Promote and Build
A Strategic Approach to Digital Authoritarianism

By Erol Yayboke and Sam Brannen

THE ISSUE
Digital authoritarianism presents overlapping and expanding challenges within autocracies and democracies. The ever evolving tools and techniques of digital authoritarianism transcend boundaries and have over the past decade advanced the interests of authoritarian states while subverting human rights, democratic principles, and more. A new strategic approach is needed to address this broad challenge set. It should be grounded in fundamental principles and framed around promoting resilience while building affirmative alternatives, then executed across the U.S. government and multilateral system.

DIGITAL AUTHORITARIANISM ON THE RISE
As the world turns its eyes to the 2020 U.S. presidential election, many are wondering what role Russia, China, and others may play and how both external and internal actors will use digital technologies and applications as disruptive tools. Misinformation and disinformation may get the most attention (especially during an election year), but they are far from the only digital tools authoritarians use to repress, disrupt, and spar with strategic competitors.

The growing threat of digital authoritarianism is well understood in Washington and other capitals around the world. The problem has been exquisitely documented, described, and diagnosed. And yet the trend is not only continuing, it is accelerating within virtually every nation on Earth. Digital authoritarianism presents overlapping and expanding challenges (1) within autocracies, (2) as tools to undermine adversaries, (3) via export to like-minded regimes, and (4) within and by democracies themselves.

Exploitation of digital tools by leaders with authoritarian tendencies threatens to take humanity backward, potentially undoing decades of post–World War II political and multilateral progress in every country from the world’s most important democracies to its most fragile. The suite of information technology their creators envisioned as bridges to enhance governance and liberty are in fact showing it is their double edge that cuts more deeply. From disinformation to corporate espionage, surveillance of citizens, and election interference, abuse of these technologies and the number of actors engaged in harm via online spaces increases by the day. At the same time, the Internet is being deliberately fragmented in a way that is likely to advantage authoritarian states. The flow of information is increasingly dictated at the national level, limiting the competition of ideas and suppressing the rights of individuals who operate in the open and must follow the rules while advantaging those who already break the law with little consequence.

Established democracies lack a consistent and collective strategic approach to combat authoritarian use of digital
and online space, even as they often preserve and promote advantageous elements of technology. As a result, concrete actions have not been taken to stem or reverse the pernicious trends of digital authoritarianism.

To address the question of why digital authoritarianism continues to rise despite ongoing counterefforts and a shared, bipartisan, allied, and multilateral understanding of the problem, CSIS twice convened a bipartisan group of experts and leading voices from the public and private sectors in late spring and early summer 2020. The first discussion focused on current trends in digital authoritarianism and the second on emerging and future trends. The objective of those discussions, accompanying desk research, and analysis has been to provide a set of actionable, politically feasible, and readily achievable recommendations to stem the tide of digital authoritarianism; these are presented at the end of this policy brief.

Why digital authoritarianism is a threat to that which we are trying to protect. The authors define digital authoritarianism as the use of the Internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties. Human rights and civil liberties are at risk, including freedom of movement, the right to speak freely and express political dissent, and the right to personal privacy, online and off. Digital authoritarianism co-opts and corrupts the foundational principles of democratic and open societies; its goal is not just to break them down, but to redefine and reshape them in their authoritarian image.

Established democracies lack a consistent and collective strategic approach to combat authoritarian use of digital and online space, even as they often preserve and promote advantageous elements of technology.

The battle between the defenders and aggressors in the digital space is fundamentally over trust. Arguably the most valuable commodity in a democracy, public trust underpins the social contract between the state and its citizens. Without public trust, institutions come undone and even the most mature democracies experience decline. Our CSIS colleague Suzanne Spaulding summed up the intent of Vladimir Putin’s Russia in this way:

“By undermining trust in institutions such as the media and the courts — institutions we look to as arbiters of truth — Putin hopes to get us to give up on the idea of truth and on the idea that we can hold our institutions accountable. He wants us to despair and disengage. Without an informed and engaged citizenry, democracy cannot function.”

TODAY, DIGITAL AUTHORITARIANISM PRESENTS FOUR OVERLAPPING CHALLENGES:

1. It is expanding within existing authoritarian-led states such as China, Russia, Iran, and Saudi Arabia. Artificial intelligence, facial recognition, and the Internet of things have increased the ability of authoritarian regimes to surveil and control individual citizens.

2. Authoritarian regimes are expanding the reach of their digital tools abroad, overtly and covertly increasing surveillance of their own citizens and citizens of other countries. They are also actively using these tools to undermine perceived state and non-state adversaries.

3. Digital authoritarians are exporting their tools to like-minded regimes both as a means to strengthen ties to these regimes and for commercial benefit. Likewise, tools of control are being commercially exported from democratic countries to partly free or authoritarian countries.

4. The tools, techniques, and strategies of digital authoritarianism are being adopted within democratic countries by political parties, interest groups, and private companies at the expense of public trust, personal privacy, and other civil liberties.
The digital tools of leaders with authoritarian tendencies are ever evolving. As means to an end, they are deployed differently depending on which type(s) of the four challenges listed above is the target or goal and what the nature of the perceived threat to the regime is. Tools for young protesters on the street will be different than for colonels in the barracks. Nonetheless, the tools can be grouped into those used for repression and disruption and those used for strategic competition among great powers.

**TOOLS OF REPRESSION AND DISRUPTION**

**Surveillance**: Long a tool of repression, surveillance has become easier and cheaper in the digital age. The proliferation of connected computers, smartphones, Internet-enabled devices, and embedded sensors provides a readymade platform for those with the means and know-how to collect data. Furthermore, advanced surveillance tools from the U.S. National Security Agency and other cyber agencies have been captured and intentionally or unintentionally released, enabling enhanced cyber surveillance by a growing number of countries and catapulting their development of advanced hacking. Former employees of top spy agencies have also offered their services for hire in a growing global gray market. The addition of surveillance driven by artificial intelligence (AI) affords authoritarians the ability to track real or perceived opponents unobtrusively with an almost unflinching eye in real time, vastly increasing the scale and reach of monitoring efforts. At least 75 countries use AI for surveillance purposes. Digital surveillance tools are also easily exported, and China has become the top global supplier. China has seized upon great economic and geopolitical influence opportunities by exporting digital surveillance tools that can be used by friendly authoritarian-minded regimes, from Uganda and Zambia to countries along the so-called Digital Silk Road, for online or physical persecution.

*Contributes most to these challenges: 1, 2, 3, 4*

**Cyberattacks and Espionage**: Authoritarian regimes routinely use digital espionage and cyberattacks to access sensitive information. Over the past decade, a much broader range of countries—notably Iran and North Korea—have developed increasingly sophisticated capabilities to conduct operations. Such capabilities have also become more commercially available both on the black market and through open commerce between authoritarian regimes and countries with sophisticated cyber capabilities. Digital espionage involves myriad tactics that include hacking, distributed denial-of-service (DDoS) attacks, phishing e-mails, spyware, malware, ransomware, and network intrusions. Digital espionage can be undertaken for economic reasons, whereby sensitive commercial data and intellectual property that provide the private sector its competitive edge are stolen. The same tactics can also be used to steal sensitive (classified) information to give the hostile actors a political advantage. Hostile powers have taken advantage of the ease with which digital applications can be downloaded to propagate the use of their own software platforms. Unbeknownst to the users, these platforms exploit the applications’ security and programming vulnerabilities to engage in espionage and collect user data.

*Contributes most to these challenges: 2, 3*

**Censorship**: Authoritarian leaders have been censoring speech and limiting access to information since the advent of the written word, but those efforts have been significantly simplified and centralized in the digital age. In China, where the government has maintained an iron fist regarding what software and platforms its citizens have access to, state authorities use measures that distract and inconvenience users who find workarounds, effectively making free speech a burdensome enterprise. An increasing number of countries simply turn information flows off, with at least 213 such shutdowns of communications infrastructure documented in over 33 countries in 2019.
An increasing number of countries are also enacting data localization measures that would grant them greater control over Internet access and—related to the aforementioned trend of surveillance—allow them to better monitor content generated by their citizens.

*Contributes most to these challenges: 1, 3, 4*

**Social and Electoral Manipulation:** Information can have lasting effects on social behavior, particularly when it pertains to sensitive issues. But the spread of misinformation (false information) and disinformation (deliberately shared false information) amplifies existing divisions in communities, increases public mistrust of institutions, and hurts social order and stability. In recent years, disinformation campaigns have been one of Russia’s preferred tactics in its efforts to weaken trust in core institutions in Europe and in the United States. When countries conduct elections, Russia leans on its propaganda channels and social media bots to spread disinformation and raise doubts about what “truth” is, creating a narrative that diminishes participatory democracy and drives political polarization. In what could pose a direct threat to the 2020 U.S. elections, authoritarian regimes are also using ransomware to attack voter registration and results databases. By weakening democratic processes, foreign authoritarian regimes not only undermine the internal political cohesion of democracies, but also erode consensus on foreign policy and make less likely that democracies will challenge actions of authoritarian states abroad. More worrisome, political parties (such as the United Kingdom’s Conservative Party) and leaders within democratic states (such as President Rodrigo Duterte in the Philippines) have adopted some of these same tools and tactics, either turning them against their rivals or simply using them to weaken institutional checks or controls once in power so they can advance their own agendas. The deliberate spread of disinformation by elected officials is an especially pernicious problem, worsened by a hyper-fragmented information environment that endangers objective information and understanding.

*Contributes most to these challenges: 1, 2, 4*

**TOOLS OF GREAT POWER**

**Digital Infrastructure:** While software platforms are the easiest and most cost-effective way to disrupt, they are not the only way. China has ambitious plans to use its Belt and Road Initiative to build a “Digital Silk Road,” using Chinese-owned companies to build 5G networks as well as underwater Internet cables. Controlling the underlying Internet infrastructure gives the country—which has its own history of using the Internet and digital technologies for social control and espionage—backdoor access to all traffic conducted through those cables. China has already made considerable advances. Its ZTE Corp provided the Ethiopian government security services to surveil opposition leaders and journalists and partnered with the Maduro regime to build Venezuela’s own system of social control. While it is true that China was merely providing the infrastructure enabling regimes to carry out their own existing authoritarian agendas, and not necessarily pushing those agendas itself, the provision of Chinese infrastructure comes with Chinese norms—namely, no desire to advance democracy or human rights. (U.S. and European-domiciled companies are subject to far greater domestic oversight and expected by their shareholders to hew to international laws and standards.) Chinese companies are particularly seizing upon opportunities in developing countries, which face burgeoning demands from their own societies for modernized infrastructure to facilitate economic growth. For example, Huawei has built around 70 percent of Africa’s 4G networks and is poised to play a big role in the development of 5G infrastructure across the continent. Without an effective alternative, developing country governments are being asked to choose between no infrastructure or low-quality infrastructure that comes with strings attached. As countries choose the latter, China expands its ability to deploy tools of repression and disruption, all while growing its influence within bodies setting international technology standards—including those related to global communications and digital infrastructure—potentially benefiting its companies commercially and advancing its intelligence collection goals.

*Contributes most to these challenges: 2, 3, 4*

**Advancing Authoritarian Visions of the Internet:** Global connectivity has allowed the Internet to be an open, interoperable, reliable, and relatively secure platform that has advanced U.S. and global commercial interests. That connectivity faces existential threats not only from deliberate acts by China and Russia, but also from measures taken by democratic countries seeking to ensure cybersecurity for their citizens. Autocratic regimes advocate for “digital sovereignty,” which gives the state greater political control over the use of the Internet in its jurisdiction, effectively ending global connectivity as we
know it. To enable this, China has sought an Internet governance model that allows for stringent data localization requirements, the adoption of a new Internet protocol (IP) that gives governments near-total control of their national Internet service systems, and the devolution of rights to curb the dissemination of information to sovereign states. At the same time, democratic governments seek to expand their legal reach on issues such as citizen privacy laws to regulate the global operations of companies doing business in their countries. Well intentioned or not, such practices set global norms and precedent in ways that authoritarian regimes can exploit to their own ends. For example, China’s draft Data Security Law seeks to expand its control over personal data within its borders on a global basis, building from the principles of Europe’s existing Global Data Protection Regime (GDPR). More recently, the United States and China have introduced dueling data security standards in the form of the U.S. Clean Network effort and China’s Global Initiative on Data Security, which could establish two essentially firewalled global networks.

Contributes most to these challenges: 1, 3, 4

The focus of this policy brief is on the deployment of these tools by leaders with authoritarian tendencies across the overlapping four areas of the geopolitical challenge set. However, it is important to note that violent extremist groups; sex, child, drug, and arms traffickers; and other non-state actors—including transnational criminal networks with ties to authoritarian regimes—all use similar tools to exploit the Internet for their gain at the expense of others. While each of these tools can be countered to some degree with a series of tactical responses, their continued expansion and evolution, along with the addition of new technologies, makes it an unwinnable offense–defense race. These authoritarian tools should be viewed as enabling an overall vision and strategy that must be countered with a coherent, affirmative, and strategic-level alternative vision.

HOW TOOLS MANIFEST AS THREATS

Digital authoritarianism is a lived experience in both democratic and non-democratic contexts, though it manifests differently in each. Whereas countries with a history of authoritarian rule (such as China, Russia, and Saudi Arabia) are evolving and increasingly exporting their tools and tactics, democracies and their institutions find themselves underprepared and vulnerable, gnawed away from inside and out.

Of the four overlapping ways presented above in which digital authoritarianism challenges democratic and human rights principles, all are worrying and worthy of a better strategic response. However, the fourth (adoption within democratic countries) poses the most significant, long-term, and direct threat for the simple reason that although only democratic countries can stop digital authoritarianism, they are being actively consumed by it. Political parties, interest groups, and even corporations within democratic countries have steadily adopted the approaches developed by authoritarian regimes, particularly over the last five years. Whereas the twentieth century saw several waves of democratic liberalization, the rise of digital authoritarianism is indicative of this century’s trend in the opposite direction, one permeating autocracies and democracies alike. This trend reversal has shown signs of accelerating in the midst of the Covid-19 pandemic, with many countries further relaxing privacy restrictions in responding to the public health emergency. The power of many governments has also grown during this period as extraordinary pressures prompt them to expand their influence over societies and economies. Established democracies such as the United States struggled with both the tools and strategic aims of digital authoritarianism even before Covid-19, often choosing tactical responses to individual threats over strategic efforts to address the broader incentive structures that have facilitated its rise.

Digital authoritarian trends have shown signs of accelerating in the midst of the Covid-19 pandemic.

On the one hand, the United States and its allies are struggling to respond to the offensive operations being taken against them by aggressors who operate in the “gray zone” of conflict that CSIS scholars have described as “in the contested arena somewhere between routine statecraft and open warfare.” On the other hand, a wave of populist or illiberal-minded political parties and figures within leading democracies have adopted approaches to domestic politics that borrow from autocratic playbooks with roots in Leninism and National Socialism. These actors
seek to sow doubt in existing institutions and non-aligned elites to propel themselves to power and avoid scrutiny and accountability. They reject the legitimacy of people or institutions who seek to judge them on their record or the viability of their policies. They find broad reach using digital tools to create powerful, new messaging platforms outside traditional media that, once open, enable them to make bold and sensational claims that are more apt to capture national attention. From their powerful communications perch, they can quickly subsume or redefine the political landscape. They are also opportunists unafraid to look for support wherever they can find it—including among extremist elements in their home countries and sympathetic or maliciously minded supporters abroad who assist in ways ranging from financial support to providing hacked information to leading disinformation campaigns on their behalf. In some instances, these authoritarian-minded parties and politicians have also proven more adept than others at making use of commercially available data on individual citizens collected by companies and vendors. Their ability to combine disinformation with targeted advertising is a powerful political weapon within already polarized environments.

For the United States to counter rising digital authoritarianism abroad—and from abroad into the United States—it must strengthen its own commitment to democracy at home. Though this will require a coherent and broadly accepted strategy (see below), a good start would be to not encourage or assume authoritarian tendencies in the first place. A better start would be to uphold our own bipartisan, democratic, and human rights principles at home.

THE IMPORTANCE AND DIFFICULTY OF PUBLIC–PRIVATE COOPERATION
A major obstacle to combating digital authoritarianism is the lack of public–private cooperation. In 2008, only two of the ten companies with the largest market capitalization in the world were technology firms. As of 2020, this number has grown to seven of the top ten, five of which are headquartered in the United States. It is not an exaggeration to say that the technology sector has been a key factor in overall economic growth—at least in the United States—over the past decade. However, this growth in the size and influence of the technology sector has coincided with a steady decline in Internet freedom and the rise of digital authoritarianism over a similar period. Legitimate questions are being raised about what responsibility these companies have to counter malign activities and whether they have become too powerful in the absence of sufficient oversight. Internet communications within free societies are often controlled by private technology companies. Governments, and especially elected officials, often lack technical expertise on rapidly evolving technologies. Digital authoritarianism has undeniably thrived in an environment of weak governance and weaker cooperation between the public and private sectors.

Technology companies have sought to portray themselves as neutral, all while rapidly evolving their own internal governance structures related to digital

U.S. LEADERSHIP ABROAD MUST START AT HOME
The authors believe that the United States has a key global leadership role to play in promoting and building an affirmative alternative to digital authoritarianism, one based on bipartisan democratic and human rights principles. However, it is worth asking (1) whether the United States maintains a sufficient moral foundation from which to lead, given its own recent struggles with democracy, and (2) what can and should be done to repair that eroded foundation. Will authoritarian leaders including a Belarusian leader who stole an election, and his Russian benefactors view as credible statements of “deep concern” coming from a government that has not committed to accepting the results of its own upcoming presidential election? Or are they more likely to notice that government has deployed unidentified federal security agents and chemicals banned under international law against its own citizens to quell political protests? For the United States to counter rising digital authoritarianism abroad—and from abroad into the United States—it must strengthen its own commitment to democracy at home.
authoritarianism to avoid new crises and reduce the risk of increased formal government regulation. On the one hand, some firms have attempted to self-regulate, and others have called for stronger government regulation—though on largely their own terms, because self-regulation without coordination or mandates across the sector could result in a loss of market share and revenue to those not similarly self-regulating. On the other hand, government-driven regulation (such as the European Copyright Directive) can limit competition by privileging large companies with the resources to comply, stifle economic growth, or even result in unintended consequences for civil society. There seems to be public–private consensus that regulation matters; however, a robust debate exists over who should regulate what. As this debate continues—often with the United States at odds with the European Union over the merits of the latter’s General Data Protection Regulation (GDPR), the highest profile government-led effort to date—one thing is clear: authoritarians are exploiting current gaps on their own platforms and those of technology firms around the world.

**FUTURE TRENDS IN DIGITAL AUTHORITARIANISM**

Looking ahead, several developments are likely. First, Covid-19 has already proven to accelerate existing trends, including further centralization of digital power in the hands of government at the expense of citizen privacy. Mass protests—another escalating global trend even before Covid-19—and other civil society and grassroots mobilization efforts have increasingly moved online, where authoritarians have more digital tools with which to silence them. Although movement restrictions are necessary to control the spread of the virus, they also present unprecedented opportunities and excuses for authoritarians to assume greater control of societies—online and off—which they are unlikely to relinquish easily post-pandemic.

Second, Covid-19–related economic and social disruptions are dealing a further blow to the rules-based international order. The unprecedented global economic growth over the past half century has been inequitable, particularly for minority groups, people of color, and women. Hyperconcentration of wealth and widening income inequality have accelerated within many countries. These same inequities are being laid bare by the pandemic, as seen in disproportionate infection, hospitalization, and death rates. At the same time, a new international regime—championed by Russia, China, Iran, and other authoritarian countries to varying degrees—is further chipping away at the post–World War II system of alliances and providing an alternative response to the rise of job-disrupting automation, changing global trade patterns, and the overall expansion of the digital economy. These attacks on the international order—some of which are coming from within—are likely to continue post-pandemic, with the tools of digital authoritarianism poised to be the weapons of choice. Thus, strategies to address digital authoritarianism should resist the desire to romanticize old ways of protecting liberties (such as post-neoliberalism) and must take into account broader societal disruptions. Affirmative alternative models must address not only the external attacks from authoritarian regimes, but also the Covid-19–exacerbated fissures from within. Technology companies, civil society, and governments can and should agree upon a baseline set of values that can foster open and inclusive societies.

Third, the complicated relationship between United States and China—and more specifically between the U.S. and Chinese technology sectors—is likely to continue regardless of who occupies the White House for the next four years. As our CSIS colleague James Lewis points out, “Chinese tech companies have fallen under the hammer of the Trump Administration.” Huawei, ZTE, Alibaba, Tencent, Baidu, Hikvision, and others are all facing punitive measures intended to limit their access to the U.S. market and damage their global reputations as well as counter real or perceived digital authoritarian threats. Recent increased tensions could lead to a “tech divorce” between China and the United States that could have consequences for digital authoritarian trends, especially the development and deployment of AI. The current digital whack-a-mole strategy might counter individual tactical threats

**Strategies to address digital authoritarianism should resist the desire to romanticize old ways of protecting liberties and must take into account broader societal disruptions.**
but will be insufficient as a strategic response to the quickly adapting tools of digital authoritarianism—and also runs the risk of stifling U.S. innovation, limiting export potential to a significant market, and taking focus away from multilateral efforts to lay the foundation for countering digital authoritarianism.

Finally, trust in institutions and democratic and human rights principles will almost certainly continue to erode without a more strategic approach to combating the digital authoritarianism that poses such a real and existential threat to it.

**PROMOTE AND BUILD: A STRATEGIC APPROACH TO DIGITAL AUTHORITARIANISM**

It is important for any coalition of democratic allies to play defense and offense at the same time: to promote resilience to digital authoritarian threats while building an affirmative alternative that diminishes the influence of authoritarian actors over time. U.S. executive-branch and congressional policymakers should view digital authoritarianism as a real threat to democratic and human rights principles at home and abroad. Tactical reactions to individual threats will not be enough; a more strategic and coordinated approach was urgently needed a decade ago, and now such an approach is long overdue.

A strategic approach to digital authoritarianism should reflect the four challenges presented above, marrying tactical solutions with strategic framing. Much as the challenges themselves are overlapping, the components of a strategy should be seen as mutually reinforcing, not mutually exclusive.

**1. PROMOTE RESILIENCE TO DIGITAL AUTHORITARIANISM BY STRENGTHENING DEMOCRACY AND HUMAN RIGHTS AT HOME**

**PROMOTE RESILIENCE AT HOME.**

- Regardless of who wins the 2020 presidential election, democratic and human rights principles promoted globally are equally relevant at home. In addition to building resilience to offensive digital tools deployed against the United States, as presented above, U.S. political leaders must focus on strengthening trust in domestic institutions. This should involve rejecting and criticizing all foreign intervention in U.S. elections, strongly supporting the right to vote in free and fair elections, resisting the urge to create or promulgate conspiracies and misinformation, committing to peaceful transitions of power, avoiding praise of authoritarians, rebuilding trust in core democratic institutions (such as a free press), and much more. For U.S. efforts to have any effect in countering digital authoritarianism abroad, it must lead by example. It is hard to imagine a successful strategic response to digital authoritarianism abroad if the United States fails to strengthen its own democracy at home.

**2. PROMOTE DEMOCRATIC AND HUMAN RIGHTS PRINCIPLES IN AND AROUND AUTHORITARIAN-LED STATES VIA FREE AND SECURE COMMUNICATION OVER A FREE AND SECURE INTERNET**

**PROMOTE FREE ONLINE EXPRESSION AND SECURE COMMUNICATION.**

- Incorporate democracy, human rights, and governance experts into cybersecurity-focused efforts to counter digital authoritarianism, primarily to ensure that these responses maintain Internet freedom and do not infringe upon human rights.

- Strengthen policies around encryption to focus on protection of rights and safety everywhere, but especially in countries (such as Belarus) at risk of sliding further into authoritarian rule.

- Fund and utilize the U.S. Agency for International Development (USAID) Digital Ecosystem Fund, which is designed “to make targeted investments to achieve a vision of open, inclusive, and secure digital ecosystems that can also withstand aggressively pursued authoritarian interference.”

- Expand the Digital Connectivity and Cybersecurity Partnership (DCCP) and affiliated DCCP Interagency Working Group—co-chaired by USAID and the Department of State, launched in 2018, and intended to build capacity to address digital authoritarianism—beyond just the Indo-Pacific region to everywhere digital authoritarian threats exist, also incorporating advice and expertise from outside government.

**PROMOTE A FREE AND SECURE INTERNET.**

- Support the execution of USAID’s 2020–2024 Digital Strategy, using its “guiding practices” as the baseline for developing an affirmative, strategic, and principles-
based approach to digital authoritarianism.

• Support the call in the 2018 National Cyber Strategy for the United States to “stand firm on its principles to protect and promote an open, interoperable, reliable, and secure Internet.”

• Be mindful and wary of efforts to create a bifurcated Internet with strong state control over censorship and access, supporting organizations such as the Freedom Online Coalition and other efforts to advance Internet openness and freedom.

• Avoid erecting expansive digital walls. While banning individual corporations (such as Huawei) and applications (such as TikTok and WeChat) may be deemed necessary for national security reasons, this power should be reserved for use based on specific national security threats rather than to over-extend censorship, which could be used as examples and excuses by China and other advocates of a more fragmented—and centrally controlled—Internet. Overall, the effort should be to advance principles or norms, not specific companies or nationalities.

3. COUNTER DIGITAL AUTHORITARIANISM AT HOME AND ABROAD NOT ONLY WITH TACTICAL DEFENSES, BUT WITH RESILIENCE ROOTED IN AFFIRMATIVE ALTERNATIVE VISIONS, NORMS, AND PRINCIPLES

BUILD TACTICAL RESILIENCE.

• Invest in tactical public and private countermeasures to digital tools of repression and disruption, including explainable algorithms, AI, and privacy-preserving machine learning. Facilitate greater cooperation and transparency by social media platforms and streamline information sharing between social media platforms, government, and outside researchers.

• Restrict the export of sophisticated surveillance tools to unfree countries and require businesses exporting dual-use technologies to report on the human rights impact of those products.

• Increase transparency requirements for foreign state-owned propaganda outlets operating in the United States and other democratic countries, imposing penalties for media interference by foreign officials. Require social media companies to report on foreign efforts to spread online disinformation and propaganda to relevant governmental and intelligence agencies. Bolster subnational resilience to digital influence campaigns.

• Create a set of standards that tests all foreign digital platforms (both current and future) for their potential to conduct espionage while operating in the United States. Clearly signal to foreign governments and actors that utilizing digital authoritarian tools will incur a significant cost, including but not limited to U.S. sanctions.

• Grant powers to the Federal Trade Commission to censure or levy fines against social media companies that fail to disclose and address the promulgation of bots on their platforms, as proposed in the Bot Disclosure and Accountability Act (S. 2125), which would also prohibit candidates, campaigns, and political organizations from using bots.

BUILD STRATEGIC RESILIENCE.

• Integrate a consistent approach to combatting digital authoritarianism into efforts related to democracy promotion, civic education, rule of law, human rights, and good governance across the interagency, including at the state and local level. Care should be taken to avoid siloed or separate capacity-building efforts that only target the technologically savvy, which would not reflect the overlapping, integrated, and equal-opportunity nature of the threat. Whether via USAID programming in Minsk or via local community organizers in Madison, these efforts require increased focus on the disruptive and repressive tools and tactics authoritarians use in the digital space.

• Compete long-term in the gray zone. Digital authoritarianism is among the most worrisome tools of gray zone competition. A full list of recommendations from our CSIS colleagues, fully endorsed by the authors of this policy brief, on how to strengthen relevant U.S. cyber capabilities—via enhanced authorities, appropriate resourcing, policy reform, and new tools—can be found here.

• Address the demand for illiberal surveillance technologies (including those incorporating AI), especially those used by police and other security forces within democratic and quasi-democratic countries. The UN’s Guiding Principles on Business and Human Rights could be a template to guide the development of clear and inclusive AI usage principles that are resistant to influence by authoritarian regimes.
4. BUILD AFFIRMATIVE ALTERNATIVES TO DIGITAL AUTHORITARIANISM, ESPECIALLY FOR COUNTRIES CURRENTLY FORCED TO DECIDE BETWEEN GROWTH AND STABILITY WITH AUTHORITARIAN STRINGS ATTACHED OR NO GROWTH AND STABILITY

BUILD AN AFFIRMATIVE ALTERNATIVE.

- Issue a presidential policy directive within the first 100 days of the new U.S. administration that prioritizes advancing democracy globally and places the protection of democratic and human rights principles squarely in the national interest of the United States.
- Create a U.S. government strategy on democracy centered around developing an affirmative vision for U.S. efforts to strengthen democracy abroad. This vision should be grounded in broadly agreed-upon principles (i.e., bipartisan and inclusive of civil society and private sector considerations) that outline what it is we are trying to protect from authoritarianism, digital or otherwise. It should reflect lessons learned from newer democracies such as Estonia and Taiwan, which were born in the digital age. The strategy should also call for the close interagency coordination of responses to digital authoritarianism and should be mutually reinforcing with the administration’s National Cyber Strategy.
- Create an interagency body based out of the White House—to be housed in the National Security Council (NSC) or in the form of a policy coordination committee—with the power to coordinate a whole-of-government response to digital authoritarianism as part of this broader strategy on democracy. The interagency body should be led by a senior director on the NSC (such as the senior director for democracy, human rights, and international organizations) with the power to counter digital authoritarianism.
- Bolster the ability of relevant experts at the Department of State and USAID to comprehend the links between their long-standing work on democracy, human rights, and governance and the modern threats posed by digital authoritarianism. Field-based personnel in particular must be able to assess and (ideally) respond to these threats as they present themselves abroad.
- Enable an affirmative alternative to Chinese digital infrastructure, even if it requires congressional approval and government intervention to do so; asking partners and allies to simply reject Chinese digital infrastructure (such as that offered by Huawei or ZTE) is not a compelling enough strategy. The United States should enable alternatives by investing in innovation within its own private sector technology and digital infrastructure firms—and those in like-minded countries—and, subsequently, by expanding their global market access through strategic use of development finance.
- Convene a global conversation (for example, at the 2021 Group of Seven and/or 2020 Group of Twenty meetings) on how a post-Covid-19 global economy can address the fundamental inequities of the pre-Covid-19 global economy, coupling this more inclusive vision with an affirmative alternative approach to digital authoritarianism.

BUILD STRONGER MULTILATERAL COALITIONS.

- Explore creating a private sector–led coalition to counter digital authoritarianism, similar to how the Global Internet Forum to Counter Terrorism unites technology companies around stopping terrorist utilization of their platforms.
- Promote the development and utilization of clearer multilateral frameworks and norms for using AI and protecting human rights.
- Avoid divergence with European allies, Japan, and other like-minded countries on digital authoritarianism. Leverage the Group of Seven and other multilateral forums to unite behind a common set of democratic and human rights principles, focusing efforts on building affirmative alternatives to digital authoritarianism (such as on digital infrastructure) in addition to coordinating tactical responses.
- Drive innovation and greater digital literacy in multilateral institutions, many of which are yet to catch up to today’s digital realities, much less digital authoritarian threats. A good example of how this can be done is the Innovation Cell within the UN Department of Political and Peacebuilding Affairs, designed to support the broader department to “understand and explore, pilot, and scale new technologies, tools, and practices in conflict prevention, mediation and peacebuilding.”
- Collaborate with U.S. private industry to ensure continued active participation and representation of U.S. and democratic interests in all relevant international technology standards-setting bodies.
including but not limited to the UN’s International Telecommunication Union (ITU), the World Trade Organization, and the World Internet Conference. Use all available political capital to promote democratic and human rights principles and counter efforts to change standards in ways that increase opportunities for digital authoritarianism, as is the case with recent Chinese efforts at the ITU to fragment the Internet. The United States and its allies need to be actively engaged in the leadership campaign and election processes of these organizations, for example when the election for ITU secretary-general, currently a Chinese national, takes place in 2022.

**Erol Yayboke** is deputy director and a senior fellow with the Project on Prosperity and Development (PPD) at the Center for Strategic and International Studies (CSIS). **Sam Brannen** leads the Risk and Foresight Group at CSIS and is a senior fellow in the International Security Program.

The authors would like to acknowledge the significant contribution of **Sundar R. Ramanujam** and would like to thank the myriad internal CSIS and outside reviewers who provided feedback on various drafts of the brief.

**CSIS** received a financial gift from Facebook in support of research on digital authoritarianism.