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.

Contributes most to these challenges: 2, 3
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