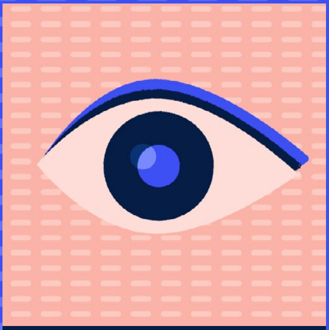
Digital Threats to Democracy: Ruling with a Silicon Fist

M. Nina Miller, Technology for Global Security



FUTURE DIGITAL THREATS TO DEMOCRACY

This ongoing series from Technology for Global Security (T4GS) and the Center for a New American Security (CNAS) examines the elements and potential implications of digital threats to democracy over the next ten years. This post breaks down the drivers of our next trend: increased digital authoritarianism.

Control. While the rise of digital authoritarianism cuts across different regime types and implicates companies developing cutting-edge technologies, a common element across these efforts is surveillance and control. The international sale and government contracting of these new and powerful tools drive us toward an uncertain, potentially less democratic future.

BUILDING AN INFORMATION WALL

The first tactic in the digital authoritarian toolkit is to establish information walls through fear, friction, or flooding. While employing traditional methods of repression and punishment to censor through fear, digital authoritarians also make it more difficult for citizens to access information through internet shutdowns, firewalls, and paywalls. In addition, digital dictators target traditional democratic values and freedoms by flooding the internet and other outlets for speech, press, and assembly. Inauthentic accounts ("bots"), deepfakes, and new tools of digital propaganda help states amplify narratives, build polarization, and increase "us versus them" divisions.

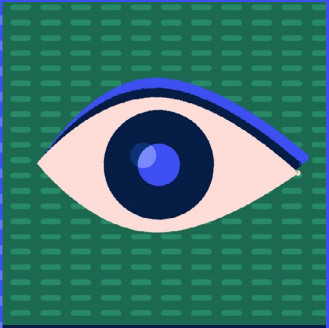
With information walls, regimes can shape public opinion in newly-sophisticated ways by establishing state control over the messages their population can access—and the information they do not. Without advanced communications technologies, these groups will be unable to contribute to online discussions or mobilization, benefit from economic growth associated with internet access, or raise global awareness of humanitarian abuses.

These novel censorship techniques make authoritarian regimes more repressive and potentially more durable. As Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright describe:

> Digital autocracies have grown far more durable than their pre-tech predecessors and their less technologically savvy peers. In contrast to what technology optimists envisioned at the dawn of the millennium, autocracies are benefiting from the Internet and other new technologies, not falling victim to them.

CONTROL DATA, CONTROL THE FUTURE

The second digital authoritarian tactic is to gather information about citizens and consumers, driven by advances in data analytics and machine learning. The basis of these new technical capabilities—ranging from mass facial recognition systems to predictive policing—is data. Citizens in both democratic and authoritarian countries face an increasingly self-sustaining cycle of surveillance and data extraction that is reducing individual consent:



FUTURE DIGITAL THREATS TO DEMOCRACY

This ongoing series from Technology for Global Security (T4GS) and the Center for a New American Security (CNAS) examines the elements and potential implications of digital threats to democracy over the next ten years. This post breaks down the drivers of our next trend: increased digital authoritarianism.

1. The introduction of consumer digital devices into every element of daily life increasingly enables mass collection of personal, biometric, consumer, and other data.
2. Increasing computing power facilitates large-scale data analysis with sophisticated artificial intelligence (AI)/machine learning (ML) techniques.
3. There is a growing mutual benefit and collaboration between illiberal governments and companies based in both Western democracies and within authoritarian states themselves. Authoritarian regimes offer data access without regulation in what one interviewee for this project called "techno-authoritarian synergy."
4. These massive datasets are used for technical research and to further development of AI/ML, autonomous systems, and augmented reality/virtual reality (AR/VR).
5. These new technologies will increasingly gather information and mine more training data for subsequent research, in addition to their use in repression.

LIVING UNDER DIGITAL CONTROL

These new methods of control are often based on surveillance and data collection, which could make their infringement on democratic freedoms and privacy less obvious and therefore less likely to provoke public objection. For instance, predictive policing uses past data to anticipate when, where, and which individuals are likely to be involved in a crime—a process that relies on correlation and pre-emption. As the quantity and wide source of data grow, digital authoritarians could instead use autonomous policing for crowd control and surveillance, drawing upon their full arsenal of AI, robotics, facial recognition, and autonomous decision-making. This possibility would make it easier for governments to abuse their own citizens, while raising well-known risks of bias and discrimination in AI that could have repressive, and likely often lethal, consequences.

Looking to the future, digital authoritarianism may face counter-innovation from tech-savvy activists. For instance, designers have created clothing and accessories to trick facial recognition software, while open-source satellite imagery analysts have identified forced labor and detention camps in China. In the future, AI identification of deepfakes could combat information operations and point out human rights abuses, and software developers could help users prevent malicious software updates that enable digital surveillance.

Yet, the digital dictator will be pragmatic, resourceful, and connected to a global network of governments and companies that mutually benefit from sharing data and funding research projects. This next innovation in authoritarianism will increasingly encourage self-censorship and cyber sovereignty to reduce the influence of democracy activists and free press, both at home and abroad. These technological trends fit into a broader crisis of liberalism and democratic backsliding resulting from multiple economic, political, and cultural challenges in Western democracies. Over the next ten years, democratic institutions worldwide will continue to face a growing threat from the entrenchment of digital authoritarianism—unless we take steps now.

M. Nina Miller is a former research analyst with Technology for Global Security. Before joining T4GS, Nina interned with the Nuclear Threat Initiative's Global Nuclear Policy Program and Scientific and Technical Affairs teams. She holds a B.A. (International Honours) from the Joint Degree Programme between the College of William & Mary and the University of St Andrews.

CNAS

T4GS
TECHNOLOGY
FOR
GLOBAL
SECURITY