the world. Oracle, a U.S.-based company, has partnered with purveyors of technology used to build China´s Orwellian surveillance state (Hvistendahl 2021). Equipment sold by Sandvine, a Canadian firm, has been used to censor the internet in Azerbaijan, Belarus, Egypt and Jordan (Gallagher 2020). France´s Nexa Technologies sold spyware to Egypt and Libya that was implicated in the torture of dissidents, among other human rights abuses (O'Neill 2021). Israel, by far the leading exporter of commercial spyware and digital forensic tools, approves export licenses for their sales (Priest et al., 2021; Feldstein and Kot 2023). So, while the conventional wisdom is that China is predominantly responsible

for providing repressive technology to autocrats around the world, Beijing is far from the only player to do so (Feldstein 2021).

The repercussions

Weaker Democracy at Home

When democracies deploy repressive technologies, they undermine the civil and political rights of their targets, including the rights to freedom of speech, association, and assembly. They also undermine the democratic character of their societies. As a study commissioned by the European Parliament put it:

Political participation is affected by spyware in that spied-on citizens can be intimidated into abstaining from engaging in interactions having political content, from sincerely expressing their views, and from associating with others for political purposes. This affects the quality of a democratic public sphere, which ultimately relies on the citizens´ inputs and reactions (Sartor and Loreggia 2022).

This is especially important because spyware targets – often journalists, opposition politicians, and activists – tend to occupy important space in a free society because of the role they play in enabling the political participation of others (Sartor and Loreggia 2022). Moreover, by silencing critics – whether journalists or opposition leaders – through the use of these technologies, governments undermine the freedom and openness of the information environment that are essential for democracy to thrive. Democracy ultimately depends on the idea that the truth is knowable, and that citizens can pursue it, share it, and use it to govern themselves (Brandt 2022a). To the extent that it abridges rights to privacy, expression, association and due process, the use of repressive technologies by democratic governments can also undermine the rule of law (American Bar Association 2022). Finally, the use of these technologies can also undermine the electoral process directly if hacked information is weaponized against opposition candidates, or if the

fear of being targeted leads individuals not to seek office or not to participate in political campaigns (Sartor and Loreggia 2022).

Diminished Credibility and Influence

By using repressive technology, democratic governments undermine the credibility of their institutions, which aspire to adhere to liberal principles. Especially given their considerable soft power and the moral authority that comes with their aspiration to liberal principles, democracies will model for governments everywhere how digital technology may be used. Their failure to live up to those principles could legitimate abusive uses of digital tools, with consequences for the rights and freedoms of millions of people around the world.

The use of repressive technology by democratic governments also makes it easier for autocrats to use "whataboutism" to dent democracy's appeal to would be-activists at home and to diminish the soft power of democratic governments. For example, China regularly casts the United States and its European partners and allies as hypocritical in their support for political freedoms and coopts the language of liberalism to position its own governance model as a "whole process democracy" (Brandt 2022a). Russia too disseminates a steady stream of propaganda content painting the Western governments as hypocritical, drawing on places where they have fallen short of their ideas (Brandt 2022a). This leaves democratic societies less-well positioned to face the emerging geopolitical competition between democracies and their authoritarian challengers – both in the information domain and beyond it. That is because the global prestige and attraction of open systems is a critical asymmetric advantage of democracies in that contest (Brandt et al., 2020).

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.

References

Ahmed, A., & Perlroth, N. 2017. Using texts as lures, government spyware targets Mexican journalists and their families. The New York Times. https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

American Bar Association. 2022. Panel warns of spyware threats to human rights, rule of law. American Bar Association. https://www.americanbar.org/news/abanews/aba-news-archives/2022/08/panel-warns-of-spyware-threats/

Brandt, J. 2022a. Autocratic Approaches to Information Manipulation: A Comparative Case Study. AidData at William & Mary. https://www.aiddata.org/publications/autocratic-approaches-to-information-manipulation-a-comparative-case-study

Brandt, J. 2022b Digital Authoritarianism: Pathways, Trends, Solutions. Montreal Institute for Genocide and Human Rights Studies. https://www.concordia.ca/content/dam/artsci/research/migs/docs/DigitalAuth/MIGSReportDigitalAuthoritarianism_2022_Aug.pdf

Brandt, J., Cooper, Z., Hanlon, B., & Rosenberger, L. 2020. Linking Values and Strategy: How Democracies Can Offset Autocratic Advances. Alliance For Securing Democracy. https://securingdemocracy.gmfus.org/linking-values-and-strategy/

Feldstein, S. 2023. Global inventory of commercial spyware & digital forensics. Mendeley Data. https://data.mendeley.com/datasets/csvhpkt8tm/10

Feldstein, S. 2021. Governments Are Using Spyware on Citizens. Can They Be stopped? Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019

Feldstein, S., & Kot, B. 2023. Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf

Gallagher, R. 2020. Sandvine technology used to censor web in more than a dozen nations. Bloomberg. https://www.bloomberg.com/news/articles/2020-10-08/sandvine-s-tools-used-for-web-censoring-in-more-than-a-dozen-nations#xj4y7vzkg

Hvistendahl, M. 2021. How a Chinese surveillance broker became Oracle's "Partner of the year". The Intercept. https://theintercept.com/2021/04/22/oracle-digital-china-resellers-brokers-surveillance/

Kirchgaessner, S. 2022. Mexico: Reporters and activists hacked with NSO spyware despite assurances. The Guardian. https://www.theguardian.com/world/2022/oct/04/mexico-nso-spyware-journalists-human-rights-hacked-pegasus

Markham, L., & Emmanouilidou, L. 2022. How free is the press in the birthplace of democracy? The New York Times. https://www.nytimes.com/2022/11/26/business/greece-journalists-surveillance-predator.html

Merriam-Webster. n.d. What is ‟whataboutism″?, Merriam-Webster.com dictionary. https://www.merriam-webster.com/words-at-play/whataboutism-origin-meaning

O'Neill, P. H. 2021. French spyware bosses indicted for their role in the torture of dissidents. MIT Technology Review. https://www.technologyreview.com/2021/06/22/1026777/france-spyware-amesys-nexa-crimes-against-humanity-libya-egypt/

Polyakova, A., & Meserole, C. 2022. Exporting Digital authoritarianism. Brookings Institution. https://www.brookings.edu/research/exporting-digital-authoritarianism/

Priest, D., Timberg, C., & Mekhennet, S. 2021. Private Israeli spyware used to hack cellphones of journalists, activists worldwide. The Washington Post. https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=lk_inline_manual_3

Ragazzi, F., Kuskonmaz, M. E., Plajas, Z. I., Ven, V. R., & Wagner, B. 2021. Biometric & Behavioural Mass Surveillance in EU Member States. The Greens/EFA in the European Parliament. http://extranet.greens-efa.eu/public/media/file/1/7297

Sartor, G., & Loreggia, A. 2022. The impact of Pegasus on fundamental rights and democratic processes. Study requested by the PEGA Committee. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740514/IPOL_STU(2022)740514_EN.pdf

Sheridan, M. B. 2021. How Mexico's traditional political espionage went high-tech. The Washington Post. https://www.washingtonpost.com/world/2021/07/21/mexico-nso-pegasus/

Stevis-gridneff, M. 2023. Meta manager was hacked with spyware and wiretapped in Greece. The New York Times. https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html

Yaron, O. 2020. Israel's Cellebrite sold phone-hacking tech to Indonesia. Haaretz. https://www.haaretz.com/israel-news/tech-news/2020-11-02/ty-article/.highlight/hacking-grindr-israels-cellebrite-sold-phone-spy-tech-to-indonesia/0000017f-db25-db22-a17f-ffb5bd550000

7. Do digital technologies benefit governments or empower civil society actors?

Anita R. Gohdes

Digital technologies are profoundly impacting state-society relations, and we are only slowly beginning to understand how far-reaching the implications are. The Internet has upended traditional media, has massively expanded the availability of information for those who have access to it, and has introduced new forms of communication and coordination. Trying to assess the Internet´s impact has remained an exceedingly difficult task for researchers, not least because it is a moving target: online spaces and the power asymmetries they produce are forever changing (Munger 2019).

Despite the difficulties of assessing the role of digital technologies at a societal level it is useful to take stock of the present status of things. I contend that presently, digital technologies are, on average, tipping the balance of power towards repressive states, when compared to the benefits they provide for civil society. It is not that digital technologies do not bring tangible benefits to civil society, but that state actors are currently able to weaponize digital technologies in ways that directly and forcefully undermine the work of human rights defenders, independent journalists, and marginalized communities.

Information and communication technologies have brought with them a range of tools that allow civil society to more effectively reach their constituents, to build cross-national and cross-sectoral coalitions, and to coordinate protests and humanitarian relief efforts. They also provide access to information for citizens who were previously constrained to consuming state-controlled media outlets. Public, semi-public and closed online spaces all enable new forums for marginalized groups, including LGBTQ+ people, racialized minorities, and for other members of society who traditionally do not have safe access to public spaces in the offline world. During the COVID-19 pandemic, digital technologies were crucial for the continuation of

routine activities (such as school), and in the aftermath of the recent Earthquake in Turkey and Syria social media apps helped coordinate relief and rescue efforts efficiently.

Notwithstanding the just mentioned benefits for civil society, I argue that governments currently have the upper hand in controlling digital technologies. I distinguish between three spheres of control: Governments can constrain civil society online activity by passing laws and regulations aimed at criminalizing online speech, by weaponizing their domestic digital infrastructure, and by manipulating online spaces.

Criminalizing online content

In response to growing concerns about online mis- and disinformation, governments across the world have instituted a variety of laws targeting both content creators and content hosts, aimed at holding them accountable for content deemed to be misinformation. States´ abilities to change laws and regulations of online spaces provide them with an advantage vis-à-vis civil society actors, in that it opens up the possibility sanctioning unwanted civil society content under the guise of non-compliance with the law (Morgenbesser 2020). Where policies to regulate online speech the law have been kept deliberately vague they have provided significant leeway for enforcement authorities to interpret the policies in political ways, for example by targeting content posted by minorities and opposition movements. Legal measures aimed at regulating online content in countries with non-democratic institutions are particularly prone to being instrumentalized for political purposes, and can also have a chilling effect on users´ willingness to engage online if they are unsure of what content is permissible, and what content is not (Parks and Thomson 2020).

Weaponizing digital infrastructure

Beyond legal means, governments in most countries yield significant power over their digital infrastructure, which facilitates the implementation of digital censorship and surveillance technologies. The non-profit organization Access Now reported that in

2021 there were 182 intentional disruptions of the Internet occurred in 34 countries across that world, considerably higher than the 159 recorded instances in the year before. Censorship technologies allow authorities to control online spaces in ways that can significantly affect the ability of civil society actors to operate effectively. For instance, a number of countries systematically block access to websites that host LGBTQ+ content (OutRight Action International et al. 2021). Censorship also occurs at the content-level, which is common in countries that have substantial control over the domestically popular social media platforms (Pan 2017). Outside of regular politics, shutting down digital infrastructure has been used as part of concerted military efforts aimed at crushing the opposition, and has been linked to an increase in indiscriminate violence (Gohdes, forthcoming). During mass protests in Iran in 2019 the Iranian authorities shut down the Internet and employed lethal repression, systematic intimidation, and threatened the relatives of victims to not talk about their experiences once the Net was restored.

Governments can furthermore weaponize digital infrastructure through online surveillance (Xu, 2021). Mass analysis of metadata and social media content can help obtain information on current and future trouble-makers, and information gleaned from such sources as well from text messages and phone calls has been used to detain civil society members in countries such as Iran, Ethiopia, and Syria. Online surveillance can expand and enrich intelligence gathering activities of governments, thereby expanding access into previously hard to reach sectors of society (Gohdes, forthcoming). The targeted employment of malicious spying software has gained increasing popularity among nation-states. The Citizen Lab published a report in 2018 that documents spyware operations in 45 different countries, underlining the global breadth of surveillance activities (Marczak et al. 2018).

Manipulating the information environment

The third way in which governments benefit from digital technologies is through the manipulation of online spaces. While civil society actors can and do engage in the manipulation of online media, evidence is accumulating on state and state-affiliated actors´ online engagement. Due to their unrivaled access to the financial and human resources needed for the successful implementation of mass online manipulation, states have become extraordinarily successful at exploiting the design and politics of social media sites. Research on China has found that state-affiliated accounts strategically flood social media with pro-government content, aimed at drowning out other voices (Roberts 2018). In the Philippines, the United States, and Turkey, among others, researchers have documented coordinated online harassment against civil society members (Nyst and Monaco 2018). Strategic multi-platform campaigns that combine different facets of media manipulation have been traced back to actors close to the Saudi government (Jones 2022).

While I have focused my arguments here on repressive states, the implications are also relevant for liberal democracies that traditionally engage in lower levels of violent coercion. As Hegghammer (2021) notes in his analysis of the technological controls that were put in place in many liberal countries across the world as part of the War on Terror: ‘the rise of states immune to rebellion is not a good thing. It is naive to think that states´ new powers will be used only against people plotting bomb attacks´.

Conclusion

States´ ability to criminalize civil society content, weaponize digital infrastructure, and manipulate the information space means that the Internet currently provides more benefits to repressive states than it does to civil society. That is not to say that digital technologies can and do not empower civil society across the world. The mere fact that repressive governments perceive unmediated access to the Internet under their jurisdiction as so problematic that they invest heavily in controlling, censoring, and manipulating it suggests that unchecked digital technologies are seen as an

existential threat to state power. Protecting and strengthening online spaces for civil society is now more important than ever.

Anita R. Gohdes is Professor of International and Cyber Security at the Hertie School in Berlin. She works at the intersection of international security and technology, and is the author of the forthcoming book titled Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence.

References

Access Now. 2022. "The Return of Digital Authoritarianism: Internet Shutdowns in 2021." https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf

Gohdes, Anita. n.d. Repression in the Digital Age: Censorship, Surveillance, and the Dynamics of State Violence. Oxford University Press

Gohdes, Anita R. 2020. "Repression Technology: Internet Accessibility and State Violence." American Journal of Political Science 64 (3). https://doi.org/10.1111/ajps.12509

Hegghammer, Thomas. 2022. "Resistance Is Futile." Foreign Affairs, April 13, 2022. https://www.foreignaffairs.com/articles/middle-east/2021-08-24/resistance-futile

Jones, Mark Owen. 2022. *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media*. London: Hurst.

Marczak, Bill, John Scott-Railton, Sarah Mckune, Abdul Razzak, and Ron Deibert. 2019. "The Citizen Lab Report on Pegasus Spyware." Nsarchive.gwu.edu. Citizen

Lab. https://nsarchive.gwu.edu/document/27613-6-citizen-lab-report-pegasus-spyware

Morgenbesser, Lee. 2020. "The Menu of Autocratic Innovation." Democratization 27 (6): 1053–72. https://www.academia.edu/42339404/The_Menu_of_Autocratic_Innovation

Munger, Kevin. 2019. "The Limited Value of Non-Replicable Field Experiments in Contexts with Low Temporal Validity." Social Media + Society 5 (3): 205630511985929. https://doi.org/10.1177/2056305119859294

Nyst, Carly, and Nick Monaco. 2018. "State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns." Institute for the Future. https://legacy.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf

OutRight Action International, Citizen Lab, and OONI. 2021. "No Access: LGBTIQ Website Censorship in Six Countries." Citizenlab.ca. Citizen Lab. https://citizenlab.ca/2021/08/no-access-lgbtiq-website-censorship-in-six-countries/

Pan, Jennifer. 2016. "How Market Dynamics of Domestic and Foreign Social Media Firms Shape Strategies of Internet Censorship." Problems of Post-Communism 64 (3-4): 167–88. https://doi.org/10.1080/10758216.2016.1181525

Parks, Lisa, and Rachel Thompson. 2020. "Internet Shutdown in Africa| the Slow Shutdown: Information and Internet Regulation in Tanzania from 2010 to 2018 and Impacts on Online Content Creators." International Journal of Communication 14 (0): 21. https://ijoc.org/index.php/ijoc/article/view/11498

Roberts, Margaret E. 2018. Censored: Distraction and Diversion inside China's Great Firewall. Princeton University Press

Xu, Xu. 2021. "To Repress or to Co-Opt? Authoritarian Control in the Age of Digital Surveillance." American Journal of Political Science 65 (2): 309–25

8. Political and Economic Tradeoffs: Understanding the Dictator's "Digital Dilemma"

Jaclyn A. Kerr

As the Internet and digital information and communication technologies (ICTs) have spread globally, governments around the world have struggled to understand the transformative impacts of these technologies and determine how best to govern them. This challenge has been particularly acute for nondemocratic states where availability of the new technologies offered citizens new mechanisms for free expression, association, information sharing, and protest mobilization. Left unrestricted, these new tools and civic spaces could contribute to political instability, risking the downfall of the ruling regime. But rulers have also had to consider potential economic and political costs of restrictions.

The concept of a "Digital Dictator's Dilemma" first surfaced in the late 2000s and early 2010s in analyses seeking to make sense of these tradeoffs (Drezner 2010; Zuckerman 2008). Models suggested that "dictators" select optimal restriction levels to maintain an equilibrium of control within the new technological environment. The concept featured in debates between web-idealists and cyber-realists, supporting arguments for why the Internet's long-term impact on society would likely bend more towards liberation and democratization or control and repression (Diamond 2010; Shirky 2011; Morozov 2011). Researchers used it to examine why policy responses differed across nondemocratic states, explaining variation between more and less repressive approaches. While dictator's dilemma models constitute a significant simplification of complex, globally interdependent and sometimes-decentralized processes, these approaches – properly-caveated – can be useful tools for better understanding the history and ongoing development of digital authoritarianism.

The Expanding Internet and Governance Tradeoffs

Early discussions of a "digital dilemma" for governments took place in a period of high-visibility mass protest mobilizations in which the Internet, mobile phones, and social media were perceived as playing prominent roles. These included Iran's Green Movement, the Arab Spring, Russia's Bolotnaya Protests, and even unusual protest and social unrest events in established democracies such as the London Riots and Occupy Wall Street movement. The global spread of digital technologies and infrastructure were widely discussed as empowering movements for liberalization, reform, and democratization. But their potential abuses to reinforce state control and enable new forms of repression were also coming into focus with research detailing digital censorship, surveillance, and manipulation of the information environment (MacKinnon 2010). While debate raged over whether the new technologies would ultimately serve a purpose more of "liberation" or "control," it became increasingly clear that how governments decided to restrict or utilize the technologies would play a role in determining these outcomes.

By the early 2010s, there was already noteworthy variation between approaches. Research on Internet restrictions in different countries demonstrated a wide variety of legal, extra-legal, and technical approaches by which governments – and authoritarian regimes in particular – sought to control the network within their territories. While some of the most closed authoritarian regimes (e.g. North Korea) had attempted to completely isolate their citizens from the global Internet, others had implemented strict filtering and blocking regimes aimed to prevent their citizens from accessing content concerning sensitive political or social issues and in some cases blocking their use of internationally popular social media sites (e.g. China, Saudi Arabia). Other countries had employed a variety of different approaches – some of them less obvious – to control content or access to particular materials at specific moments (e.g. Russia). Regimes employed a wide range of control tactics, including: cutting off or throttling access at key moments, limiting use through high costs, weaponizing draconian laws and prosecutions, pressure on or takeovers of private sector companies, pervasive as well as targeted forms of surveillance, and covert production or manipulation of content (Deibert et al 2010).

Digital dictator′s dilemma models and comparative research across cases made sense of this variance explaining factors that prompted states to adopt more or less repressive approaches to the Internet or could influence selection of particular control approaches. Regime type was one obvious explanation. There was good reason to expect a regime's approach to the Internet to resemble its prior policies in regulation of offline civic freedoms such as freedom of expression, media, association, and protest. Nondemocratic regimes were overall more inclined to censor and repress Internet use. Thus, China's "Great Firewall" emerged as an exemplar of a system to censor Internet content in order to prevent protest mobilization and maintain social stability (King, Pan, and Roberts 2013). Yet many nondemocratic states did not censor the Internet or did so less robustly than they did other media forms leading sometimes to surprisingly asymmetric online-offline policy gaps. Economic, political, and technical factors helped explain these asymmetries and the different approaches taken by states of relatively similar regime types. These factors also clarify how digital policy dynamics have changed over time.

Rising Authoritarianism and the Spread of Digital Illiberalism

The last decade has seen significant decline in digital freedom globally. This has involved both intensification and wider uptake of digital illiberal practices. Some of these developments can be explained by changes in the digital governance dilemmas confronted by nondemocratic regimes. Taking off in the post-Cold War period of globalization, the Internet and ICT sector′s global expansion was seen in most countries as critical to economic growth and development. Even among nondemocratic states, many governments focused first on the opportunities associated with building a vibrant digital ecosystem and avoided restrictions that would hamper this development or frighten off investment. This coincided with the global expansion of hybrid and competitive authoritarian regime forms many of which maintained power partly through public support, relying on perceptions of economic performance and facades of democracy more than extreme forms of coercion and

repression. Such regimes utilized "low intensity coercion" and targeted repression, but abstained from overt and widespread violations of democratic norms in order to benefit from global economic integration and avoid consequential reputation costs at home and abroad (Levitsky and Way 2010). In digital governance this sometimes took the form of subtle, covert, and plausibly deniable "next generation" manipulations of the information environment in lieu of systemic censorship (Deibert et al 2010).

This balance became more challenging though as Internet penetration grew and, with it, the perceived role of ICTs in mass protest mobilizations. Following the prominent protest movements of the early 2010s, threat perceptions around the role of the Internet hardened in many nondemocratic countries. What once had been seen as a source of growth and performance legitimacy became viewed as a threat to regime stability and survival. In 2014, for example, Russian President Vladimir Putin famously referred to the Internet as a "CIA project" – a rapid about-face from Dmitry Medvedev's presidential Twitter account and touring of Silicon Valley (Clark 2010; MacAskill 2014). Though governments seeking to rein in the role of ICTs had sometimes been constrained by lack of technical know-how, low state capacity, or public opinion blow-back, the 2010s saw a period of significant authoritarian learning and the increasing availability of affordable censorship and surveillance systems through global markets. The normative environment regarding appropriate democratic approaches to Internet freedom simultaneously became more fragmented and contentious, lessening the costs of noncompliance. Diffusion dynamics across states of similar regime types demonstrated that digital policy outcomes were no longer isolated choices of particular regimes but increasingly also involved elements of legal or technical emulation, collaboration, or transfer (Kerr 2018).

A rapidly changing geopolitical and technological environment over the last decade has further complicated the digital dilemmas faced by governments, shaping the ongoing evolution of digital illiberalism as well as debates within and across democracies. The rise of interstate cyber and information conflict and increasing

technological competition has shifted common understandings of the Internet and cyberspace from a primarily positive sum arena to a nexus of great power competition and security vulnerability. This has coincided with growing consideration of risks as well as benefits associated with interdependence and globalization, manifest in the digital realm in calls for "data localization," "digital sovereignty," or "decoupling" (Drezner, Farrell, and Newman 2021; Kerr 2022). The changing natures of the technologies themselves, furthermore, alter what uses are being governed and what mechanisms of control or repression are possible. We see this, for example, in debates about the civil liberties and security repercussions of smart cities and the Internet of Things, privacy and equity concerns around big data and facial recognition, as well as in discussion of novel proliferation threats or ethical concerns related to data-centric fields of AI, additive manufacturing or synthetic biology (Bajema 2018; DeNardis 2020; Horowitz et al 2018; Wright 2019). Considerations about appropriate democratic governance of social media and online speech in the face of growing concerns around disinformation and extremism highlight the potential for emerging digital technologies to unsettle existing governance arrangements.

Conclusion: Implications and Policy Consideration

The global spread of the Internet and digital information technologies is an ongoing historic transformation with far-reaching repercussions for the future of government and society. Initially destabilizing to some prior systems of government, growing Internet and ICT use has engendered various adaptive responses and consequent further differentiation and evolution of political regime types. Part of this adaptive process has amounted to closing online-offline policy asymmetries as governments learn how to implement similar online measures to their preexisting offline tendencies – whether authoritarian, democratic, or of some hybrid regime form. But as digital technologies become more pervasive in society, regulating their use becomes less about a separate governance sphere and more about overarching regime approaches to control or repression. The technology becomes a forcing device

towards the establishment of new governance equilibria. Allowing different new affordances for both states and civil society actors, it engenders and facilitates innovation on both parts, whether to maintain or challenge existing forms of governance and control.

The conceptualization of a "digital dictator's dilemma" as a model for understanding these processes and making sense of the spread of illiberal digital governance practices is of renewed relevance today in light of the increasing extremity and spread of digital repression. The conceptualization of digital policy outcomes in states as resulting primarily from separate, deliberate, centralized, unitary, and rational decision processes can risk being overly reductionist. It can miss the roles of more decentralized or path-dependent processes, complex interdependencies across states, or nuanced variations in forms of digital control and their implementation. But such models can also be a critical piece in understanding conflicting pressures shaping policy options, particularly in nondemocratic settings where researchers have limited insight into precise political processes. They can counter tendencies to see digital policy in black-and-white terms of democratic versus authoritarian binaries. By helping clarify forces influencing policy outcomes in nondemocratic contexts, they can also serve as a tool for developing better foreign policy interventions to limit the spread and extremity of digital illiberalism.

Dr. Jaclyn A. Kerr is Senior Research Fellow for Defense and Technology Futures at the Center for Strategic Research at National Defense University's Institute for National Strategic Studies. She is also a Nonresident Fellow with the Brookings Institution, an adjunct faculty member at Georgetown University's Center for Eurasian, Russian and East European Studies, and an affiliate with the Center for International Security and Cooperation at Stanford University. Her research focuses on digital and emerging technologies and their current and future impacts on international politics, national security, and democracy. Dr. Kerr has conducted overseas research on digital activism and illiberalism in the former Soviet region. She has held fellowships at the US Department of State, Lawrence Livermore National Laboratory, and Harvard and Stanford Universities. She also has worked as a software engineer. Dr. Kerr holds a PhD and MA in Government from Georgetown University, and an MA in Russian, East European, and Eurasian Studies and BAs in Mathematics and Slavic Languages and Literatures from Stanford University.

The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the US government.

References

Bajema, Natasha. 2018. "WMD in the Digital Age: Understanding the Impact of Emerging Technologies." Emergence and Convergence Series (4). Center for the Study of Weapons of Mass Destruction, National Defense University. October 25, 2018. https://wmdcenter.ndu.edu/Publications/Publication-View/Article/1672667/wmd-in-the-digital-age-understanding-the-impact-of-emerging-technologies/

Clark, Andrew. 2010. "Dmitry Medvedev picks Silicon Valley's brains." The Guardian. June 23, 2010. https://www.theguardian.com/business/2010/jun/23/dmitry-medvedev-silicon-valley-visit

Deibert, Ronald, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, and Miklos Haraszti, eds. 2010. Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. Cambridge, Mass: The MIT Press. https://doi.org/10.7551/mitpress/8551.001.0001

Deibert, Ronald, and Rafal Rohozinski. 2010. "Liberation vs. Control: The Future of Cyberspace." Journal of Democracy 21 (4): 43–57

DeNardis, Laura. 2020. The Internet of Everything: Freedom and Security in a World with No Off Switch. New Haven: Yale University Press

Diamond, Larry. 2010. "Liberation Technology." Journal of Democracy 21 (3): 69–83. https://doi.org/10.1353/jod.0.0190

Drezner, Daniel W. 2010. ‟Weighing the Scales: The Internet's Effect On State-Society Relations.″ Brown Journal of World Affairs XVI (II): 31–44 https://www.jstor.org/stable/24590907

Drezner, Daniel, Henry Farrell, and Abraham Newman, editors. 2021. The Uses and Abuses of Weaponized Interdependence. Washington, D.C.: Brookings University Press.

Gladwell, Malcolm, and Clay Shirky. 2011. ‟From Innovation to Revolution: Do Social Media Make Protests Possible?″ Foreign Affairs. https://www.foreignaffairs.com/articles/2011-01-19/innovation-revolution

Horowitz, Michael, Gregory Allen, Elsa Kania, and Paul Scharre. 2018. ‟Strategic Competition in an Era of Artificial Intelligence.″ Artificial Intelligence and International Security Series. Center for a New American Security (CNAS). July 25, 2018. https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence

Kerr, Jaclyn A. 2018. ‟Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region.″ International Journal of Communication 12: 3814–3834. https://ijoc.org/index.php/ijoc/article/view/8542/2460

Kerr, Jaclyn A. 2022. ‟Runet's Critical Juncture: The Ukraine War and the Battle for the Soul of the Web.″ SAIS Review of International Affairs 42(2): 63-84. doi:10.1353/sais.2022.0011.

King, Gary, Jennifer Pan, and Margaret Roberts. 2013. ‟How Censorship in China Allows Government Criticism but Silences Collective Expression.″ American Political Science Review 107 (2): 1–18. https://gking.harvard.edu/publications/how-censorship-china-allows-government-criticism-silences-collective-expression

Levitsky, Steven, and Lucan A. Way. 2010. Competitive Authoritarianism: Hybrid Regimes after the Cold War. New York: Cambridge University Press

MacAskill, Ewen. 2014. "Putin Calls Internet a 'CIA Project' Renewing Fears of Web Breakup." The Guardian. April 24, 2014. https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia

MacKinnon, Rebecca. 2012. Consent of the Networked: The Worldwide Struggle For Internet Freedom. New York: Basic Books

Morozov, Evgeny. 2011. The Net Delusion: The Dark Side of Internet Freedom. New York: PublicAffairs

Shirky, Clay. 2011. "The Political Power of Social Media: Technology, the Public Sphere, and Political Change." Foreign Affairs 90 (1): 28–41. https://www.foreignaffairs.com/political-power-social-media

Wright, Nicholas D. 2019. Artificial Intelligence, China, Russia, and the Global Order. Maxwell Air Force Base, Alabama: Air University Press.

Zuckerman, Ethan. 2008. "The Cute Cat Theory Talk at ETech." My Heart's in Accra. March 8, 2008. http://www.ethanzuckerman.com/blog/2008/03/08/the-cute-cat-theory-talk-at-etech/

9. Responding to Digital Repression: Opportunities for Governments

Allie Funk

Digital repression is more sophisticated, entrenched, and transnational than ever before. Governments across the democratic spectrum are deploying technology as a vehicle for control. This chapter outlines key opportunities for states to respond: (1) more effective multilateral coordination; (2) bolstered national protections for human rights online; and (3) increased investment in local actors.

Ultimately, no government can address this problem alone. Human rights groups, media institutions, and activists are on the front lines of resisting repression, and industry experts possess technical knowledge and experience from years of confronting censorship and surveillance. States should take an inclusive approach to policymaking, closely working with civil society, academia, the private sector, and other experts to create and implement these recommendations, monitor their effectiveness, and innovate new approaches. Working together, governments, civil society, and industry can foster a more democratic future.

At the international level

Greater coordination among likeminded states is necessary to respond to digital repression. At the international level, governments can reinvigorate norms in multilateral and bilateral settings, incorporate internet freedom in democracy assistance, and reduce opportunities for foreign actors to use digital technology for harm.

Democratic investments in multilateral bodies like the United Nations (UN) and the Freedom Online Coalition (FOC) are important counterweights to efforts led by authoritarian states like Russia and China, which have vied to cement their model of digital control at global forums. Established in 2011 largely for diplomatic coordination

(Jackson et. al 2022), the FOC presents an unrealized opportunity for human rights online, and recent investments in the body – including by the U.S. government as 2023 FOC chair – present a chance to reinvigorate the alliance. Member states should strengthen the body´s name recognition and its ability to drive diplomatic coordination around tech policy. They should also proactively articulate the advantages of free and open internet and engage with the so-called "swing states˝ of internet freedom, showing that protecting human rights benefits local economies and national security.

Democracies should not shy away from participating in multilateral standards-setting bodies. The UN´s International Telecommunication Union (ITU) has been an unexpected breeding ground for authoritarian influence, particularly under China´s recent leadership. In these spaces, democracies can prevent slides toward digital repression, including by safeguarding the internet´s decentralized infrastructure and supporting internet-related multistakeholder bodies – like the Internet Corporation for Assigned Names and Number (ICANN) – where civil society and non-governmental experts have decision-making power.

Democracies should also combat digital repression through bilateral engagement. More than three-quarters of the world´s internet users live in countries where they face legal repercussions for expressing themselves online (Shahbaz et. al 2022); when engaging with perpetrator countries, democracies should advocate for repealing laws criminalizing free expression and unconditionally releasing people detained under these statutes.

A free-for-all private market has allowed spyware, social media monitoring, and other advanced technology to be sold at affordable prices. This has lowered the cost of entry for security agencies, law enforcement, and other state entities that target their populations at home and abroad. Democracies should strictly limit the sale and export of censorship and surveillance technologies that can undermine human rights, particularly to governments that have engaged in patterns of repression.

Finally, democracy assistance programs should support civil society working on these issues and limit the impact of digital repression on communities. Non-governmental groups and human rights defenders face daunting challenges, from legal and physical repercussions to constrained financial resources. Assistance programs should provide easy-to-access funding, technical expertise, and other support, and prioritize creating open-source and user-friendly technology for censorship and surveillance circumvention. Courts also serve as a bulwark for human rights online (Shahbaz et. al 2022). Assistance programs should aim to safeguard judicial independence, improve technical literacy among judges, and provide resources for strategic litigation.

At the national level

Democracies´ problematic behavior at home resonates beyond their borders: autocratic leaders often point to democracies´ actions to justify their own repression. For example, Germany´s controversial Network Enforcement Act – which compels companies to remove vaguely defined "illegal" content without judicial oversight (Human Rights Watch 2018) – has been used as a model by at least 13 governments, including by less free states to silence the speech of civil society and opposition politicians (Freedom House 2022). Responding to the global misuse of technology requires democracies to look inward and embed human rights protections into national-level policies.

Disproportionate surveillance remains one of democracies´ most glaring problems in this space. An increasingly securitized mindset has driven a misguided belief that intrusive tools and access to troves of data will bring about a safer society. Policymakers should instead strengthen domestic privacy protections, and surveillance rules – including those that use biometrics and open-source intelligence methods like social media monitoring – should adhere to the International Principles on the Application of Human Rights to Communications Surveillance (2013),

guidelines created by an expert coalition outlining under what circumstances state access to data is justified.

Democratic leaders have also sought to undermine end-to-end encryption, a necessary cybersecurity protocol for human rights defenders, journalists, businesses, and governments themselves. Policymakers should not mandate "back doors," establish requirements for traceability of messages, or reduce intermediary liability protections for providers of encryption services. Democracies' disparaging of encryption benefits autocratic leaders seeking a pretense to dismantle the technology for their own political ends.

Strong data protection laws that minimize what data the private sector can collect, how it can be stored, and with whom it can be shared can reduce digital platforms' vulnerability as vehicles for state repression. For instance, if specific categories of personal data cannot be fed into recommendation systems, state propaganda campaigns that rely on microtargeting people based on personal characteristics may not have the same reach.

Additionally, free expression and access to information should be central pillars to states' policy and governance of the digital ecosystem, but censorship has been normalized as a legitimate policy tool. In 2021, India secured its bleak title as the world's leader in internet shutdowns for the fourth time (Access Now 2022). And blocks to websites hosting political, social, and religious content reached an all-time high in 2022 (Shahbaz et. al 2022).

Governments should refrain from disrupting internet access and blocking services that host content with which they disagree. While platforms can present genuine human rights and national security concerns, blocking them entirely is arbitrary, disproportionate, and unduly restrictive. Instead, policymakers should incentivize platform responsibility and bolster transparency across advertising systems, content moderation, algorithmic systems, and other core practices. Vetted researchers can

also be given access to certain forms of data from large platforms, which can inform future policy development, research, and advocacy. Strengthened transparency can shed light into how the private sector contributes to digital repression. The European Union's Digital Services Act serves as one promising model for regulating large platforms.

Finally, content hosts should benefit from safe-harbor protections for most user-generated and third-party content. Strong protections against intermediary liability are imperative amid rising state censorship. They encourage responsible content moderation of violent, incendiary, or harmful speech that may otherwise be legal in a given country and, without them, websites and platforms may err on the side of censorship rather than protect speech in order to avoid being held liable.

At the local level

Local stakeholders – including state officials, news outlets, and grassroots activists – are most directly connected to their communities and are critical for building digital resilience. Diverse and independent local media are at risk from hostile actors, market concentration, and a lack of sustainable funding. People are thus losing access to reliable information that encourages public participation, explores the impact digital technology has on human rights, and holds powerful actors accountable. Democracies should support local media environments by giving full access to state officials and resources, protecting from online harassment and intimidation, and supporting financial assistance and innovative financing models, skills training, and mentoring.

Finally, civic education and digital hygiene programs can help build capacity to identify and debunk unreliable information, including from state disinformation campaigns. Funding to local schools and training programs, at all educational levels, should prioritize digital and media literacy, and digital hygiene best practices, like using virtual private networks. Fostering a strong public understanding of and

resilience to digital repression empowers people to defend human rights domestically and support foreign policies that protect them abroad.

Allie Funk is Research Director for Technology and Democracy at Freedom House. She leads the organization's technology and democracy initiative, including Freedom on the Net, Election Watch for the Digital Age, and work related to protecting a free and open internet. She also represents Freedom House on the Freedom Online Coalition's Advisory Network, and her analysis on human rights online has been published in numerous Freedom House reports and in the Washington Post, the Los Angeles Times, WIRED, the Hill, the Information, the Diplomat, and Just Security, among others.

References

Access Now. 2022. "Report: Internet Shutdowns in India in 2021." Access Now. https://www.accessnow.org/internet-shutdowns-india-keepiton-2021

Freedom House. 2022. "Freedom on the Net 2022: Singapore." Freedom House, October 2022. https://freedomhouse.org/country/singapore/freedom-net/2022

Human Rights Watch. 2018. "Germany: Flawed Social Media Law." Human Rights Watch, February 14, 2018. https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

International Principles on the Application of Human Rights to Communications Surveillance. 2013. "International Principles on the Application of Human Rights to Communications Surveillance." 2013. https://necessaryandproportionate.org

Jackson, Rose, Leah Fiddler, and Jacqueline Malaret. 2022. "An Introduction to the Freedom Online Coalition." Atlantic Council. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/introduction-freedom-online-coalition/

Mchangama, Jacob, and Joelle Fiss. 2019. "Analysis: The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship." Justitia. https://justitia-int.org/the-digital-berlin-wall-how-germany-created-a-prototype-for-global-online-censorship/

Shahbaz, Adrian, Allie Funk, and Kian Vesteinsson. 2022. "Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet." Freedom House, October 2022. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

10. The Role of Multinational Corporations in Combating Digital Repression

Richard Crespin, Caroline Logan and Ana Blanco

In the aftermath of the Russian invasion of Ukraine, Russian citizens found their digital and social media channels inundated with messages claiming Ukraine´s "Nazi-led government" planned to invade their country and that international reports stating the opposite were a hoax. This kind of digital repression leaves Russian citizens in the dark and has severely impacted the Russian economy, as pressure from investors and consumers has led to hundreds of multinational corporations (MNCs) forfeiting their investments and leaving the country (OECD, 2022 and Scientific American, 2022).

Alongside the obvious human costs, digital repression negatively affects business, as trade and commerce suffer in the absence of access to truthful information and autocratic regimes often subvert market economies, depriving businesses and their customers of healthy competition. Digital platforms are caught in a global cat-and-mouse struggle between autocrats seeking to exploit communication technology for political gain, and citizens and corporations who need the same tools to fight such regimes (Feldstein 2021). MNCs across industries, and tech platforms in particular, play a crucial role in combating digital repression and must take action to protect business interests and the public.

Digital repression carries a high cost for MNCs including:

1. Business operations: digital government censorship and information manipulation impede company operations and disrupt supply chains.
2. Corporate reputation & brands: especially if they are perceived as cooperating with government censorship or surveillance.
3. Financial losses: blocking a company's website or services limits its reach with customers and consequently its revenue.

4. Legal compliance challenges: if a company complies with local laws that restrict online speech or inappropriately hands over user data to the government, these activities may conflict with privacy laws and human rights in other jurisdictions.

Maintaining a free and open digital economy while respecting human rights is both good morals and good business. Digital transformations have benefitted MNCs immeasurably, opening new forms of communication, commerce, and service delivery. Growth, however, comes with risk and responsibility. As the economic and political influence of MNCs grow, consumers, investors, and employees increasingly want to support companies that stand up for what is right, rejecting those that do not.

To be good digital corporate citizens, MNCs must implement policies that protect against the harms of digital repression, use their influence to push digital literacy, and eliminate investments that directly or indirectly fund digital repression.

Second, they should consider directing political contributions to democratic governments and participating in international coalitions that support digital freedoms. Through partnerships and funding, businesses can promote and support modern international and national regulatory frameworks conducive to an open, global digital space.

Third, multinationals must abide by the highest standards of data privacy and eradicate commercial spyware and targeted surveillance from their operations. Simultaneously, they should fight government restriction orders that seek to limit citizens' (and their employees´) access to accurate information.

Tech companies that own and manage the digital platforms that connect billions of people at an unprecedented speed and scale should take responsibility for ensuring proper use of their platforms. Many tech firms are reluctant to intervene when authoritarian governments use their platforms to repress the public. Although understandably wary of being accused of censorship or partisanship, these firms

should take the following steps to ensure their platforms promote an open exchange of information and are not used as the weapon of choice by autocrats and their allies.

1. Allow Free Speech, but Limit Reach:

When Elon Musk took over Twitter, he fired many content moderation teams responsible for removing prohibited material from the site. Within hours, the use of derogatory racial slurs spiked 500 percent (Mcintyre 2023). However, roughly a month into Musk's tenure, he changed his tune, noting, "freedom of speech does not mean freedom of reach" (Mcintyre 2023). In other words, users are entitled to the free expression of your opinion but not to its free distribution. Big Tech platforms need to exercise judgment, especially on distribution of content (CollaborateUp 2022).

2. Transform and Invest in Content Moderation:

The sheer volume of content on social media makes it nearly impossible to establish a comprehensive editorial system. Therefore, platforms must develop more sophisticated tools that maximize synergies between AI and human intelligence (Yaraghi 2022). One tactic: prioritize topics for moderation based on the threat the information poses. Spreading misinformation that the Earth is flat, as an example, is relatively innocuous, while spreading information that undermines trust in vaccines can cost lives. Content moderators should prioritize accordingly. In addition, tech companies should invest more in local partnerships for better content moderation, as local experts better understand digital repression in the context of their country (Hook and Verdeja 2022).

3. Reform Algorithms:

Social media does more than host third party content, its algorithms actively and profitably amplify it (Mcintyre 2023). Tech companies should publish their algorithms to promote transparency and better-informed choice for users.

4. Partner with Democratic Governments:

Tech companies should continue and enhance dialogue with democratic governments to better understand and anticipate threats (CollaborateUp 2022).

5. Invest in Pre-bunking:

CollaborateUp´s report on mis- and disinformation reveals that correcting a message after it enters the digital space often backfires by unintentionally reinforcing the very message it sought to discredit (CollaborateUp 2022). Pre-bunking anticipates potential lies, tactics, or sources before they strike. Tech companies should more actively ˝vaccinate the public˝ against disinformation. For example, Facebook may not want to make a public statement on climate change, but can explain the building blocks of a conspiracy theory using a neutral example (Sander Van Der Linden 2022). Public education can help the average citizen better identify potentially false information or ˝shallow fakes˝ coming from authoritarian governments and their trolls.

6. Flag Untrustworthy Sources:

While platforms have improved their use of indicators that flag unverified or untrustworthy sources, it can sometimes backfire. Platforms must provide greater clarity and specificity on community guidelines to avoid biases in automated flagging systems as they can sometimes inadvertently censor the people trying to bring correct information to light (Cheikosman et al. 2022).

7. Arm and Empower the "Good Guys" with Widely Accessible Resources:

The Digital Ministry of Ukraine developed guidelines to enable anyone with a cell phone and/or access to the Internet to counter the massive amount of computational propaganda Russia publishes by arming the public with smart tools. In an NPR interview with Vera Bergengruen, she highlighted how the Ukrainian government repurposed Telegram bots originally used for basic customer service functions, such as registering for a driver´s license, to allow ordinary citizens to report Russian Army movements (Davies 2022). MNCs must do likewise, using their resources to counter the spread of disinformation at scale.

8. Invest in Upstream Monitoring and Partnerships:

Tech companies must continually invest in upstream preventative monitoring and not just when there is public scrutiny (Hook and Verdeja 2022). MNCs can maximize their effectiveness by sponsoring and participating in digital media literacy programs, provide journalism grants that allow media paywalls to be removed during crises, and develop grant programs for the longitudinal study of digital repression (CollaborateUp 2022; Hook and Verdeja 2022).

When it comes to combating digital repression, if everyone is responsible, no one is responsible. Because they have benefited so much from the growth of the digital economy, MNCs have a special responsibility to use their resources to maintain a free and open digital exchange of information. They also have a special ability to do so using their employee engagement, brands, and supply chains. Working in concert with civil society and democratic governments, MNCs can and should do more to combat digital repression. No one said it would be easy.

Richard Crespin, CEO, CollaborateUp, Caroline Logan, Manager, CollaborateUp, and Ana Blanco, Founding Principal, LinkUp Global.

Photo by cottonbro studio

References

Bushwick, Sophie. 2022. "Russia Is Using 'Digital Repression' to Suppress Dissent." Scientific American, March 15, 2022. https://www.scientificamerican.com/article/russia-is-using-digital-repression-to-suppress-dissent/

Cheikosman, Evin, Emily Ratté, and Marcus Burke. 2021. "3 Tech Design Principles to Help Curb Digital Repression." Weforum.org. World Economic Forum. July 13, 2021. https://www.weforum.org/agenda/2021/07/three-tech-design-principles-can-help-curb-digital-repression-algorithm-ai-bias-online-harm-data-policy/

CollaborateUp. 2022. "News Literacy and Misinformation/Disinformation in the Era of COVID-19." Collaborate Up. https://collaborateup.com/news-literacy-and-misinformation-disinformation-in-the-era-of-covid-19/

Davies, Dave. 2022. "Ukraine Is Inventing a New Way to Fight on the Digital Battlefield." NPR.org, March 31, 2022. https://www.npr.org/2022/03/31/1089660395/ukraine-is-inventing-a-new-way-to-fight-on-the-digital-battlefield

Feldstein, Steven. 2021. The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance. Oxford: Oxford University Press USA – OSO

Hook, Kristina, and Ernesto Verdeja. 2022. "Social Media Misinformation and the Prevention of Political Instability and Mass Atrocities." Stimson Center. July 7, 2022. https://www.stimson.org/2022/social-media-misinformation-and-the-prevention-of-political-instability-and-mass-atrocities/

Linden, Sander van der. 2022. "Misinformation: Susceptibility, Spread, and Interventions to Immunize the Public." Nature Medicine 28 (3): 460–67. https://doi.org/10.1038/s41591-022-01713-6

McIntyre, Lee. 2022. "Twitter and the Fight over Free Speech." Deseret News, December 21, 2022. https://www.deseret.com/2022/12/20/23509557/twitter-elon-musk-free-speech.

Niam Yaraghi. 2019. "How Should Social Media Platforms Combat Misinformation and Hate Speech?" Brookings.edu. Brookings. April 9, 2019. https://www.brookings.edu/blog/techtank/2019/04/09/how-should-social-media-platforms-combat-misinformation-and-hate-speech/

OECD. 2022. "Disinformation and Russia's War of Aggression against Ukraine." OECD.org. OECD. November 3, 2022. https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/

11. How can NGOs and people's movements oppose the rise of digital repression?

Jennifer Earl

Research on social movement repression has often focused on explaining the use of repressive capacities and its consequences, with less attention to how to reduce repression (Earl and Braithwaite 2022) or mitigate its impacts (save important counterexamples, e.g., Reynolds-Stenson 2022). Research on digital repression, though, has focused more on its methods (Knockel et al. 2020; Marczak et al. 2015) and policy implications (Feldstein 2021). Taking advantage of these differences, I make three arguments about how digital repression can be opposed and/or mitigated.

Applying Existing Resistance Techniques

Because so many scholars who study digital repression don't have a background in the study of social movement repression, discussions of digital repression often forget that social movements have been challenging repression long before the Internet existed. For instance, local and international human rights organizations have worked together to shame countries for their use of traditional forms of repression (Murdie and Davis 2012). This is so common that highly repressive countries may attempt to curtail the ability of organizations to monitor and raise awareness about human rights abuses (Smidt et al. 2021). Playing a longer game for the reduction of repression, other scholars have examined attempts to prosecute former leaders for their roles in human rights abuses (Sikkink and Kim 2013). Still other researchers have examined how social movement communities and organizations support activists who repeatedly experience repression (Reynolds-Stenson 2022).

It is quite likely that some forms of digital repression may be opposed or mitigated in similar ways, particularly forms of digital repression that have strong parallels to pre-Internet forms of repression such as the use of physical violence against digital

targets or the use of digital surveillance (Earl, Maher, and Pan 2022). To be sure, digital forms of repression like digital surveillance will create pressure on advocacy groups (Richard, Rigaud, and Maddow 2023) and researchers (e.g., Hulcoop et al. 2017; Marczak et al. 2018) to grow their capacities to discover and monitor digital repression. Moreover, it will be important that technologists who help identify digital repression also aid in efforts to, for instance, name and shame in hopes of raising international scrutiny and pressure.

Making Repression Risky

While substantial agreement exists amongst repression researchers about the causes of traditional social movement repression, the consequences of repression have remained fundamentally unsettled (Davenport 2007). In fact, empirical research can be found that shows repression reduces protest, amplifies it, deters specific activists, radicalizes specific activists, alternates over time between these, or has some curvilinear shape, amongst many other empirically supported options (Earl 2011). From the perspective of the repressor, one of the most dangerous outcomes of repression is backlash or backfire (Sutton, Butcher, and Svensson 2014; Hess and Martin 2006). While often discussed in relation to nonviolent resistance, backfire or backlash generally refers to situations in which social movements experience increases in engagement as a result of repression (e.g., Odabaş and Reynolds-Stenson 2018). Key to efforts to reduce repression, the risk of backfire makes the decision to repress riskier for repressors. When the risk of repression is simply resilience, repressors gamble only against the risk of inefficiency and/or lost resources. But, when repressors risk actually escalating support and engagement in the very social movements they were hoping to diminish, the decision to repress becomes far riskier.

Connecting this with digital repression, the very real potential for backfire or backlash is often ignored. This leads some, for instance, to make doomsday claims about the impacts of digital repressive capacities under the assumption that digital repression

always 'works' (e.g., Morozov 2011). Fortunately, a growing amount of research shows that backlash or backfire effects are quite likely with digital repression (Beyer and Earl 2018; Earl and Beyer 2014; Odabaş and Reynolds-Stenson 2018). Since social movements and allies can work to facilitate backfire (Hess and Martin 2006), mitigating repression should take advantage of the risk of backfire to make digital repression more of a gamble for repressors.

Keying Mitigation to the Form of Digital Repression

Digital repression encompasses a very broad and divergent set of actual activities, which can be committed by various levels of government and also by private actors. Drawing on a review of research on digital repression, Earl, Maher, and Pan (2022) provide the most comprehensive and nuanced typology of forms of digital repression to date. For instance, they integrate scholarship ranging from research on the imprisonment of bloggers to digital surveillance to more active measures campaigns like disinformation. Key to their argument is that both explanations of digital repression and explanations of the impact of digital repression need to be keyed to more specific forms of digital repression instead of a one-size-fits-all view.

This is clearly an important point when considering resistance to repression. For instance, private repressors, with their multiplicity of motives, are likely to be dissuaded from repression in very different ways than regimes. While naming and shaming tactics may cost both private and state-based repressors, it may be possible to create market consequences for private repressors and export controls that are more effective than the closest analog for regimes, economic sanctions. Similarly, there are likely very different ways of supporting resilience or backfire to digital surveillance than to censorship campaigns, for instance. It is important that policymakers and academics attend to these differences and key their plans for mitigation to the specific form of digital repression and its perpetrator.

In conclusion, while the rise of digital repression may seem novel in many ways, it is important to connect research on digital repression to research on more traditional forms of repression as important insights can be drawn. In this essay, I have pointed to the ways in which traditional forms of mitigation (e.g., shaming), risks to repressors (e.g., backfire), and attention to differences amongst types of digital repression can aid in the mission to reduce digital repression and mitigate its impacts.

Jennifer Earl is a Professor of Sociology and Criminal Justice at the University of Delaware. Her research focuses on social movements, information technologies, and the sociology of law, with research emphases on social movement repression (including digital repression, youth activism, Internet activism, and legal change. She is the recipient of a National Science Foundation CAREER Award for research from 2006-2011 on Web activism, was a member of the MacArthur Research Network on Youth and Participatory Politics, and co-authored with Katrina Kimport, Digitally Enabled Social Change.

Photo by Markus Spiske

References

Beyer, Jessica L., and Jennifer Earl. 2018. "Backfire Online: Studying Reactions to the Repression of Internet Activism." In The Paradox of Repression and Nonviolent Movements, edited by Lester R. Kurtz and Lee A. Smithey, 102-142. Syracuse, NY: Syracuse University Press

Davenport, Christian. 2007. "State Repression and Political Order." Annual Review of Political Science 10 (1): 1-23

Earl, Jennifer. 2011. "Political Repression: Iron Fists, Velvet Gloves, and Diffuse Control." Annual Review of Sociology 37: 261-284

Earl, Jennifer, and Jessica L. Beyer. 2014. "The Dynamics of Backlash Online: Anonymous and the Battle for WikiLeaks." Research in Social Movements, Conflicts and Change 37: 207-233.

Earl, Jennifer, and Jessica Maves Braithwaite. 2022. "Layers of Political Repression: Integrating Research on Social Movement Repression." Annual Review of Law and Social Science 18 (1): 227-248

Earl, Jennifer, Thomas V. Maher, and Jennifer Pan. 2022. "The digital repression of social movements, protest, and activism: A synthetic review." Science Advances 8 (10): eabl8198. https://www.science.org/doi/abs/10.1126/sciadv.abl8198

Feldstein, Steven. 2021. The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance. Oxford University Press

Hess, David, and Brian Martin. 2006. "Backfire, Repression, and the Theory of Transformative Events." Mobilization 11 (1): 249-267

Hulcoop, Adam, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ronald J. Deibert. 2017. Tainted leaks: Disinformation and phishing with a Russian nexus. Citizen Lab. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

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

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. 2018. Hide and Seek: Tracking NSO Group´s Pegasus Spyware to Operations in 45 Countries. University of Toronto. https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald J. Deibert, and Vern Paxson. 2015. China´s great cannon. Citizen Lab. https://citizenlab.ca/2015/04/chinas-great-cannon/

Morozov, Evgeny. 2011. The Net Delusion: The Dark Side of Internet Freedom. New York: Public Affairs

Murdie, Amanda M., and David R. Davis. 2012. "Shaming and Blaming: Using Events Data to Assess the Impact of Human Rights INGOs." International Studies Quarterly 56 (1): 1-16.

Odabaş, Meltem, and Heidi Reynolds-Stenson. 2018. "Tweeting from Gezi Park: Social Media and Repression Backfire." Social Currents 5 (4): 386-406

Reynolds-Stenson, Heidi. 2022. Cultures of Resistance: Collective Action and Rationality in the Anti-Terror Age. New Jersey: Rutgers University Press

Richard, L., S. Rigaud, and R. Maddow. 2023. Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy. Henry Holt and Company

Sikkink, Kathryn, and Hun Joon Kim. 2013. "The Justice Cascade: The Origins and Effectiveness of Prosecutions of Human Rights Violations." Annual Review of Law and Social Science 9 (1): 269-285

Smidt, Hannah, Dominic Perera, Neil J. Mitchell, and Kristin M. Bakke. 2021. "Silencing Their Critics: How Government Restrictions Against Civil Society Affect International ‘Naming and Shaming´." British Journal of Political Science 51 (3): 1270-1291

Sutton, Jonathan, Charles R. Butcher, and Isak Svensson. 2014. "Explaining political jiu-jitsu: Institution-building and the outcomes of regime violence against unarmed protests." Journal of Peace Research 51 (5): 559-573.

Conclusion: Accelerating Digital Repression and Its Existential Threat to Democracy

Chris Ogden and Olivia Hagen

This e-book has provided an in-depth analysis of digital repression, which is a growing threat to democratic governance globally. Comprising eleven chapters written by leading scholars and policymakers, it has highlighted how the rapid expansion of new and emerging internet and communication technologies (ICTs) has significantly increased any state´s capacity for repression and social control. This ever-growing technological capacity poses a serious threat to internet freedom and human rights, which can potentially have a devastating – and irrevocable – impact upon our societies worldwide. Although digital repression is often associated with autocracies, many of the contributors have also shown how democracies utilise repressive technologies, albeit less frequently, as they are subject to more significant normative and constitutional constraints (Feldstein 2021).

Through the diverse perspectives presented in this book, stakeholders at the local, national and global levels can now better understand the intricate environment of digital repression and develop effective strategies to combat this growing threat. As such, this E-Book serves as a valuable resource for those seeking to safeguard internet freedom and human rights in the face of digital repression. Exploring the various facets of digital repression, this project encompassed four distinct themes, each delving into important aspects of this phenomenon.

The first theme, emphasised by Steven Feldstein, Andrea Kendall-Taylor, and Erica Frantz, focused on identifying and understanding digital repression. In Chapter 1, Feldstein shed light on the underlying causes - and dispelled some common misconceptions - surrounding digital repression, noting that ‘policymakers should look at regime incentives, political interests, and resource capacity to better understand why regimes acquire and deploy repressive technologies´. Frantz and Kendall-Taylor´s Chapter 2 then considered the complex and multi-faceted reasons behind states adopting or abstaining from digital repression tactics and specifically considered regime type, digital capacity and levels of wealth.

The second theme then looked into the question of responsibility in digital repression, with contributions from Marcus Michaelsen, Xiao Qiang and Adrian Shahbaz. In Chapter 3, Michaelsen illuminated how autocrats employ digital repression tactics beyond their borders, including phishing campaigns, and examined the associated risks of such a strategy. Chapter 4 by Xiao then investigated China´s role in global digital repression through three key dimensions, namely the export of surveillance technology, investment in digital infrastructure and influencing international organisations. Finally, in Chapter 5, Shahbaz investigated private sector companies´ involvement in the digital repression nexus, elucidating their complicity as either unwitting or unscrupulous agents of state repression.

The third theme accentuated the perils of digital repression, and featured insights from Jessica Brandt, Anita Gohdes and Jaclyn Kerr. In Chapter 6, Brandt scrutinised the utilisation of digital repression by democracies and the resulting implications for democratic governance. In turn, Gohdes, in Chapter 7, examined whether or not ICTs primarily benefit states or civil society, ultimately identifying three spheres of control relating to criminalising civil society content, weaponising digital infrastructures and manipulating the information space. Finally, Kerr, in Chapter 8, assessed the 'dictator´s digital dilemma´, exploring how autocracies navigate the delicate balance between complete internet control and fostering economic development, which enhances how to decipher the evolution of digital repression.

The concluding theme then underscored effective policy responses to digital repression, featuring contributions from Allie Funk, Richard Crespin, Caroline Logan, Ana Blanco and Jennifer Earl. In Chapter 9, Funk outlined practical strategies for states to counter digital repression at the local, national, and international levels, including having more effective multilateral coordination, bolstering national protections for human rights online and increasing investment in local actors. Subsequently, Chapter 10 by Crespin, Logan and Blanco highlighted eight ways in which multinational corporations can combat digital repression, so as 'to ensure their platforms promote an open exchange of information and are not used as the weapon of choice by autocrats and their allies´. In the final chapter, Earl discussed how non-governmental organisations (NGOs) and people´s movements can oppose digital repression, specifically by applying existing resistance techniques, making repression risky, and keying mitigation tactics to combat different kinds of digital repression.

Generative AI's Exponential Threat

In light of the recent release of generative AI language models such as Open AI´s ‘ChatGTP´ and Google´s ‘Bard´, understanding how governments employ digital repression and how to respond to it has become even more crucial. Disinformation researchers have voiced concerns that these models could be harnessed as potent tools for spreading misinformation at an exponential rate. Whilst disinformation ‘is not a new problem´ (Sanders and Schneier 2023), with Facebook, for example, removing over a billion fake accounts a year that generate ‘fake news´ (Ibid), experts warn that rampant AI technology can make disinformation easier to produce on an industrial scale, and thus more challenging to stop.

With personalised chatbots that can mimic language, tone and human logic, disinformation could be spread in ever more credible and persuasive ways (Hsu and Thompson 2023). A 2020 study by the Center on Terrorism, Extremism, and Counterterrorism from the Institute of International Studies at Middlebury found that GPT-3, the technology behind ChatGTP, had an impressive knowledge of extremist communities and could create online content that mimics the content created by such groups (Hsu and Thompson 2023). Although Open AI has policies in place to prevent the creation of harmful or biased content and offers moderation tools to protect against misuse (OpenAI 2023), these measures are unlikely to be entirely effective. As ChatGTP itself has acknowledged, it ‘may occasionally produce harmful instructions or biased content´ and Sam Altman, CEO of ChatGPT´s Open AI, has noted that AI can be used to manipulate voters and target disinformation (Fung 2023).

In addition to concerns about the spread of disinformation, ChatGTP and similar AI technologies could also make ‘democracy even more messy´ (Cowen 2022), as they have the potential to intervene in democratic regulatory processes. In the US, for example, there is a comment period before new regulations take effect, which interested parties could potentially flood with the help of ChatGTP, similar to the Russian Internet Research Agency´s attempt to influence the 2016 US elections (Sanders and Scheiner 2023). Experts note that currently, there are no effective mitigation tactics to combat such disinformation, adding to the complexity – and ambiguity – of democratic processes (Hsu and Thompson 2023). As a result, stakeholders must be aware of the potential impact of both known and unknown AI technologies on democratic systems and develop appropriate strategies to mitigate all risks.

In autocracies, where digital repression has become a large part of the autocrats´ repressive toolkit, the threat to internet freedom and human rights is further amplified by the advent of AI technologies. For example, in the years leading up to the 2021 military coup in Myanmar, Facebook turned into an 'echo chamber of anti-Rohingya content´ (Amnesty International 2022), allowing the military junta and radical Buddhist nationalist groups to spread disinformation targeting the Muslim community. The consequences of the disinformation campaign were devastating, resulting in the military junta´s crackdown on the Rohingya in 2017, where the Rohingya were subject to widespread atrocities, including murder, rape, and torture, which forced hundreds of thousands of people to flee to nearby Bangladesh.

An Amnesty report from 2022 also revealed that Facebook 'knew or should have known´ (Amnesty International 2022) that their algorithms were not only spreading but also actively intensifying the dissemination of anti-Rohingya disinformation. This active role played by Facebook´s platform ultimately contributed significantly to the Rohingya genocide (Amnesty International 2022). Facebook later revealed that the key reason disinformation was allowed to flow on their platform was the lack of Burmese-speaking content moderators, with the company having only two such specialists available as of early 2015 (Solon 2018). This example underscores how AI has the capacity to contribute to the rapid spread, intensification and even normalisation of digital repression across different ICT platforms. Furthermore, it highlights the urgent need for stakeholders to proactively recognise the implications of AI technologies and develop robust strategies –regulatory, educational and practical – to counteract their negative impact on internet freedom and human rights.

In an authoritarian context, the development of potent AI software can, therefore, potentially turbocharge digital repression and authoritarian tactics. In countries like Myanmar, where the state lacks the incentive to moderate online content, AI could facilitate the mass production of disinformation. Consequently, this could perpetuate hatred and exacerbate the persecution of marginalised groups and activists. In more advanced autocratic states, led by the poster child of China, AI technology could also be used much more systematically by leaders to deeply manipulate information and heighten social control and regime survival. Once developed domestically, such technology could then be exported to other autocracies.

- - -

AI technology can – and most likely will – be exported in efforts to influence and subvert political processes in established democracies. Such efforts are entirely conceivable vis-à-vis the coming 2024 general elections in the United States and India and those in the United Kingdom in 2025. We can thus expect new AI-powered versions of Cambridge Analytica to personally and collectively target voters on an industrial scale, and in a highly specific, evolving and manipulative manner. Such a tactic will embolden a highly polarised political - and emotionally charged - atmosphere within these countries and elsewhere, significantly disrupting the conduct and outcome of these elections. If unchallenged, this technology will therefore be a destabilising, frightening and destructive force that poses a major existential threat to the world's oldest, largest and most essential democracies. Such an attack will invigorate authoritarian regimes, and tip humanity into an autocratic future.

Dr Chris Ogden is Senior Lecturer / Associate Professor in Asian Security and Asian Affairs in the School of International Relations at the University of St Andrews, Scotland. His research interests concern the global rise of India and China, great power politics, shifting world orders, authoritarianism, the Asian Century, Hindu nationalism, and the interplay between national identity, security and domestic politics in South Asia (primarily India) and East Asia (primarily China). Chris' latest book concerns The Authoritarian Century: China's Rise and the Demise of the Liberal International Order (Bristol UP) and he was also the Series Consultant for the 2023 BBC Documentary Series, India: The Modi Question. For more information, see http://chris-ogden.org
Olivia Mills Hagen is currently in her final year of an MA (Hons.) in International Relations at the University of St Andrews and an intern for Global Policy Online. Before university, she decided to do her National Service and spent a year in Northern Norway in the Norwegian Army's Artillery Battalion. During her time at St Andrews, Olivia has been the director of the Lumsden Leadership Summit, a platform that invites successful and inspiring women to speak to inspire the student body and help them become the next generation of leaders. As the director, she focused the summit on sustainability and invited women whose diverse careers shared sustainability as the common denominator. Her academic research is centered on the intricate and multifaceted phenomenon of digital repression, as well as international development, foreign policy of India and China and force and statecraft.

References

Amnesty International. 2022. "Myanmar: Facebook's Systems Promoted Violence against Rohingya; Meta Owes Reparations – New Report." amnesty.org. Amnesty

International. https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/

Cowen, Tyler. 2022. "ChatGPT Could Make Democracy Even More Messy." Washington Post, December 6, 2022. https://www.washingtonpost.com/business/chatgpt-could-makedemocracy-even-more-messy/2022/12/06/e613edf8-756a-11ed-a199-927b334b939f_story.html

Feldstein, Steven. 2021. The Rise of Digital Repression How Technology Is Reshaping Power, Politics, and Resistance. Oxford: Oxford University Press USA – OSO

Fung, Brian. 2023. "Mr. ChatGPT Goes to Washington: OpenAI CEO Sam Altman Testifies before Congress on AI Risks" CNN Business. May 16, 2023. https://edition.cnn.com/2023/05/16/tech/sam-altman-openai-congress/index.html

Hsu, Tiffany, and Stuart A. Thompson. 2023. "Disinformation Researchers Raise Alarms about A.I. Chatbots." The New York Times, February 8, 2023, sec. Technology. https://www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation.html

OpenAI. 2023. "OpenAI API." Platform.openai.com. OpenAI.2023. https://platform.openai.com/docs/guides/moderation/overview

Sanders, Nathan E., and Bruce Schneier. 2023. "How ChatGPT Hijacks Democracy." The New York Times, January 15, 2023, sec. Opinion. https://www.nytimes.com/2023/01/15/opinion/ai-chatgpt-lobbying-democracy.html

Solon, Olivia. 2018. "Facebook's Failure in Myanmar Is the Work of a Blundering Toddler." The Guardian, August 16, 2018. https://www.theguardian.com/technology/2018/aug/16/facebook-myanmar-failure-blundering-toddler