DECLASSIFIED by DNI Haines on 24 April 2023

[redacted]

NATIONAL INTELLIGENCE COUNCIL

ASSESSMENT

31 October 2022 NICA 2022-22810

(U[redacted]) Digital Repression Growing Globally, Threatening Freedoms

(U) Key Takeaways

(U[redacted]) ***Scope Note:*** *This NICA responds to a request from the DNI for an assessment of the implications of governments' use of the Internet and other digital technologies to suppress freedom and control public debate. The assessment focuses on digital repression, which we define as the use of digital information and communication technologies to surveil, manipulate, or coerce individuals or groups to control public debate and prevent challenges to leaders' hold on power. Several related topics are outside the scope of this paper, including governments' efforts to influence public opinion outside their borders, with the exception of their diaspora communities; to shape foreign election outcomes; or to conduct cyber attacks.*

(U[redacted]) We assess that foreign governments are increasingly using digital information and communication technologies to monitor and suppress political debate domestically as well as in their expatriate and diaspora communities abroad. Leaders exercise digital repression because they fear that open debate of political or social topics could jeopardize their hold on power.

- (U[redacted]) Censorship, misinformation and disinformation, mass surveillance, and invasive spyware are the primary tools of digital repression. During the past few years, governments—including some backsliding democracies—have become adept at using these tools to suppress public debate.

- (U[redacted]) Digital repression is threatening freedom globally because both autocrats and personalist leaders in backsliding democracies are increasingly using such practices to try to exercise control over domestic content creators and their audiences as well as dissident expatriates.

- (U[redacted]) The risks are likely to intensify in the coming years in view of the growing use of social media platforms with global reach and debate about how Western social media platforms should think about the challenges.

(U[redacted]) We assess that states' use of these methods to monitor and limit dissent probably will become even more pervasive, targeted, and complex in the next few years, further constraining freedoms globally. Mitigating against the growth of digital repression probably would require the establishment of unified international norms and protecting the Internet's architecture through coalitions with likeminded governments, civil society, and technology corporations. The development and spread of innovative technologies and approaches that help populations bypass governmental controls could help create openings for individuals to exercise greater digital freedoms within repressive states.

(U) This assessment was prepared under the auspices of the Director of the Strategic Futures Group (SFG). [redacted]

[redacted]

(U[redacted]) Governments Repressing Publics Through Digital Technologies

(U[redacted]) During the past decade, many foreign governments—both authoritarian regimes and backsliding democracies—increasingly have used digital information and communications technologies to monitor and suppress political dissent in their domestic populations as well as expatriate and diaspora communities abroad. Digital repression has grown as governments have become more concerned about their publics' expanded access to information online that could threaten their power.

(U[redacted]) Some regimes, notably China and Russia, have worried that open debate of political or social issues, facilitated by social media and other communication technologies, could eventually cost them their hold on power. In the years since the "Color Revolutions" in post-Soviet countries (2003-05) and the 2010-11 Arab Spring, many of these governments have incorporated digital technologies as vital components of state repression and broader statecraft. This has helped them stifle dissent beyond traditional means—such as censoring print media or physically harming dissidents—which they also continue to do.

- (U) This year, global Internet freedom declined for the 12th consecutive year—with China identified as the country providing the least Internet freedom for the eighth year in a row. Governments worldwide increasingly are blocking social media platforms, disrupting networks, manipulating online discussions, and arresting individuals who post political or social content that the governments want to suppress, according to Freedom House.

- (U) The commercial spyware industry, which makes tools that allow users to hack digital devices such as mobile telephones to surveil users, grew rapidly in the past decade and now has an estimated worth of $12 billion, according to a Western media report. While some states use such spyware tools and lawful intercept programs to target criminals and terrorists, governments also are increasingly using spyware to target political opposition and dissidents.

- [redacted] Mass surveillance of publics through artificial intelligence/machine learning (AI/ML) in combination with closed-circuit television cameras and social media—already prevalent in the People's Republic of China (PRC)—is becoming an increasingly common method used by regimes to try to prevent political unrest. Moreover, Beijing has been forward leaning in marketing these tools to other authoritarian governments. By 2019, Huawei and other PRC companies had provided or were negotiating to provide mass surveillance technology under its "Safe City" and "Smart City" programs in roughly 60 countries, [redacted].

(U[redacted]) Wariness of Publics and Hunger for Power Drive Digital Repression

(U[redacted]) We assess that the key drivers prompting most state leaders to exercise digital repression have been fears that open public debate of political or social topics could endanger their hold on power. Some authoritarian regimes grew concerned about the implications of the Internet early in its usage, with the Arab Spring uprisings possibly a pivotal global turning point, when authoritarian governments came to recognize that their publics' digital connectivity posed an existential threat to their grip on power. Autocrats' beliefs that Western governments, particularly the United States, have been using the Internet's influence to undermine their regimes' stability have exacerbated these fears. Since the Arab Spring, public protest activity—much of it supported and fed by digital connectivity—has been high globally, keeping many leaders on edge.

- (U) Since 2011, the number of protest movements and demonstrations has risen sharply worldwide, according to a US-based think tank; demonstration activity surged globally for the second consecutive year in 2021, with antigovernment sentiment often featuring prominently in protests.

- (U[redacted]) Authoritarian leaders have been justifiably concerned about losing power through street protests or other forms of public anger. Before 2000, authoritarian regimes were overthrown primarily in coups, but between 2000 and 2017, they were more likely to be ousted by protesters or to lose power in elections that followed demonstrations, according to academic research.

- [redacted] In September, Iranian state media justified social media outages as a tactic to prevent riots, as widespread protests—which Iranian leaders claimed the United States fueled—unfolded following the death of a woman taken into custody by the morality police.

- [redacted]

(U[redacted]) Digital Repression Enhancing State Control

(U[redacted]) States are increasingly shifting from reactive modes to more proactive measures to guard against the threats they perceive. Those that engage in digital repression of their publics and diaspora communities generally are practicing one or more of the four key types of repression: censorship, misinformation and disinformation, mass surveillance, and use of invasive spyware against specific individuals. These approaches extend repressive regimes' reach beyond traditional measures, aid in concealing repression from domestic publics and international media, and often are tolerated by publics. In addition, the necessary technologies to carry them out are relatively easy to acquire.

- (U) **Censorship.** In 2021, Internet shutdowns—a major mode of digital censorship—took place in 34 countries for a total of 182 shutdowns, with shutdowns resulting in $5.45 billion in financial losses globally, according to two separate sets of researchers. Shutdowns have enabled autocrats to prevent or deter critics from shedding light on illiberal practices, such as regime massacres of demonstrators, or otherwise organizing against their interests, according to separate academic research.

- [redacted] **Misinformation and Disinformation.** Governments mislead their publics to prevent dissent or disable it quickly. For example, in early 2021, Russian authorities sought to obstruct protests by characterizing messages from jailed opposition activist Aleksey Navalnyy's Anticorruption Foundation as spam, judging from [redacted] a Western press report. [redacted]

- [redacted] **Mass Surveillance.** [redacted]

- [redacted] **Invasive Spyware.** At least 24 countries now use commercial cyber surveillance tools[redacted]. These technologies allow governments to gain access to an individual's digital devices often without any action on the user's part; some governments have used these tools to surveil political opponents, dissidents, and their contacts. For example, in October, a prominent digital rights organization assessed that the phones of two journalists and a human rights defender in Mexico had been infected with spyware between 2019 and 2021, despite public assurances by Mexican President Manuel Lopez Obrador in 2019 that spyware would no longer be used against the public.

(U[redacted]) Digital Repression Taking Global Toll

(U[redacted]) We assess that the use of digital tools for control of publics goes beyond the borders of authoritarian states and is contributing to a global loss of freedom. Several backsliding democratic governments—

(U) Citizens and Activists Finding Ways To Circumvent Digital Censorship

(U) Even in highly repressive environments, some citizens and activists are finding ways to work around digital censorship to continue to share information and organize, even if only temporarily or partially. Currently, they rely on the following technologies and simple approaches to do so.

- (U[redacted]) **Virtual Private Networks (VPNs)** are publicly accessible protocols that allow users to access many blocked sites by providing Internet service outside a censored country using a proxy server. Since last summer, several VPN providers have relocated their servers outside India to sidestep the Indian Government's requests for data on the nearly 270 million people in the country who use VPNs, according to [redacted] Indian and western media reports.

- (U) **The Onion Router (TOR)** uses multiple servers and encrypts each step of the way to prevent someone who is monitoring the network from uncovering private communications. The Switzerland-based Tor Foundation reported on social media that Iranian users of its software rose from 2,000 to more than 8,000 during four days in September.

- (U) **Mesh networks** involve individuals using Bluetooth or WiFi technology to create a chain of devices that can send messages to each other in close proximity. Activists in Hong Kong relied heavily on mesh networks to facilitate peer-to-peer communications during protests in 2019 and 2020, according to a think-tank researcher.

- [redacted] **Word play**—including the use of homonyms, puns, and English instead of Mandarin—is a simple workaround that some netizens in China have used to evade censored words and phrases, according to US academic literature and media reporting. In July, China-based chat application Weibo announced new regulations prohibiting the use of homophones in online messaging, [redacted] presumably under pressure from the regime, posing a potential new obstacle to covert word play.

- (U) Posting **mirrored or upside-down copies of video or images** is another way that users in China have evaded censorship. In April, WeChat users temporarily evaded AI-enabled censorship of a video critical of China's COVID-19 Shanghai lockdown by uploading mirrored and upside down copies of the video, according to a US press report.

and at least one liberal democracy—have used them to try to shape public views and spy on political opponents. Authoritarian states regularly use these tools to conduct transnational repression, reaching beyond their borders to try to control their expatriate and diaspora populations, and silence dissidents around the world.

(U[redacted]) Digital Repression Contributing to Erosion of Democracy

(U[redacted]) Some democracies—primarily those that are backsliding—have been using many of the same repressive approaches as authoritarian governments to try to control domestic political and social debate. Personalist leaders in these states have used censorship, misinformation and disinformation, and commercial spyware to target political opponents. We assess that the adoption of these digital repressive approaches is contributing to further democratic erosion globally.

- (U[redacted]) [redacted]
- [redacted] The government of [redacted] [redacted] has employed spyware and probably other tools to surveil opposition politicians and other regime critics since at least 2018, using legislation that provides a broad national security justification for almost all intrusions, according to [redacted] open-source reporting.
- (U[redacted]) [redacted]
- [redacted] [redacted]
- (U) [redacted]

(U[redacted]) Digital Transnational Repression Harming Free Speech Globally

(U[redacted]) Authoritarian states are using digital tools to conduct transnational repression against individual critics and diaspora communities to limit their influence over domestic audiences. Monitoring and threats against these communities limit freedom of speech wherever they reside, including in the United States and other liberal democracies. These actions are occurring against the backdrop of broader digital influence operations that many autocrats are concurrently conducting globally to try to shape how foreign publics view their regimes, create social and political upheaval in adversarial democracies, shift policies, and sway voters' perspectives and preferences.

- (U) In October, the US Justice Department charged 13 individuals, including PRC intelligence officers, for alleged efforts to unlawfully exert influence in the United States that included a scheme to forcibly repatriate a PRC national residing in the United States and efforts to surveil, harass, and coerce a US resident to return to China, according to press reporting.

[redacted] Comparing How Beijing and Moscow Conduct Digital Repression

[redacted]) China and Russia each seek to use digital repression to try to control public debate, but there also are key differences between them in both their goals and capabilities. We assess that Beijing exceeds Moscow in its ability to censor digital information and surveil the population, in part because Beijing prioritized digital controls earlier.

- (U) The CCP seeks to preempt challenges to its rule by demonstrating its responsiveness, eliminating dissent, and remolding society to achieve China's "national rejuvenation," prompting it to use digital repression techniques to downplay domestic shortcomings and try to reinforce the CCP's legitimacy as well as its all-encompassing reach, judging from President Xi Jinping's public statements and US academic literature.

- (U[redacted]) Beijing created its "Great Firewall" in the late 1990s, which helped China reduce its dependence on foreign Internet companies and foster the growth of its own robust Internet ecosystem consisting of companies it can more easily control.

- [redacted] Russian officials may aspire to similar levels of control over Russia's digital infrastructure and seek to deepen international partnerships to enhance Moscow's technical capabilities. Since 2019, Moscow has progressed toward creating a sovereign Internet that would host only government-approved platforms and content[redacted]. Moscow is likely to face difficulties developing a similarly effective system because it probably will continue to depend on Western Internet companies.

- [redacted] However, it has been less successful in controlling expressions of dissent by PRC citizens abroad or eliminating low-level expressions of dissent domestically, judging from [redacted] a commercial data aggregator, [redacted] and US academic studies.

- [redacted] The Kremlin probably will continue trying to increase its digital control through temporary access constraints to Internet services owned by US and European companies, taking down selected websites, applying fines and foreign agent designations, and creating indigenous social media and IT platforms, judging from [redacted] French and Russian press reports.

- [redacted]

- [redacted] China engages in extensive online harassment of real and perceived regime critics living abroad—particularly Tibetans, Uyghurs, and Hong Kong prodemocracy activists—on social media platforms. As of May, activists from these diasporas residing in France reported receiving frequent threatening messages on their social media and WeChat accounts, [redacted]. As of February, an ethnic Uyghur PRC national studying at a US university was unable to create group chats on WeChat, according to an FBI source, possibly because of PRC Government restrictions on Xinjiang residents' use of social media.

- (U) Between at least 2019 and 2020, PRC intelligence officers conspired with a China-based US technology company employee to disrupt anti-PRC speech, including in the United States, according to a US Justice Department indictment. The intelligence officers worked to sabotage online meetings that commemorated the Tiananmen Square massacre in 1989; provided the names and email and Internet Protocol addresses of overseas users to China, where PRC officers made threats through the US persons' family members; and helped surveil online meetings of dissidents, according to the indictment.

- (U[redacted]) Between 2016 and 2019, the UAE hired former USIC employees to create tools to try to hack into the accounts of global human rights activists, journalists, and rival governments, according to press reports and a Department of Justice press release. Open-source analysis from July 2021 indicated that the UAE was one of 10 countries using the commercial spyware Pegasus to target these types of individuals, including associates of Saudi journalist Jamal Khashoggi following his murder in Turkey in 2018, and the investigating Turkish prosecutor.

(U[redacted]) Digital Repression Efforts Likely To Grow

(U[redacted]) We assess that the use of digital tools and methods to monitor and limit dissent probably will become even more pervasive, targeted, and complex during the next few years. This trend is likely to further distort publicly available information and probably will outpace efforts to restore digital freedoms. Leaders' anxieties about potential and actual public unrest are likely to increase as they continue to deal with the ongoing social and economic challenges exacerbated by the COVID-19 pandemic and, more recently, by food insecurity and energy stresses caused by the war in Ukraine, further driving them to seek mechanisms to pacify their publics. Leaders also are likely to continue learning from and deploying other governments' repressive tactics.

- (U[redacted]) Mass surveillance of publics to stifle potential dissent probably will be a more readily available option for governments in the coming years as Closed-Circuit Television usage becomes even more prevalent. The global surveillance camera market was valued at $28.02 billion in 2021, and is expected to rise to $45.54 billion by 2027, with an increase in volume of units sold from 214.30 million in 2021 to 524.75 million by 2027, according to industry experts.

- (U) Academic studies have found that higher food prices tend to correlate with protests and riots, suggesting that instability risks will be higher than usual in the coming months and beyond. Increases in energy prices and the cost of living as well as food shortages already have manifested in heightened protest activity in many places around the world this year.

- (U) [redacted]

- (U[redacted]) Growing use of social media platforms with global reach will offer autocrats increasingly enriched user data to target select groups. In October, an investigative international media report alleged that China-based ByteDance—the parent company for TikTok, the most popular social media platform worldwide—had a plan to use the application to monitor and surveil US citizens. The increasing popularity of foreign social media platforms—as well as some ambiguity in how Western social media platforms think about the challenges posed by efforts to compete with and leverage their platforms—will likely pose greater risks in the years ahead.

- (U) Foreign powers almost certainly will also continue to use their online presences to shape foreign audiences' opinions; in September, public researchers discovered a Russia-based influence operation that managed more than 60 websites impersonating news organizations and had accounts on major US social media platforms.

(U[redacted]) Governments' Repressive Technological Capacities Likely To Improve

(U[redacted]) During the next several years, we expect that governments will grow more sophisticated in their use of existing repressive technologies and will learn quickly how to exploit new and more intrusive technologies, particularly automated surveillance and identity resolution techniques. There are numerous plausible means for how governments may expand their ability to harness digital technology to suppress people.

- (U[redacted]) Internet shutdowns that cover a particular geographic region or country are likely to grow less common, as governments increasingly adopt more precise blocking methods to deny access to specific websites, Internet services, and platforms. With the associated reduction in collateral harm, the broader public in countries where this is occurring may be less likely to complain about censorship, even as specific individuals and communities continue to suffer because of it. Similarly, the damage from targeted blocking probably will be less obvious to journalists and the international community, reducing the potential for international condemnation of shutdowns.

- (U[redacted]) Authoritarian regimes may begin to use AI/ML to predict who might be likely to become a dissident and target them before they have criticized or acted against the regime, regardless of the accuracy of their predictions. As of 2018, at least a dozen Chinese companies had begun conducting emotional surveillance of their employees' brainwaves to monitor for outliers with the alleged intention of boosting workers' morale before distress can cause a problem, according to industry reporting.

- [redacted] China-based firms are emerging as world leaders in AI-enabled virtual personas—which use an empathetic computing framework to perform real-time sentiment analysis of online users—suggesting that Beijing may work toward using such personas to manipulate public views. [redacted]

- (U) Governments already have used deepfakes—which include AI-enabled falsified videos, voice cloning, images, and generative text—to supplement online influence operations by generating false personas, but they also could expand use of deepfakes to harass and suppress dissidents. For example, posting deepfake nude images or videos of female dissidents could become a more common way to undermine their credibility.

- [redacted]

[redacted]

- [redacted] Russia's online influence actors have continued to adapt to hide their activities, judging from a social media company's analysis, [redacted] suggesting that the Kremlin will find workarounds to conceal much of its misinformation and disinformation operations targeted at Russian domestic and diaspora publics.

(U) Possible Options To Mitigate The Growth of Digital Repression

[redacted] In this era of digital information and communications technologies, mitigating against the encroachment of digital repression probably will require the establishment of international norms related to digital space and protection of Internet architecture. Such efforts probably would be most effective if the United States and likeminded liberal democratic governments coordinated their efforts in coalitions that included civil society and technology corporations.

[redacted] Heavily repressive states probably will be unresponsive to calls by the United States and other liberal democracies to ease digital repressive practices domestically or internationally. Encouraging the development and spread of innovative technologies and approaches, however, might help puncture even small holes in states' repressive apparatuses, allowing small openings of freedom for at least some of their citizens.

(U[redacted]) The Creation of a Unified Norms Scaffolding Might Help

(U[redacted]) Widely held norms have not yet been developed to shape how governments engage in and oversee many of the technologies that are used for digital repression, making this a potential area for US leadership. Norms development, including the adoption of regulations and laws, generally lags the adoption of new technologies. Many partner countries and multilateral entities—some with US involvement—have begun working to achieve accepted norms. There probably is a need for international leadership, though, to bring these disparate efforts together and address the differing ideologies among liberal democracies on the role of government in controlling private-sector technology conduct and the location and transmission of citizens' digital data. Developing a greater sense of urgency among partners about the growing threat that misuse of digital technologies poses to freedoms within their borders might help overcome some of these challenges.

- (U) No country in the world currently has a legally binding mechanism to govern AI use and most liberal democracies still are working to determine appropriate regulations for social media corporations and conduct. The commercial spyware industry is largely unregulated, with individual countries' export controls leading much of the current regulatory environment.

- (U[redacted]) Many countries and civil society groups might be receptive to US leadership on norms development at the second US-led Summit for Democracy when it occurs in early to mid-2023. Leaders of the Summit's Technology Cohort [redacted].

- (U[redacted]) The US-initiated Declaration for the Future of the Internet (DFI) emerged from the first Summit for Democracy in December 2021 and was released in April 2022 with the endorsement of 60 partner governments. The Declaration commits signatories to a single global Internet that is open and fosters competition, privacy, and respect for human rights. [redacted]

[redacted].

- (U) Established in 2011, the Freedom Online Coalition is a diplomatic network of 34 governments including the United States that works to support free expression, association, assembly, and privacy online. The United States is slated to become Chair of the Coalition in 2023, presenting an opportunity to emphasize the necessity of moving forward on digital protections for publics. One possible option might be to press members to adopt a voluntary code of conduct.

(U) Additional ongoing norms development arenas further point to the need for a unification of efforts.

- (U[redacted]) This year, the Council of Europe—in which the United States is a non-voting observer—began working toward an international, legally binding instrument to govern AI. In 2021, the European Commission released a draft AI Act that is intended to legally regulate all AI systems deployed in the EU, [redacted]. Resolving US differences with Europe over AI regulation in the interest of ensuring human rights and democratic freedoms could help increase the pressure on major state perpetrators to ease digital repression.

- (U[redacted]) [redacted]

[redacted].

- (U[redacted]) In 2019, the OECD first led the way on norms development in AI, when all member states and some non-member governments agreed to AI principles, which "focus on how governments and other actors can shape a human-centric approach to trustworthy AI," according to the OECD website, and that respects human rights and democratic values. [redacted].

- (U[redacted]) The Global Partnership on AI, first conceived of at a G7 summit in 2019, is now an additional OECD-housed effort of 25 countries including the United States, and aims to guide the responsible development and use of AI that is "consistent with human rights, fundamental freedoms, and shared democratic values."

(U[redacted]) Protecting the Internet's Architecture Would Help Preserve Freedoms

[redacted] We assess that steps to thwart efforts by China and Russia to undermine existing Internet governance would help ensure the integrity of the global Internet architecture and prevent the development of country-led Internet structures that allow for heavy censorship and harm free speech. In recent years, China and Russia have worked to weaken and replace the existing US-backed multi-stakeholder model of Internet governance.

- [redacted]

[redacted]

- (U[redacted]) Several [redacted] multilateral and US-based technical, engineering, and standards bodies play an important role in shaping the topography of global cyberspace, and present opportunities for US leadership to stem efforts by Beijing, Moscow, and other authoritarian governments to reshape the Internet. These include organizations such as the Internet Governance Forum, Internet Corporation for Assigned Names and Numbers, Internet Engineering Task Force, Telecommunications Industry Association, 3rd Generation Partnership Project, American National Standards Institute, and the Institute of Electrical and Electronics Engineers.

- (U[redacted]) Some EU countries might be interested in exploring partnerships ahead of technical meetings of these Internet-related bodies. EU officials have advocated for Western states to increase their focus on countering China's behavior in technical bodies, [redacted].

[redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]