CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

DIGITAL DEMOCRACY NETWORK

Issues on the Frontlines of Technology and Politics

Steven Feldstein, editor

OCTOBER 2021

Issues on the Frontlines of Technology and Politics

Steven Feldstein, editor

The Carnegie Endowment thanks the Charles Stewart Mott Foundation for the support that has made the establishment of the Digital Democracy Network possible. Additional valuable support has come from the Ford Foundation, the Open Society Foundations, and the UK Foreign, Commonwealth & Development Office. The authors alone are responsible for the views expressed.

For your convenience, this document contains hyperlinked source notes indicated by copper-colored text.
For complete source notes, please read this article at CarnegieEndowment.org.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

This publication can be downloaded at no cost at CarnegieEndowment.org.

Photo: Cate Gillon/Getty Images

Contents

Introduction

STEVEN FELDSTEIN

Global political trends in recent years have put to rest any illusions that the relationship between technological innovation and progress in democratic politics would be largely positive. Digital technology is disrupting international politics in myriad ways. To start, it is bringing new dimensions to the authoritarian playbook, enabling governments to more easily manipulate information consumed by citizens, to monitor dissent and track political opponents, and to censor communications. Democracies, meanwhile, struggle to strike the right balance between rewarding economic innovation and reaping the financial benefits of Big Tech, while protecting user privacy, guarding against surveillance misuses, and countering disinformation and hate speech.

The COVID-19 crisis has intensified these tensions. Governments have seized upon the pandemic as an excuse to introduce a new wave of restrictions—emergency decrees that prohibit public gatherings, measures that censor online speech, and directives that affect user privacy. States have deployed new applications to counter the spread of the disease, rolling out contact tracing apps, facial recognition systems, and digital health passports. Some of these technologies represent legitimate attempts to control the virus but many measures lack basic safeguards to protect data privacy. Certain governments are using data collected from public health interventions in pursuit of unrelated law enforcement activities. It is unclear whether states will retract these restrictions when the pandemic finally ebbs or if they are here to stay.

As the United States' influence decreases and emerging states, particularly China, increase their power, the global online commons is fraying. Experts once divided internet governance into "democratic" and "authoritarian" domains. On one side stood the United States and its allies, which advanced a model centered round an "open, interoperable, reliable and secure internet" that prioritized individual freedom of action, liberal values, and minimal government interference. On the other side stood a smaller group of countries led by China, Russia, and Iran, which offered an alternative model premised on "information

security"—maintaining that a country's sovereign interests should dictate which rules apply. Despite insistence by U.S. President Joe Biden's administration that the world remains divided between "techno democracies" and "techno autocracies," a more accurate description would be *fragmentation.* Increasingly, the world is splintering into national or regional internets, governed by different norms and rules and incorporating democratic and authoritarian characteristics.

In 2021 alone, a slew of countries, many of them democratic, have adopted restrictive digital regulations more at home in authoritarian states. In June, for example, Nigeria banned Twitter from operating in the country. The reason was that Twitter had removed a tweet from President Muhammadu Buhari that the company claimed violated its community guidelines. In response, the government accused Twitter of "undermining Nigeria's corporate existence" and outlawed the service. Meanwhile in India, the government decreed in February that all online media outlets and video-content providers were required to appoint local representatives to respond to every government complaint within fifteen days. The law also authorized state officials to censure or delete content that crossed certain lines. Several months later, Prime Minister Narendra Modi became so incensed after Twitter labeled a post from his ruling Bharatiya Janata Party "manipulated media" that he authorized a special forces raid on the company's offices. Similarly, the governments of Turkey, Uganda, the Philippines, and Indonesia have cherry-picked regulatory approaches to create distinctive local versions of the internet—whether incorporating social media taxes and localization requirements or enacting burdensome content restrictions. More recently, Russian authorities have refined a new tactic—demanding that Apple and Google remove programs from their app stores linked to opposition leaders—ahead of Duma elections.

These trends cause growing concerns about how technology, politics, and state authority will evolve. Can democracies strike an appropriate balance between safeguarding their societies from dangerously polarizing online rhetoric while maintaining commitments to protecting free expression? Can democratic leaders reach consensus about how to address core policy problems such as establishing coherent rules about personal data protection and privacy, devising guidelines for the responsible use of emerging technologies like facial recognition, or finally reining in Big Tech's excessive market and surveillance power? What will be China's influence on technology and data governance, and will its efforts to rewrite cyber norms allow digital authoritarian approaches to gain ground? Can civic activists, independent journalists, and human rights advocates continue to find innovative ways to push back against government repression using new tools, tactics, and technologies? The answers to these questions are not foretold—all of them represent major areas of contestation.

While policymakers seek resolutions to these pressing questions, they can benefit from the ground-level insights of experts, scholars, researchers, and activists. The Carnegie Endowment for International Peace has assembled the Digital Democracy Network—a diverse group of cutting-edge thinker-activists engaged in work on technology and politics. The network aims to facilitate cross-regional knowledge sharing, support collaborative strategies to pressing problems, and investigate previously unknown and emerging questions in the field. This report represents the network's first effort to describe challenges to governance posed by digital technology.

This collection highlights four themes.

First, it focuses attention on the COVID-19 pandemic and evaluates national and regional responses to the disease. Experts are divided about the long-term political consequences of the pandemic. Groups such as Freedom House, International IDEA, and International Center for Not-for-profit Law (ICNL) document how surveillance overreach, data and privacy vulnerabilities, media suppression, content restrictions, and emergency decrees have challenged democratic institutions and undermined civil liberties. ICNL, for example, reports via its COVID-19 Civic Freedom Tracker that through September 2021, 109 countries had issued emergency declarations, 57 had instituted measures that impact freedom of expression, 150 had implemented restrictions on freedom of assembly, and 60 had enacted restrictions on privacy.

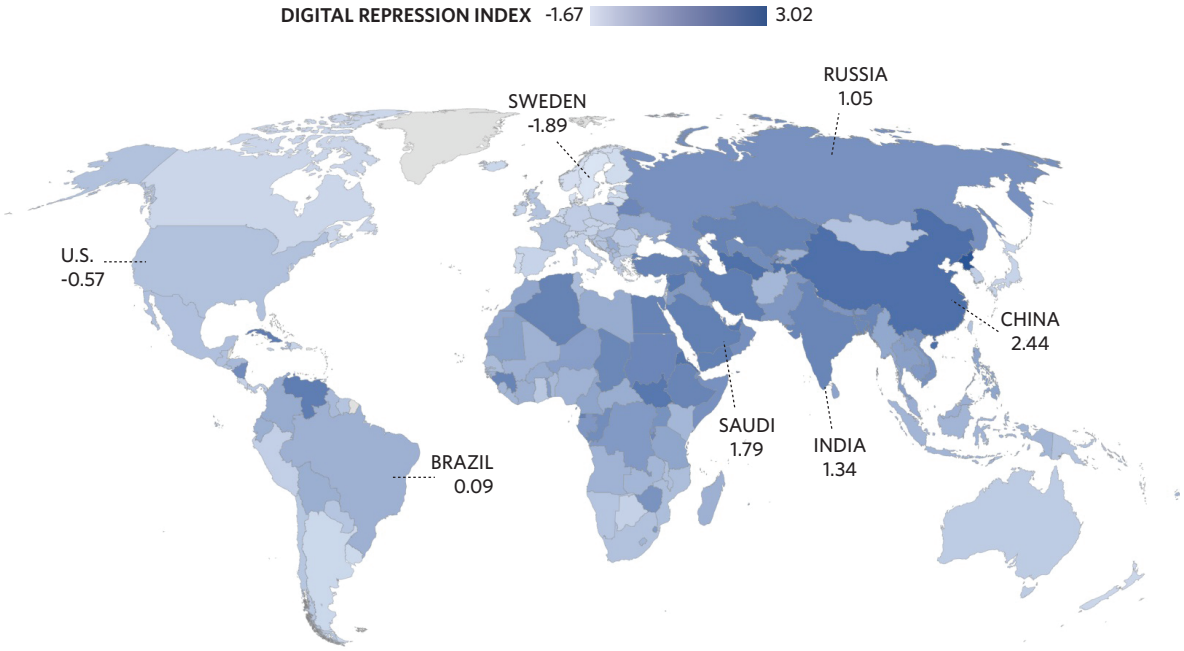
Other organizations, however, paint a less grim picture. Researchers from the Varieties of Democracy project write: "The COVID-19 pandemic has registered several wins and losses for democratic standards. While high-income Western democracies have generally performed quite well, several low and lower-middle income countries stand out for their innovation and advances." They note that the most serious democratic violations have tended to occur at the beginning stages of the pandemic and that the number of restrictions has declined over time. They observe that courts have pushed back successfully against overreach by executive branches, that certain countries have managed to avoid discrimination while establishing safe COVID-19 protocols, and that a number of states have successfully countered public health misinformation while avoiding broader media restrictions.

But, even if certain countries are witnessing recent governance improvements, several concerning trends stand out. One, in countries already prone to repression, the pandemic has given greater license to governments to enact additional restrictions on citizens' liberties. Countries like China, Russia, Saudi Arabia, Thailand, and Turkey have pursued a mix of new surveillance technologies and legal directives that have significantly constrained freedom of association and expression. Two, governments have used the threat of disinformation as a pretext to persecute under "fake news" statutes scores of individuals, many of whom happen to be civil society activists and political opposition figures, while at the same time these governments have expanded their own public health disinformation efforts. State disinformation follows one of three lines: **denialist** (governments discredit or deny reports of outbreaks in their countries), **anti-science** (authorities minimize COVID-19 dangers while rejecting accepted medical recommendations), and **curist** (leaders promote unfounded treatments for the virus—such as Brazil's President Jair Bolsonaro's endorsement of hydroxychloroquine).

Members of the Digital Democracy Network offer their own perspectives about the meaning and import of the COVID-19 pandemic. Janjira Sombatpoonsiri, affiliated with Chulalongkorn University and the German Institute for Global and Area Studies (the GIGA) and Sangeeta Mahapatra, also with the GIGA, provide a case-study analysis of COVID-19 restrictions in Southeast Asia. 'Gbenga Sesan, executive director of Nigeria's Paradigm Initiative, turns his eye to sub-Saharan Africa, where he finds a similar pattern of COVID-19-related digital abuses occurring in Kenya, Nigeria, and Zambia. Irene Poetranto and Lotus Ruan, researchers affiliated with the University of Toronto's Citizen Lab, present a global overview of new technologies adopted in response to the pandemic. They examine the cost of countries' growing reliance on advanced digital tools in public health and where this reliance might lead.

Second, network members describe how authoritarian regimes are employing new technologies to strengthen their rule and counter opposition and civic challenges. An expanding set of countries are relying on facial recognition technology, big data analytics, predictive policing techniques, and Safe City systems to enhance their security capabilities. The latest data from the Digital Society Project, updated to include 2020 statistics, continues to show a close relationship between authoritarian regimes, constraints on political freedoms, and corresponding government reliance on digital repression techniques. As Figure 1 shows, countries with the greatest prevalence of surveillance, censorship, internet shutdowns, and disinformation include authoritarian stalwarts like China, Russia, Iran, and North Korea, members of the Gulf Cooperation Council, and countries in Central Asia and the Horn of Africa. Conversely, Europe and the Americas display reduced levels of digital repression.

Figure 1. Global Distribution of Digital Repression in 2020



Source: Valeriya Mechkova, Daniel Pemstein, Brigitte Seim, Steven Wilson, Digital Society Project Dataset v3, 2020.

Note: 0 = Global Mean. This figure charts experts' survey responses on their perceptions of how prevalent digital repression is in a given country but do not represent quantitative tallies of specific incidents.

The analysis in this section explores different aspects of these repression trends. They ask: Why do states choose to adopt advanced technologies from authoritarian sources? What technological methods are Gulf states using to enact their political agendas? What can civil society make of the growth of internet shutdowns and social media blockages around the world? How are Myanmar's armed forces incorporating digital techniques as a means to enforce troop loyalty and maintain their control over the country?

Akin Unver, an associate professor of international relations at Turkey's Özyeğin University, argues that economic considerations, rather than geopolitical or ideological preferences, are more relevant in determining whether countries will source artificial intelligence technologies from China or from democratic states. Afef Abrougui, affiliated with the Social Media Exchange, writes about the adoption by Gulf Cooperation Council countries of a wide range of repressive measures. She emphasizes that high-tech tools not only support their political objectives but are also crucial for future economic growth. Jan Rydzak, affiliated with Ranking Digital Rights, describes the increased use of internet shutdowns to suppress dissent and block communications. He warns that government disdain for international human rights principles "is pushing resistance to the breaking point." Sarah Gordon, a research assistant at Carnegie, profiles how Myanmar's military is spreading online propaganda to reinforce troop loyalty, identify dissent, and isolate soldiers from the outside world.

The third section tackles problems of disinformation. Disinformation has become the tool of choice for many illiberal regimes, such as those in Brazil, Hungary, and the Philippines. They seek to manipulate public opinion to remain in power but are wary of instituting harder-edged repressive methods. In liberal democracies, meanwhile, the threat of disinformation increasingly stems from extreme political movements, particularly far-right groups, which harness social media to propagate falsehoods, spread conspiracy theories, and foment polarization and identity politics. Disinformation strategies involve common tactics: disseminate false narratives (whether pro-government propaganda, anti-vaccine conspiracies, or #StoptheSteal election claims), flood social media channels with competing or distracting information that overwhelms legitimate information sources, and deliberately post offensive content online to provoke or disrupt conversations.

In response to the deluge of misinformation, disinformation, and hate speech, governments have started cracking down on platforms—requiring companies to remove unacceptable content faster. Some governments, such as India's, only give platforms twenty-four hours to remove "manifestly unlawful" content. The EU has adopted an even stricter rule for terrorist content—platforms have one hour to remove offensive material. Many countries have also weakened or discarded intermediate liability protections for platforms. This is an understandable reaction in liberal democracies reeling from false and polarizing content. However, more cynical autocratic regimes have seized upon the opening this trend presents and classified any content critical of their agendas as "fake news" and subject to removal.

A bigger question is how much governments should hold platforms responsible for facilitating the spread of bad information. The evidence is murky, particularly in liberal democracies, about whether the surge in polarizing content is primarily a consequence of social media. While platforms provide useful targets for regulators eager to make a dent in disinformation, new research indicates that false information spreads due to a complex interaction between them and mainstream media outlets. It is insufficient to blame Facebook or Twitter's poor leadership for the much more complicated proliferation of politically motivated falsehoods.

Agustina Del Campo, who heads the Center for Studies on Freedom of Expression and Access to Information at the University of Palermo in Argentina, contends in her contribution that policymakers have been too quick to label disinformation as a new category of social harm—discarding prior consensus

about what constitutes legal speech. She argues that the very notion of distinguishing and taking down disinformation is premised on the shaky assumption that a "single authoritative source" exists "against which all information can be assessed for truth." Jonathan Corpus Ong, with the University of Massachusetts Amherst, explains how the internet has accelerated the spread of hate speech against minority communities. He explores the growing levels of disinformation and hate speech targeted against Asian American and Pacific Islander communities in the United States.

The fourth section presents case studies from two influential countries: India and Indonesia. As two of the world's largest democracies, both have experienced an illiberal resurgence in recent years. They represent crucial areas of struggle when it comes to determining whether information and communication technologies can enhance good governance or whether they will intensify polarization, identity politics, and autocratic control. Arindrajit Basu, a researcher in India's Centre for Internet and Society, emphasizes the importance for democracies like India to facilitate uncomfortable conversations around the rule of law and human rights at home in order to geopolitically compete against autocratic adversaries. Sinta Dewi Rosadi, a scholar at Padjadjaran University in Indonesia, scrutinizes digital privacy in that country. She observes that Indonesia's patchwork of regulations related to surveillance and data privacy has frequently resulted "in the denial of transparency and due process to Indonesian citizens."

These varying global perspectives shed light on emerging areas of contestation and highlight the complexities, urgency, and dangers involved in the advance of digital technologies and their effects on politics globally. The hope is that their contributions will help policymakers connect local perspectives with global concerns, and that it will bridge the research gap between international conversations taking place in capitals and local realities on the ground that are driving specific trends. Over time, Carnegie expects the network to generate new ideas that will influence relevant policy conversations—whether coming up with innovative approaches to strengthening digital safeguards, offering new regulatory models for the responsible governance of emerging technologies, or confronting concerning policies related to the COVID-19 crisis.

Steven Feldstein is a senior fellow in Carnegie's Democracy, Conflict, and Governance Program.

COVID-19 Intensifies Digital Repression in South and Southeast Asia

JANJIRA SOMBATPOONSIRI AND SANGEETA MAHAPATRA

Before the COVID-19 pandemic, several countries in Asia had experienced rising levels of autocratization and digital repression as governments leveraged digital technologies to stifle online dissent and surveil critics. The pandemic, however, could deepen governments' capacities for digital repression. Recent developments in South and Southeast Asia offer insights about this worrying trend.

The trend toward "lawfare"—the abuse of laws to criminalize oppositional civil society and generate a chilling effect to achieve self-censorship—emerged in South and Southeast Asia long before the pandemic. Provisions condemning defamation, sedition, and public assembly have been instrumental in suppressing pro-democracy voices for years in established autocracies such as Vietnam, increasingly authoritarian regimes such as in Cambodia and Thailand, and democracies like India. In the past decade, computer- and cyber-related laws have added a new ingredient to this cocktail of legal repression. In Thailand, for instance, social media users have been charged under the Computer Crime Act for online speech offending the royal family. In India, Section 66a of the Information Technology Act have empowered the authorities to censor posts and websites or to arrest citizens for any online content deemed offensive or inciting.

Table 1 lists examples of these laws and their respective dates of enactment in South and Southeast Asian countries.

COVID-19 has spurred governments in South and Southeast Asia to accelerate the weaponization of these laws—particularly to punish critics under the guise of combating "fake news." For instance, between January and March 2020, the police in Vietnam took action against 654 cases of purported fake news and sanctioned 146 people, including a dissident publisher. In Cambodia, by April 2020, around thirty activists and opposition members had been detained on the charge of spreading "fake

Table 1. New Laws Enabling Online Censorship in South and Southeast Asia

Country	Law	Year of Enactment
India	Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules (executive rule)	2021
Nepal	Information Technology Bill	2020
Pakistan	Citizen's Protection (Against Online Harm)	2020
Singapore	Protection from Online Falsehoods and Manipulation Act	2019
Sri Lanka	False News Bill (draft)	2019
Thailand	Cybersecurity Law	2019
Bangladesh	Digital Security Act	2018
Malaysia	Anti-Fake News Act	2018, revoked in 2019, reintroduced in 2021
Vietnam	Cyber Security Act	2018
Thailand	Amended Computer Crime Act	2016
Laos	Law on Prevention and Combating Cyber Crimes	2015
Bangladesh	Section 57 of the Information Technology and Communication (ICT) Act	2013
Myanmar	Telecommunications Law	2013
Singapore	Internet Code of Practice	2013
Philippines	Cyber Crime Prevention Act	2012
Cambodia	Cyber Law	2012
India	Sections 66A and 69A of the Information Technology (Amendment) Act	2008
Indonesia	Electronic Information and Transaction Law	2008
Sri Lanka	Computer Crime Act	2007
India	Section 54 of Disaster Management Act	2005

news" about COVID-19. In Singapore, alleged spreaders of "fake news"—including political rivals of the government and independent journalists—were targeted under the Protection from Online Falsehoods and Manipulation Act. In Malaysia, the government used a health emergency decree as a pretext to revive a "fake news" bill that had been revoked in 2019. In Indonesia, one of the region's last-standing democracies, the government arrested citizens, including a West Papuan pro-independence leader, for spreading supposedly false information.

The state of digital rights is not looking any better in South Asia. In India, hastily introduced executive rules gave the government sweeping new powers over digital content, curbing peoples' rights to free speech and privacy. Following a devastating second wave of COVID-19 infections, these rules enabled the broadening of the definition of disinformation to include criticism of the government. Subsequently, user

posts were taken down on Twitter, Facebook, and Instagram. At least fifty-five journalists who reported on COVID-19 were attacked or arrested in 2020, a number that has climbed since then. In Sri Lanka, the police arrested multiple individuals who criticized the government's response to the pandemic on social media. Similarly, in Bangladesh, the government exploited the Digital Security Act to crack down on journalists critical of its overall corruption and management of the health crisis.

The pandemic has increasingly normalized the deployment of facial recognition technology by governments in the region and increased the prospects of mass surveillance by legitimizing invasive measures on public health grounds. These developments present a special risk in countries that lack institutional checks against the misuse of digital surveillance. COVID-19 has enabled states to reformulate public health surveillance as law-and-order issues; in Singapore, for example, the authorities now use data collected from a contact tracing app in criminal investigations. Many such surveillance measures lack sunset clauses, thereby establishing new norms for states to control their citizens through their data.

Janjira Sombatpoonsiri is an associate at the German Institute of Global and Area Studies (the GIGA) and researcher at the Institute of Asian Studies at Chulalongkorn University in Thailand.

Sangeeta Mahapatra is a visiting fellow at the GIGA.

COVID-19 Digital Restrictions in Africa

'GBENGA SESAN

As lockdowns started in response to the spread of COVID-19 in 2020, it was clear that flattening the curve would require quick action, including massive data collection and the implementation of quarantine laws. However, it was also apparent that some governments would use the pandemic as an opportunity to clamp down on dissenting voices. This presented a dilemma for human rights and data protection advocates, who demanded that all actions taken by governments restricting individual liberties be lawful, proportionate, and necessary. My organization, Paradigm Initiative, documented the problematic measures taken by governments around Africa in the name of combating COVID-19 in our annual digital rights and inclusion report, Londa.

Several African governments used the pandemic to restrict political rights and repress opposition parties. For instance, Ethiopia passed state-of-emergency legislation that permitted the "suspension of rights . . . to counter and mitigate the humanitarian, social, economic, and political damage that could be caused by the pandemic." This authorization to restrict the rights of citizens raises many red flags in a country with a record of political repression. Across the continent, Cameroon's minister of territorial administration demanded that telecommunications providers MTN and Orange close the mobile money accounts of an opposition party fundraising to support citizens affected by the pandemic. Meanwhile, Togo launched a digital financial assistance program using its electoral database rather than its complete registry of citizens, thus excluding activists who had refused to vote in the elections in protest of the autocratic regime and depriving them of welfare during the pandemic.

Beyond conventional political repression, Africa witnessed an increasing amount of digital repression during the pandemic. Nigeria is a case study of these trends. The minister of communications and digital economy announced that the government was mining SIM card registration data without user consent to identify the poorest Nigerians in order to direct financial aid during the pandemic. Officials also

announced plans to apportion relief funds using biometric information linked to bank accounts and confidential data provided to mobile networks, violating the digital privacy of citizens.

In Kenya, there were numerous allegations that the government was tracking the mobile phones of citizens subjected to mandatory fourteen-day COVID-19 quarantines. In one complaint, a citizen under quarantine received a call from a National Intelligence Service (NIS) official warning her as she was walking toward a local market to turn around and return home. She reported that "COVID-19 patients live in constant fear while in private confinement and do not have an assurance about the protection of their privacy." This example illustrates the pervasiveness of monitoring in Kenya carried out by the NIS in conjunction with health agencies.

Other nations across Africa have used the pandemic as an excuse to crack down on online media and freedom of expression. In April 2020, Zambia's Independent Broadcasting Authority canceled the license of an independent television station after it refused to broadcast the government's COVID-19 messaging for free. Tanzania's government similarly suspended Kwanza Online TV's license after its Instagram account shared information from the U.S. embassy about the elevated risk of contracting COVID-19 in the country. Zimbabwe's government enacted even more sweeping measures, restricting freedom of expression and enabling defamation lawsuits against journalists and individual citizens.

Such repressive actions during the pandemic have not been unique to African countries. However, the introduction of vague provisions targeting dissenting voices, the suspension of independent media licenses, and the implementation of politically and digitally repressive measures are all indicative of broader trends that shrink civic spaces in African countries. As they begin to plan for life beyond the pandemic, it will be important to avoid a scenario in which the new normal preserves laws silencing dissenting voices or actions targeting civic spaces in the name of public safety.

'Gbenga Sesan is the executive director of Nigeria's Paradigm Initiative.

Intrusive Surveillance After the Coronavirus Pandemic

IRENE POETRANTO AND LOTUS RUAN

In response to the COVID-19 pandemic, countries around the world were quick to use various surveillance technologies to help mitigate the virus's spread, from drones monitoring crowds to enforced social distancing reliant on app-based contact tracing. But intrusive surveillance has not resulted in countries ending the pandemic. Instead, such powerful capabilities have left the door open to future human rights violations. Civil society can expect governments to justify using digital surveillance beyond the pandemic as a means to protect national security, implement governance priorities, and serve future public health interests. What is the cost of states' growing use of these tools?

Historically, governments have used national security and public safety concerns to legitimize surveillance. They typically introduced new surveillance measures during times of crisis or leading up to the start of major sporting events. The Olympic Games, for example, are known for catalyzing heavy surveillance. The security measures for the 2016 Summer Olympics in Rio de Janeiro, Brazil, included installing 2,000 high-resolution cameras in the areas near the competitions. Following the September 11 terrorist attacks in the United States, governments worldwide similarly broadened the surveillance mandates of state agencies and law enforcement.

Surveillance has become a central component of a digitally repressive governance model. The authorities in China have installed an array of digital surveillance technologies in nearly all subway stations across the country, including 5G-powered facial recognition systems and deep-learning-enabled luggage scanners. The motivation to monitor and predict "suspicious behaviors" has also led to a booming surveillance industry based on discredited pseudoscience, such as "emotion recognition" technologies. As the domestic market has reached saturation, Chinese companies have expanded internationally, especially to countries strategically important to China. China alone cannot be blamed for proliferating surveillance technologies to aid the functions of repressive governments, however. Western nations have historically

developed backdoors to technology to allow for government intrusion. Democratic governments have also allowed companies to export these capabilities throughout the world with few restrictions, including to governments with poor human rights track records (as the Pegasus Project investigation shows).

An emerging risk is that governments will extend public health measures to digitally track the locations and biometric data of citizens. From March to May 2020, Israel's Shin Bet intelligence service used tracking technologies commonly employed in counterterrorism operations for contact tracing. South Korea, meanwhile, has established one of the most extensive contact tracing systems in the world, with authorities gathering data using credit card transaction logs, mobile phone location tracking, and closed-circuit television footage. Local governments and private companies in China also proudly demonstrated their abilities to locate cases of possible close contacts with the help of big data, without explaining how relevant data were collected, analyzed, and stored.

The negative implications of pervasive surveillance and personal data collection, even in situations of public health, are clear. There have been COVID-19-related data breaches in China and Israel, and the scope of publicly available data in South Korea has raised privacy concerns. Proper oversight and accountability measures are needed to safeguard citizens' privacy and security, including detailing for how long data is gathered, stored, and used, as well as who has access to it, to reduce the potential for abuse and avoid mission creep.

Irene Poetranto is a senior researcher at the Citizen Lab, based at the University of Toronto's Munk School of Global Affairs and Public Policy.

Lotus Ruan is a researcher with the Citizen Lab, based at the University of Toronto's Munk School of Global Affairs and Public Policy.

Motivations for the Adoption and Use of Authoritarian AI Technology

AKIN UNVER

In the last decade, U.S. policy discourse around the adoption of artificial intelligence (AI) technology has largely been framed in the context of great power competition with China. However, for most of the rest of the world, AI technology is better understood as an issue of economic development determining a country's relative standing in the global technology race rather than as a geopolitical or ideological preference. What democratic countries must understand is that developing countries value affordability and accessibility over an AI provider's ideology. Whether the technology comes from China rather than Europe or the United States matters very little if Western technology is prohibitively expensive. Furthermore, if the United States and Europe want to overtake China as the world's leading provider of AI technologies and spearhead a more democratic global AI movement, they have to structure this technology provision as part of a more inclusive and imaginative global economic model that provides tangible and realistic developmental goals in addition to liberal norms.

There seems to be a mismatch between the level of concern about Chinese technology partnerships and existing research into why democracies adopt AI technology from authoritarian sources. On the one hand, it is well established that China has successfully expanded its influence by cooperating with democratic countries and spearheading AI partnerships through its Belt and Road Initiative (BRI). In 2019, a Lowy Institute report indicated that 126 countries and twenty-nine international organizations had signed more than 3,000 high-technology cooperation agreements under the BRI framework. What is less understood, however, is why established democracies like Austria, Ireland, and the Netherlands have joined more authoritarian countries in partnering with China, and whether the United States or EU could provide similar high-technology partnerships with developing nations. In order to answer these questions, democratic nations need to understand the variegated factors that cause a country to purchase Chinese AI technologies over Western alternatives.

China's success in proliferating advanced technology is premised on supplying affordable products. For instance, a country's adoption of AI technology is dependent on first acquiring expensive hardware, such as large networked storage clusters and advanced processing units. What is more, if China can provide such hardware at an affordable price, this can affect the behavior of the purchasing state's allies and rivals. Its allies, for instance, may inform each other about low-cost sources from which to secure technologies to achieve shared military or economic objectives. Less obviously, its rivals may also turn to the same suppliers of affordable technology in order to swiftly acquire competing capabilities and resolve their security dilemma. In other words, if a state sees its rival acquiring affordable AI components, it will perceive the disparity between them as a relative capabilities issue and will seek to acquire similar low-cost technologies from the same source. This dynamic reflects the fact that first adopters of new and affordable technology tend to drive the technology's adoption by other states in the same region.

These tensions over the security dilemma and relative capabilities issues of AI adoption mean that concerns about relying upon Chinese "authoritarian tech" are less relevant. This will remain true as long as the sources of democratic norms—Western nations—are unable to provide digital infrastructure to developing nations at a reasonable cost. This in turn could reinforce the bureaucratic consolidation of authoritarian technology adoption, meaning that authoritarian suppliers may monopolize the diffusion of AI technologies to all but the most liberal democratic countries. Such an imbalance could limit regional norm-building for future AI technology development and usage.

Western nations also risk charges of hypocrisy for denouncing sales of Chinese AI technology even while wealthy European countries have announced plans to purchase high-tech Chinese infrastructure. According to a February 2021 Council on Foreign Relations report, while Poland, Sweden, and the United Kingdom have formally banned Huawei from involvement in their 5G networks, Belgium and France are allowing the use of Huawei equipment with certain conditions. Meanwhile, Austria, Hungary, Ireland, and the Netherlands intend to acquire Chinese 5G networks and infrastructure. These divergences significantly hamper the EU's ability to serve as a "norm superpower" that touts its legal and ethical standards-defining edge over the United States and China.

The United States and the EU have announced the formation of a joint Trade and Technology Council, building on momentum from June's G7 summit. This partnership could work to emphasize norm building in quantum computing, AI, and 5G networks. President Joe Biden's infrastructure plan may boost the United States' capacity to challenge China's trade power if passed. However, it appears unlikely that a U.S.-led or EU-led global movement can successfully counteract China's dominant position in selling AI technology to countries with lower technological bases unless they can offer credible, realistic, and affordable alternatives. In the near term, global scholarship should explore how developing countries can build transnational economic infrastructure systems that incentivize the development of ethical AI and the adoption of algorithmic best practices, while addressing affordability concerns.

Akin Unver is an associate professor of international relations at Özyeğin University in Istanbul.

Digital Authoritarianism in the GCC and Its Broader Regional Consequences

AFEF ABROUGUI

For the autocratic monarchies of the Gulf Cooperation Council (GCC)—Bahrain, Kuwait, Oman, Saudi Arabia, and the United Arab Emirates (UAE)—technology has served for many years as an enabler of digital oppression. Their go-to digital oppression toolbox includes internet filtering and censorship software, surveillance spyware, and bots disseminating state propaganda and disinformation. Beyond using technology as a tool to control dissent and maintain power, the GCC countries are also betting on the technology sector to help drive economic development as they embark on ambitious plans to diversify their hydrocarbon-dependent economies.

The UAE and Saudi Arabia in particular have emerged as key players driving investments in the tech sector, including in international tech companies. But, given their abysmal human rights records, their growing influence over the international tech industry is bad news for human rights and democracy in the Middle East and North Africa. Both countries have a record of deploying tech to wage disinformation campaigns and surveillance operations to bolster autocratic regimes and their allies across the region. Saudi Arabia is notorious for abusing technology to repress its population, crack down on dissent, and serve its interests across the region. Its intelligence services have allegedly infiltrated Twitter using spies and gained access to the personal information of dissidents. They used spyware from Israeli firm NSO Group to surveil the communications of journalist Jamal Khashoggi before he was assassinated and dismembered by agents acting upon orders from Crown Prince Mohammed bin Salman, the country's de facto ruler.

The UAE also has a poor track record. In 2019, for example, together with Egypt, it waged a social-media disinformation and propaganda campaign in support of Sudan's military and its leaders. This occurred just days after a crackdown that killed at least one hundred protesters taking part in a pro-democracy sit-in demanding an end to military rule.

The GCC countries have also demonstrated willingness to use their collective power to suppress human rights and freedom of expression toward geopolitical ends. This was manifest during the Gulf diplomatic crisis, in which Saudi Arabia, the UAE, Bahrain, and Egypt cut diplomatic ties with Qatar and imposed an embargo on the country for its support to the Muslim Brotherhood and its ties with Iran. The digital research laboratory Citizen Lab found that Saudi Arabian and Emirati operators hacked the iPhones of thirty-six journalists working at Qatari-funded Al Jazeera using spyware from NSO Group (Al Jazeera's reporting has long been an irritant to governments in the region). This digital assault, occurring in the midst of the crisis, sent a pointed and intimidating message to journalists operating in Qatar. These actions could be a harbinger for further human rights abuses if Saudi Arabia and the UAE cement their status as lead sponsors of technological development in the region.

Poor human rights records have not deterred international tech companies from doing business with Gulf states and other actors in the region. This is largely because, in addition to their high internet penetration rates and large investments in information and communication technology infrastructure, the GCC states are home to sovereign wealth funds, high-net-worth investors, and national companies looking to invest in the technology sector. For example, in 2020, Saudi Arabia's Public Investment Fund invested $3.5 billion in Uber, and the UAE's Mubadala invested $75 million in Telegram this year.

Most recently, Google announced an agreement with Saudi Arabia's oil giant Aramco to establish a Google Cloud regional platform in the country. Human rights groups have denounced the plan over concerns that establishing "one of the largest data storage and cloud computing services in the world" brings significant human rights risks, in light of Saudi Arabia's documented censorship and surveillance interests.

As GCC countries become more interested in the opportunities technology offers for economic diversification and development, their influence in the tech industry will continue to increase. This is particularly true for the UAE and Saudi Arabia, which have emerged as leaders in the GCC for investing money in international technology companies and incentivizing them to launch operations in the region. Given their records of exploiting technology to control dissent and advance their geopolitical interests, such investments have serious implications for human rights and pro-democracy movements not only in the Gulf but also across the Middle East and North Africa.

Afef Abrougui leads research at the Social Media Exchange, a digital rights NGO in the Arab region.

A Tightrope Over the Shadows: Grim Prospects in the Fight Against Shutdowns

JAN RYDZAK

In 2019, for the first time, a majority of the world's population was able to access the internet. But just as humanity had crossed that threshold, governments worldwide set an appalling record of their own, shutting down the internet and communication networks more frequently than ever before. The COVID-19 pandemic soon created a tapestry of overlapping crises that throttled access to critical health information. Civil society, researchers, investors, and much of the private sector agree that shutdowns flout a litany of human rights, sabotage local and national economies, and routinely fail to achieve their stated goals. Nonetheless, there is mounting evidence that the human rights community is losing ground.

Shutdowns have evolved from shambolic tactics to strategic instruments used alongside an array of other repressive tools. As governments have diversified their tactics, they have also dialed up the hostility of their discourse. Officials often justify today's network shutdowns by decrying the "arrogance" and alleged political favoritism of social media companies, denouncing how platforms undermine the "sovereignty and integrity" of the nation, and emphasizing that communication networks threaten the "corporate existence" of the countries in which they operate.

The increasingly adversarial relationship between governments and platforms is complemented by another trend: the hijacking of arguments formulated by the digital rights community. In rationalizing recent blackouts and regulatory moves to tame social media, the governments of India and Nigeria, for example, have accused platforms of spreading misinformation, a frequent charge leveled by advocacy groups. Using this language cloaks repressive government actions with a semblance of legitimacy. But these warning shots are being leveled not just at social media giants, but at all tech companies operating in those countries, especially firms that provide critical communications infrastructure for millions of people.

Taken to an extreme, governments' disdain for international human rights norms and their defiant stance against open communications networks is pushing civic resistance to the breaking point. One example is the announced withdrawal of the Norwegian telecommunications firm Telenor from Myanmar this year. Unlike Myanmar's other three operators, the company had vocally opposed internet shutdowns for years and taken steps to mitigate their impact. When the military junta seized power in February, however, Telenor faced the prospect of carrying out orders in support of a nationwide digital siege while presumably under a gag order. Ultimately, the company sold its operations in Myanmar to an investment group with a dubious human rights record with no indications of due diligence in this regard. In executing the sale, Telenor transferred user data for 18 million individuals to an entity that had made no commitment to protect it, virtually ensuring future erosions of digital rights. Telenor's retreat has sent an unfortunate signal that resistance to shutdowns is futile—at least when dealing with committed authoritarian regimes.

To make matters worse, few governments have presented any evidence about the necessity for carrying out shutdowns, nor demonstrated accountability for their impact. India's telecom suspension rules of 2017, for instance, are often completely ignored. Shutdown orders worldwide are rarely made public. High-level declarations, such as the G7 Open Societies statement, also provide little reason for optimism; under pressure from the Indian government, the communiqué only condemned "politically motivated" shutdowns, perpetuating the false notion that a country could shut down the internet for matters of law and order separate from political motivation. These loopholes will allow scores of internet blackouts to continue.

Yet, there are glimmers of hope. International civil society has maintained a relentless focus on preventing shutdowns and keeping them in the spotlight. Individual groups and diverse coalitions alike have scrutinized companies' shutdown policies, issued collective statements ahead of contentious elections, thrown their weight behind legal interventions, blown the whistle using traffic measurement tools, and exposed government-mandated killings that blackouts had concealed. The United States has also been outspoken in increasing diplomatic pressure against countries regularly shutting down the internet. Furthermore, the recent ruling by the Court of the Justice of the Economic Community of West African States against Togo regarding its 2017 shutdowns creates a strong precedent for successful litigation. Nonetheless, for every time a government is held accountable for its actions, dozens of its peers continue to plunge their citizens into darkness with little consequence. With millions of lives on the line, continued pushback against shutdown-prone governments must be an urgent priority for the international community.

Jan Rydzak is the company and investor engagement manager at Ranking Digital Rights.

Using Technology to Preserve Military Loyalty: The Tatmadaw in Myanmar

SARAH GORDON

Technology has emerged as a crucial factor in political struggles around the world, playing an outsized role in helping regimes maintain power. A recent manifestation of this dynamic has emerged in Myanmar, where the military, known as the Tatmadaw, seized power in a coup in February. For its leaders, a key component to sustaining the coup is to prevent soldier desertions. To that end, they are using digital tools to spread online propaganda to strengthen soldiers' resolve, to identify dissent in the ranks, and to sequester troops from the outside world.

An insular and paranoid organization since its founding, the Tatmadaw has always prioritized building an isolated and segregated information ecosystem in order to enforce organizational unity among its members. Senior operatives skilled in psychological warfare routinely spread disinformation and conspiracy theories in Facebook groups frequented by soldiers. Even before the military coup, generals had regularly used Facebook to incite ethnic violence against Muslim Rohingya. The Tatmadaw's viral disinformation campaigns and online coordination sparked mass killings and genocide against the group. More recent disinformation campaigns have portrayed opposition groups protesting the military takeover as a "Muslim cabal" attempting to destroy the Buddhist faith or as George Soros-backed Westerners aiming to undermine the country. Interviews reveal that this onslaught of propaganda has led most soldiers to believe that their country will crumble without their intervention. Online disinformation in Myanmar is so pervasive that Facebook announced it was shutting down Tatmadaw news pages and leader accounts due to the proliferation of false and inciting material.

But the Tatmadaw's digital strategy is not limited to spreading disinformation. Another tactic is the deployment of surveillance technology. Soldiers and their families live in military compounds, allowing their superiors to scrutinize their every move. Soldiers' online activities are under constant surveillance by overseers, who monitor Facebook groups for any sign of dissent. In combination with the Safe City

technology—which tracks individuals' movements—installed by Huawei in the capital, Naypyidaw, these digital tactics allow officers to identify and root out dissent, and they exert a chilling effect on all soldiers.

The Tatmadaw also deploys internet shutdowns to restrict soldiers' online access. While shutdowns are used by regimes around the world to deprive protesters of tools to organize and share information with the outside world, reporting suggests that the Tatmadaw's internet stoppages have soldiers in mind. In particular, the blackouts are designed to stop them from questioning orders, planning defections, or witnessing abuses committed by fellow soldiers. Without the internet, soldiers have been forced to rely upon their commanders and state media as gatekeepers for information.

However, despite a decades-long investment in building a closed digital environment, the Tatmadaw is far from infallible, in part because Myanmar lacks the resources of more advanced digitally authoritarian nations such as China. Civil society has had success in engaging the Tatmadaw in a game of technological cat and mouse. Civilians have developed significant technical skills over the past decade and are able to nimbly adapt to internet restrictions, using their grassroots digital capabilities to build solidarity with other protest movements in Southeast Asia and to even to doxx Tatmadaw members and their families. However, while social media appears to have influenced the few soldiers who have deserted, meaningful defections have yet to occur, showcasing the powerful combination of online indoctrination, surveillance, and shutdowns.

While analyses of digital repression frequently focus on state usage of technology to suppress citizens and maintain power, the coup in Myanmar presents a unique example of a military using digitally repressive techniques to preserve organizational cohesion. The Tatmadaw case offers insights into the lengths to which militaries in the digital era may go to deter defections and withstand pressure from outside actors.

Sarah Gordon is a research assistant at the Carnegie Endowment for International Peace.

Disinformation is Not Simply a Content Moderation Issue

AGUSTINA DEL CAMPO

When the World Health Organization declared an "infodemic" in the midst of the COVID-19 pandemic, it signaled that the spread of health disinformation had become a global concern. Countries have taken different approaches to addressing disinformation in this and other contexts. Some, like Singapore, have enacted formal legislation; others, such as Argentina, have prosecuted individuals for disseminating fake news as a "crime against public order." But mostly, there has been increased pressure on internet companies, particularly social media platforms, to monitor, identify, and filter "untruthful" content circulating on their networks. The willingness of these companies to accommodate the new demands constitutes a paradigm shift.

This paradigm shift has been generally welcomed around the world and has become an important focus of civil society and academia. Many of the solutions proposed by policymakers and platforms, however, represent quick fixes, such as removing or blocking harmful content from heads of state, labeling expressions from public officials, or prohibiting content that contradicts official sources of information. Notwithstanding the effectiveness (or lack thereof) of these measures, they entail a fundamental break with existing standards and represent a shift in how states assess the value of free speech and the free flow of information and ideas for democratic self-governance.

Defining what constitutes disinformation and how to prevent its spread is complicated and requires special consideration. Disinformation is ill-defined and is different from other targets of content moderation—like hate speech, threats, or fraudulent activity. First, disinformation seemingly represents the introduction of a new social harm. Second, it encompasses different types of falsehoods and therefore differently defined social harms—some legal, others illegal—such as libel, slander, fraud, and propaganda. And, third, moderating disinformation assumes one can make a clear distinction between truthful and untruthful information—that there is a unique source against which truthfulness can be tested.

Policymakers increasingly assess disinformation to be an existential challenge to democratic governance. The European Union has argued that disinformation is a threat to democracy and European values.

Across the Atlantic, statements from U.S. President Joe Biden's administration on disinformation and its impact on the COVID-19 vaccine campaign reinforce this idea. This rhetoric challenges international human rights standards that widely protect free speech—including the dissemination of false information in public discourse. Under the Inter-American Convention on Human Rights, for example, states are specifically obligated to protect against private restrictions of freedom of expression that may result in indirect censorship. The new consensus against disinformation, which conditions free-speech protections on truth, does not only challenge free-speech norms; it also empowers private companies to arbitrate truth while denying this power to others in society. This shift should not be taken lightly.

The treatment of falsehoods and whether they constitute a social harm that requires state action differs significantly from one country to the next. Abundant jurisprudence exists that defines libel and slander, and most democracies have also identified specific instances in which society and/or the state may punish individuals for telling lies (such as witnesses in court proceedings or public officials). These concepts arrived at their current iterations following long debates. Accordingly, states already have determined which falsehoods constitute threats to their democracies and which should be tolerated as a condition for self-government. Addressing anew these categories in bulk under the term disinformation, whether through regulation or moderation, would mean discarding the democratic deliberations that led to current definitions of legal speech.

Finally, unlike in other moderation areas, efforts to counter disinformation assume that there is a single authoritative source against which all information can be assessed for truth. This assumption is particularly problematic when it comes to political disinformation, which is likely why most jurisdictions distrust the state to regulate false or misleading political discourse. But subjecting speech to a single source "truth" test can also be problematic when it comes to regulating more objective topics, such as science. The COVID-19 pandemic provides a useful illustration of the problem. As scientists learn more about the virus, some of their core assumptions and subsequent guidance has changed. For instance, scientific consensus now holds that the virus is transmitted primarily through the air, contrary to scientific views at the beginning of the outbreak. Science thrives when peers can build on and correct each other's mistakes. Confronted with differing expert opinions from different countries, schools of thought, and scientific institutions, who should internet companies hold as the ultimate authority to validate the truth? In other words, is it possible for them to craft legitimate rules regulating disinformation without veering into censorship?

The disinformation dilemma speaks to cultural, political, and legal weaknesses and strengths within each democracy. At the heart of the issue is a crisis of legitimacy among traditional knowledge producers. As legal scholar Jack Balkin writes, "A public sphere doesn't work properly without trusted and trustworthy institutions guided by professional and public-regarding norms." He argues that social media companies need to earn and develop that legitimacy while acknowledging that the same standards apply to societal institutions that traditionally have maintained public spheres and which now struggle over questions of disinformation.

Agustina Del Campo heads the Center for Studies on Freedom of Expression and Access to Information at the University of Palermo in Argentina.

Online Disinformation Against AAPI Communities During the COVID-19 Pandemic

JONATHAN CORPUS ONG

Misinformation, disinformation, and online hate speech have led to widespread violence in India, Myanmar, and Sri Lanka in the past several years. Unfortunately, the United States has also registered rising levels of disinformation and hate speech targeted against the Asian American and Pacific Islander (AAPI) communities, especially in the wake of the COVID-19 pandemic. When former president Donald Trump blamed China for the coronavirus, his use of racially charged language, such as referring to COVID-19 as the "Kung Flu" or "Chinese virus," corresponded with increased reports of hate crimes against individuals of Asian descent. This rise in physical violence against the AAPI community can be attributed to the spread of racial animosity on the internet—the latest illustration of the offline consequences of online misinformation campaigns.

Conspiracy theories targeting the AAPI community have caused upswells in hate crimes in past eras of U.S. history. For instance, the "Yellow Peril" discourse of the 1800s represented East Asian people as a source of vague and ominous danger. The 1982 Vincent Chin murder was motivated by racial scapegoating in the wake of Japan's rise as a world power. Meanwhile, the persistent "model minority" narrative was used by White Americans as a racial wedge to divide Asian and Black people during the 1960s civil rights movement.

The ubiquity of the internet, however, creates a different context for the spread of anti-Asian hatred today. In online spaces, hateful hashtags such as #ChinaLiedPeopleDied and #Chinazi have spread rampantly, and conspiracy theories about COVID-19's origin as a biological weapon from China have gone viral. Online media outlets, meanwhile, have covered hate crimes against the AAPI community, such as the March 2021 Atlanta spa shootings, from the perspectives of the perpetrators rather than the victims. Explicit and implicit bigotry in the online information ecosystem continues to fuel the marginalization of Asian people in the United States during a volatile period of the country's history.

The current surge of discrimination and violence against the AAPI community would not be possible at this scale without the internet. My colleagues and I at Harvard's Shorenstein Center observe that a right-wing media ecosystem has strategically targeted AAPI communities. These news sites and influencers proliferate misleading statistics and videos to stoke anti-Asian hatred and even sow divisions between the AAPI and Black communities. Right-wing Asian digital media platforms and influencers have simultaneously exploited feelings of alienation to recruit Asian Americans into more extreme conservative viewpoints. Media manipulators stand at the ready to push political propaganda and gain passionate followers. This antagonism is amplified through platform algorithms that promote controversy and stoke resentment between different social groups to drive online engagement. The rate at which disinformation and divisive content can spread in the digital era is unprecedented, and they consequently lead to real-world unrest.

The misrepresentation and underrepresentation of AAPI voices by politicians and the media has permitted online disinformation to spark violence against minority groups during the pandemic. As a communications scholar and disinformation researcher, I find it essential to conduct more interdisciplinary research into how members of the AAPI community navigate the diverse threats of the contemporary digital environment, from racist conspiracy theories to an extremist right-wing ideology that preys on the community's current state of fear and anxiety. What are new memetic expressions of the "model minority" myth on the internet? What are the popular vernaculars, ethnolinguistic codes, and cultural humor that right-wing influencers use to appeal to their followers while evading platforms' content moderation? These are challenging questions that require more data, more deliberation, and more community-engaged research.

The violent consequences of online disinformation targeting AAPI communities demonstrate the power of the internet to stoke racial resentment at a faster pace and broader scale than earlier media ecosystems. This is one example of the larger trend of ethnic violence originating from online discourse around the globe and emphasizes how viral hatred is not limited to autocratic countries overseas but has also taken root in democratic nations such as the United States.

Jonathan Corpus Ong is an associate professor of communication at the University of Massachusetts at Amherst and currently a research fellow at Harvard's Shorestein Center.

Preaching and Practicing Digital Democracy: The Case of India's Restriction of Chinese Applications

ARINDRAJIT BASU

Democracies claim that spreading democratic values and upholding an open internet is contingent upon countering Russia and China's authoritarian influence and their growing influence on technology. However, this focus risks obscuring a fundamental requirement for democratic resilience in politics and technology: that societies must resist their own domestic inclinations to adopt repressive principles. To defend against those impulses, democracies need to candidly assess the trajectory of their own policies while also protecting their citizens from extraterritorial authoritarianism from adversarial nations. India's recent restriction of Chinese applications offers an important case study that helps unpack this argument.

In 2020, after continued tensions and clashes at the border with China, India's government banned over one hundred Chinese apps. This accompanied other sanctions on Chinese technology, including blocking Huawei and ZTE from participating in 5G trials and imposing cumbersome obligations on Chinese foreign direct investment.

The app ban was designed to reduce India's economic and technological dependence on China and to hinder Chinese state surveillance purportedly facilitated by the apps. Proponents of decoupling rightfully argued that economic reliance upon such an unpredictable and adversarial neighbor limited New Delhi's means to counter China. The government directives announcing the ban also justified it as a way to promote digital democracy, citing concerns of Chinese data mining, the risk of digital profiling by foreign entities, and protecting the privacy of citizens as reasons for the restriction.

Policymakers drew an important distinction between India's digital values and China's repressive approach to technology. However, if India is genuinely committed to countering digital repression, it needs to carefully scrutinize democratic integrity at home. For instance, the legal provision used by the government to impose this restriction (Section 69A of the Information Technology Act) has been criticized by pro-

democracy advocates for facilitating censorship. India also failed to publish a thorough public report on the restricted Chinese apps, which made it more difficult for citizens to understand the government's rationale for the ban. The process for blocking Chinese apps was opaque and rooted in problematic legislation, which undermines India's democratic ideals.

Furthermore, while concerns over China's digital surveillance architecture are justified, India's surveillance policy is in dire need of reform. This has been underscored by recent revelations alleging the government's deployment of the NSO Group's Pegasus spyware to surveil journalists, lawyers, activists, and bureaucrats. Banning Chinese apps is one method of curtailing repressive Chinese influence, but the authorities must also restrict their own discretionary powers of surveillance to prevent misuse and preserve the trust of citizens.

The case of India has implications for all countries seeking to strengthen digital democracy, including the members of the G7. For democracies, ensuring rule of law and human rights protections within their borders is just as critical as sustaining military might or economic progress. Countries in multilateral coalitions that seek to promote democratic values must also facilitate uncomfortable conversations about their own democratic shortcomings. In the end, governments around the world will not preserve democratic norms simply because that is what other nations preach; democracies must demonstrate, in practice, the merits of upholding digital freedoms and the rule of law.

Arindrajit Basu is the research lead at India's Centre for Internet and Society.

Privacy vs. Democracy in the Digital Age: Indonesia's Challenge

SINTA DEWI ROSADI

Information and communication technologies (ICTs) have enabled citizens to gain information quickly and in large quantities, to communicate with their networks through social media, and to convey political opinions freely. Indonesia, the third-largest democracy on earth, has not been an exception to this trend: more than half of its population actively uses social media. With the proliferation of ICTs, many Indonesians hope that the internet will energize their democracy. But the expansion of ICTs has created challenges to protecting digital privacy. Digital records of online behavior can broadcast an individual's personal information in ways that they cannot anticipate or control, and this can pose a significant threat to democracy if not protected by enforceable privacy norms and legal frameworks.

Indonesia has at least thirty regulations relating to privacy, but the protection these offer is very minimal. The constitution, for example, does not even mention the word privacy. Indonesia's regulations do not define the governing bodies responsible for authorizing surveillance measures, what constitutes legitimate justifications for surveillance, or the time period during which surveillance is permitted. There is no single authority charged with overseeing surveillance procedures or granting warrants; instead, various agencies can initiate surveillance actions at their own discretion. Under urgent circumstances, the government can even surveil communications without any kind of judicial authorization. Additionally, the patchwork of legislation opaquely allows a broad range of scenarios in which the government can surveil civilians. Indonesia also does not place strict limits on the length of a surveillance period: different authorities can arbitrarily prolong them from thirty days to six months, with the possibility of indefinite further extensions. This fragmented mandate frequently results in the denial of transparency and due process to citizens.

The unchecked surveillance powers of government institutions is exemplified by the weakening of a 2019 amendment to Indonesia's anti-corruption law. The amendment established a governing board overseeing investigations of graft and mandated that the Corruption Eradication Commission apply for

authorization to conduct wiretaps of its targets. Yet, the constitutional court upheld the commission's right to conduct warrantless surveillance—weakening the amendment. Thus, even a small measure to curb the surveillance powers of a government agency was overruled by another branch of the government.

Indonesia's lack of a unified framework for legal surveillance virtually ensures that citizens' digital rights will be violated. And because there is no oversight mechanism for regulating surveillance operations and ensuring they remain within the bounds of the law, the prospects for abuse are heightened.

It is imperative that Indonesia's authorities work to resolve these ambiguities and implement a precise and robust legal framework for conducting legitimate surveillance. Such legislation should standardize the process for warranted surveillance, regulate which type of data can be collected by the state, restrict the number of parties that can access data collected through surveillance, and limit the usage of intercepted material as evidence in a court of law. Citizens also require remediation options if they feel they have been illegally or arbitrarily surveilled. Without these protections, government surveillance in Indonesia will leave citizens vulnerable to further human rights abuses.

Sinta Dewi Rosadi is an associate professor at Padjadjaran University in Indonesia.

Carnegie Endowment for International Peace

The Carnegie Endowment for International Peace is a unique global network of policy research centers in Russia, China, Europe, the Middle East, India, and the United States. Our mission, dating back more than a century, is to advance peace through analysis and development of fresh policy ideas and direct engagement and collaboration with decisionmakers in government, business, and civil society. Working together, our centers bring the inestimable benefit of multiple national viewpoints to bilateral, regional, and global issues.

Democracy, Conflict, and Governance

The Carnegie Democracy, Conflict, and Governance Program rigorously analyzes the global state of democracy, conflict, and governance, the interrelationship among them, and international efforts to strengthen democracy and governance, reduce violence, and stabilize conflict.

Digital Democracy Network

Carnegie's Digital Democracy Network is a global group of leading researchers and experts examining the relationship between technology, politics, democracy, and civil society. The network is dedicated to generating original analysis and enabling cross-regional knowledge-sharing to fill critical research and policy gaps.

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org