CENTER for ETHICS and the RULE of LAW
UNIVERSITY of PENNSYLVANIA

Autocrats’ Tech Assault and Democracy’s Response

November 21-22, 2019

Conference Report

Introduction

Democracies are facing increasing threats by autocratic regimes around the world and by autocratic movements within their own borders. Many experts believe the rise is intertwined with advances in technology. This two-day conference examined whether technological developments are contributing to the rise of autocracy around the world and what the United States and other democracies can do to thwart their infiltration and effectiveness. The first day focused on the affinity between technology and autocracy, technology tools, and China’s development and use of technology in unprecedented ways for government and population control. The second day examined democracy’s defenses: regulatory and policy response, efforts by the media, and civic engagement and education.

There were six closed sessions attended by 31 participants from academia, think tanks, and the media. With a few exceptions, participants attended all six sessions. Several submitted new papers or drafts of papers for the conference, which were discussed in the sessions. CERL will use the submitted manuscripts as the foundation for a proposal to be submitted to the Oxford University Press for publication as a volume in the *Oxford Series in Ethics, National Security, and the Rule of Law*. In addition, there was a two-hour public keynote panel on November 21 that touched on the main discussion topics of the closed sessions.

This report provides an overview of the key issues discussed during the conference sessions and the public keynote panel discussion. Because the sessions operated under the Chatham House Rule, the report does not attribute specific comments to identified participants by name, although the conference guest list is public knowledge.

Session 1: Why Technology Favors the Autocrat

The first session was intended to lay the foundation for the following five sessions. The participants considered the relationship between technology and autocracy from a broad perspective.

The discussion began with a question: is there a basis for thinking that the technological revolution has caused a rise in autocracy? Participants discussed three current phenomena that have helped encourage the rise of autocracy: the increased relevance of ever-autocratic China on the global stage; rising illiberal movements in historically racially homogenous European nations; and the rise of an illiberal movement in the United States. While it is not clear whether these phenomena are isolated or interrelated, or whether technology caused their ascent, the consensus was that technology is at least amplifying autocracy’s rise by increasing connectivity among those holding autocratic views and likely playing a role in converting simmering dissent to autocratic zeal. In other words, these phenomena would have occurred on their own; technology was a “force multiplier.”

Technology has successfully advanced autocracy because it is an equalizer. It allows weaker nations to have equal impact on propaganda, and it is a cheap addition to their national security arsenal. It is no longer just the wealthy or elite or the current installed political leaders who control public opinion and have access to data. Data access is arguably the most effective tool in the autocrat’s tool kit.

The participants discussed the role of liberalism and illiberalism in both a democracy and in an autocracy. While there is a temptation to use technology to enhance power (more difficult to do in liberal democracies where power is diffused), its use is not inherently liberal or illiberal. Again, technology is simply an equalizer, particularly data collection and access.

Another discussion thread focused on whether autocratic regimes' use of technology is inherently dangerous. For instance, an autocratic leader using technology may obtain a better understanding of the interests of his people than a leader of a democracy, where the populace may not always vote for what is in its best interests. How autocrats may use technology for benign purposes is not the concern or even the question, however. The autocrat's aim is to consolidate and monopolize power not constrained by the rule of law. Technology is helping autocrats achieve these ends primarily by gaining access to data and platforms. Participants also discussed the connection between data and power in the private sector. While private tech companies hold a great deal of data in the end states have the control because they monopolize the permissible use of technology within their borders. For instance, China blocks Chinese viewers from Google.

The discussion moved to concerns regarding the use of technology to win hearts and minds, or propaganda, to which the United States has been especially vulnerable. Many believe that social media companies are problematic because they are unaware of or indifferent to their impact on political discourse and voting decisions. In 2016, algorithms rewarded articles that incited, and even news companies were incentivized to agitate readers. But an important normative question was raised: does it matter that tensions are being fomented?

Technology allows values to be subverted, which is particularly evident via partisan gerrymandering, considered a troubling example of autocratic creep. But the larger and perhaps most problematic issue of all is what underlies gerrymandering: data collection and possibly privacy infringement. There are three data-related technologies: privacy enhancing (encryption), privacy diminishing (data collection), and privacy neutral (information dissemination). The participants believe that the co-opting of privacy enhancing technology by autocrats is particularly problematic.

Does data collection technology overwhelm all other technology? Is it the root cause of democratic hijacking by autocrats, that is, democracy's Achilles heel? For example, data gathering and crunching algorithms have resulted in new easy-to-redesign district maps favoring targeted partisan lawmakers. Data collection also enables microtargeted political advertising, which inhibits democracies' ability to check untruths. And democracies are at a disadvantage because they are more restricted from placing limitations on data collection, making them more vulnerable to manipulation. The EU, however, has substantially limited the collection and sale of personal data. Is this un-democratic? Some argue it is not.

The last major theme centered on the people's trust of their government to handle private data. To what extent should government's access to private information be limited? But there is the other side: government's responsibility to protect and defend citizens. Thus, it becomes necessary to strike a balance between placing restraints on government and enabling it to lead homeland defense. Some believe that the conversation about limits on governmental access to private data is a distraction from the real issue: how to control the tech giants.

Session Two: The Tech Tools: The Means to an Authoritarian End

The session began with two questions: How are authoritarians using technology to consolidate power and survive longer? How are people using technology to support their political parties and ideologies within a democracy?

Cryptocurrency kicked off the discussion. Does it liberate or control? While cryptocurrency itself cannot be regulated, the on-ramps and off-ramps (exchange points) used for trading currency are regulated around the world. Many assume that cryptocurrency is decentralized, but that is not necessarily the case. Permissioned blockchain networks can be used by a government as a surveillance tool. China is using cryptocurrency to gain more data on business transactions, and Bitcoin can be used to track transactions as seen in law enforcement investigations. China is looking into digitizing its official currency, RMB, which could result in Beijing monitoring civilian spending. In sum, cryptocurrency can be used in ways consistent with autocratic aims.

Because technology now allows much greater disruption on a global scale, the Internet is no longer the ally of democracy. It is difficult to identify what the target should be for any countermeasures. Is it disinformation, foreign influence campaigns, or polarization and extreme opinions? Disinformation is false or misleading information intended to deceive; the information can contain false facts or deliberately taken out of context. Because democracy is concerned with information as opposed to data, disinformation is one of its chief concerns.

The broader issue is information control: having an open information system vs. restricting the information within it. Free speech used to be a tool of control; an information flood would be released, and we expected the truth to rise to the top. This occurred in a time when only a few media entities managed information. But because social media has opened incalculable floodgates of information, the truth now faces many barriers to "working its way to the top." And today's Internet speed and quantity of information allows for massive doubt to be sown. Adding to mix is the potential profitability of producing content that is false, incendiary, and odious ("the dark side of transparency").

Platforms like Facebook have a financial interest in maintaining the trust of its customers, however. Disinformation is most dangerous for persons who hold fervid, extreme views and whose confirmation bias will propel them to seek more of it.

Session Three: The Case of China and Its Progeny

Chinese citizens' concern about privacy is beginning to "bubble up," and acceptance of government tactics is beginning to erode. There are reactions to China's social credit system in which individuals earn a score based on their behaviors (e.g., financial, criminal, and social), associations, and other factors. The score dictates their ability to get jobs, take out loans, travel, and numerous other life activities. In addition to this government strand, there is an Alibaba strand, which tracks purchase transactions and assigns a score based on the individual's economic behavior. China is exporting its control and surveillance technology to other countries via its Belt and Road Initiative. Underlying China's technology strategy and development is its notion of cyber sovereignty or its belief that all cyber space is China's space.

There is significant concern that China is targeting the United States and other western democracies for infiltration through hardware, especially via Huawei and its possible construction of U.S. 5G networks. China is increasing its pressure on U.S. private actors to not run afoul of its ideology unless they wish to suffer substantial economic reprisals, as seen recently when an NBA Houston Rockets executive defended Hong Kong protesters in a tweet. Is it a betrayal of U.S. values to curb personal views to ensure a steady flow of profit? Are U.S. companies betraying long-held values in other ways?

Is the world witnessing a new great power competition between the United States and China? Participants discussed a number of contributing factors, including China's theft of U.S. military and private sector technology, its development of dual use technology and hardware like the assassin satellite, its use of grey zone tactics, and the advantages gained by not adhering to international law and the law of war. Can the United States prevail in the great power competition when it complies with long-established law that China ignores?

Participants concluded the session by discussing whether technology can help to consolidate power in the United States as it has in China. Consolidation in the United States is likely to happen but perhaps in a different way--in one political party, for example.

Session Four: The Role of Policymaking and Legislation, and the Global Stage

This session focused on potential policy and regulatory mechanisms for addressing tensions between autocracy and technology. In the background were four "buckets" identified by the moderator that could influence the kind of policy and regulation recommended: harm by autocracies against their own people, harm by autocracies against the United States, harm by autocracies against third-party states, and harm to Americans by U.S. companies.

There was much discussion about mechanisms to protect Americans from U.S. companies. They include the antitrust route and national regulation of access to private data such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). In connection with election integrity, ways to address like fraud protection or a harmful/ inflammatory speech coalition were also raised. Threats that originated internationally would be remedied by a domestic policy. Neither solution, however, is the focus of any policy proposal.

This led to a discussion for a need to first establish a principle of distinction between malicious influence and typical business influence and to consider First Amendment concerns before investigating remedies. Applying the principles may be challenging, however.

After establishing the principle of distinction and working through First Amendment concerns, what follows? To identify ways to restrict, minimize, and disincentivize adoption of malicious technologies, the group discussed looking at tools used in other contexts. For instance, there is an entire legal framework around restricting certain exports. But with social media and software, there is no hardware like surveillance cameras that can be regulated. Another approach would be to restrict certain enabling technologies or to permit exports only in certain situations. And another is installing review boards like those established in professional industries.

All the above are domestic approaches. There is much concern about multinational companies. How can domestic approaches to regulation be effective in their case? There was consensus that while MNEs operate around the globe, all have a home country. Perhaps we should look to the home country to direct regulatory efforts. One participant stated that in the case of MNEs whose homes are in the United States, the U.S. government should be responsible for addressing their egregious acts. Another participant expressed concern that these U.S.-based MNEs would simply reincorporate somewhere else. But another said that in the case of Apple, for example, U.S. government's leverage is Apple's U.S. customer base and that if Apple reincorporated outside the United States, the government could impose tougher restrictions.

There was more in-depth discussion about antitrust analysis and action around Facebook. (The New York Attorney General is conducting a multistate investigation to determine whether it should bring an action against Facebook for anticompetitive behavior.) There is political debate about whether to upend the assumption that a monopoly is good, so long as the barriers to market entry are low (because it drives entry into the market). In the case of Facebook, though, its more than two billion users could very well act as a barrier to entry. Fundamental factors that should be considered before deciding whether antitrust doctrine even applies are the structure and roles of the business under scrutiny. In the case of Facebook, is it a platform or a publisher? Does its role differ among markets? Additionally, because of the unprecedented number of networked users worldwide, the decision to break up Facebook would destroy the existence of a unique product. Finally, if Facebook cannot be broken up on antitrust grounds, can it be categorized differently, owing to its "public purpose," and thus be regulated?

The group discussed the creation of a nonprofit or NGO network with better safeguards as an alternative to Facebook. A participant suggested the formation of an FATF-type organization to develop policies on global Internet regulation. The organization would be composed solely of democratic states that would regularly peer review each other and have clear and lengthy processes for member acceptance and expulsion. Another participant suggested that businesses could mobilize and exercise corporate responsibility and push for improved governance of Facebook.

Session Five: Media Response: Transparency, Outreach and Collaboration with Tech's Private Sector

The session opened with a brief description on the instruments of national power: diplomacy (Department of State), military (Department of Defense), and economic (Department of the Treasury) or

"DIME." Information is also an instrument of national power yet there is no centralized government agency dedicated to its management. Other governments respond to disinformation campaigns. For instance, tech companies in Germany must remove false information within 24 hours, and the UK government decides if the information is false and then requires the tech company to remove it. The question that opened the discussion is whether Americans can trust their government to manage information and ensure its integrity. A participant opined that the people must get over their distrust of government because it is a mistake for tech company executives to decide what the people have access to.

A major shortcoming of the government to manage information is its reaction speed. In the UK, several examples of disinformation were described, including microtargeted campaigns relaying that Turkey was going to join the EU (and that UK citizens should "get out"). The information was false, but the government could not stop it because of the speed of dissemination. Do we insist then that tech companies be on the front lines validating the information? Or should the news media validate what they report?

One participant opined that interventions to solve a minor problem (e.g., a misleading article that was barely read aside from a small group of individuals seeking to confirm their own bias) have created a much bigger problem within the realm of journalism. Others took the view that misleading articles are not a minor problem and that the desire of foreign powers to erode our election system is one of the biggest national security issues we face. Ironically, if Western democracies fail to limit such information, then they risk losing the very democracy that supports their free speech rights. Europe has tools to address this problem, but the United States does not, given its robust First Amendment culture. Is it time to re-examine the First Amendment (e.g., the meaning of yelling fire in a crowded theater)?

The discussion turned to the plausibility of a centralized information agency in the United States, a market-based solution in which news sources are certified as reputable by the government, and a more direct channel from the intelligence community to the public. Another view held that more financial investment in journalism, including government funding, would attract the best and the brightest to more expertly assess content and elevate the credibility of the profession.

The most formidable impediment to countering disinformation is the high speed of dissemination. Conversely, the most effective way to combat disinformation is to slow down the speed. Should tech companies intentionally introduce friction into the system to reduce the speed of dissemination? Looking at the problem from this perspective requires a deep dive into understanding the lifecycle of information—from the source, through media outlets, to the public.

Session 6: The Role of Education: Civics and Media Literacy

This session opened with the observation that what happened in 2016 is known, but how to protect against persistent Russian interference is not. A participant raised the thesis of Suzanne Spaulding, a senior adviser at the Center for Strategic & International Studies, that civic education is a national security imperative. The public's understanding of our democratic institutions and government system is poor. The overemphasis on STEM instruction has displaced civics. Additionally, there has been a decline in democratic engagement and participation.

U.S. vulnerability is not limited to its election system. The judicial system is susceptible to foreign interference. A three-prong preventive strategy was proposed: better computer security for judges (who tend not to see themselves as targets), awareness of the forms of disinformation, and response mechanisms to protect judges after their opinions are issued.

One participant argued that democracy has not failed us, that we have failed democracy. Democracies are more than institutional structures. They are the way people are organized in a polity, which needs to be shaped, polished, and flexible to allow individuals to grow. Active members are needed. A democratic community only survives if there is robust civic virtue, knowledge of democracy's building blocks, a public spirit that is willing to look beyond personal interest to the community's well-being, and possibly a moral capacity for democratic ambivalence.

Another participant talked about the atrophy of civic engagement, the need for mandatory participation, and the importance of ethics education and investigations into disinformation campaigns. We need to re-examine what we mean by civic engagement, focus on digital literacy, combat the decline in civic mindedness, and stop the flattening of political conversation.

Other issues raised included the importance of teaching empathy, critical thinking, and independent thinking, and instructing teachers on how to teach civics education.

The session concluded with the observation that being able to step back from politics is a luxury and that civics engagement in our country has been highest when confronted with emergencies or heightened levels of dissent. The goal is not to return to a "garden of Eden" view of civic engagement but to create something entirely new.

Concluding Remarks: A Blueprint for Protecting Democracy and the Rule of Law

There was one very clear point of agreement among participants: our democracy is in trouble, and autocratic forms of government and illiberal political movements are on the rise.

There was no wholesale agreement around these political trends' relationship to technology. To the extent there was, it was a sense that democracy and the philosophy of an open marketplace of ideas are vulnerable to tech tools such as surveillance, deep fakes, and generally technologies that allow autocracies to consolidate power, primarily through access to data.

We can reign in and control technology; regulate its creation, use, and exportation; or punish our reliance on it. Other responses include flooding the public marketplace with ideas, breaking up the large social media platforms, and using education to combat technology's influence and effects.

Tech companies will not likely to self-regulate, but many participants would support legislation that would regulate for at least some basic level of screening for fake news. Most participants did not think an antitrust approach was likely to work. There are several legislative solutions to pursue, including the Beneficial Ownership Disclosure Bill, the Illicit Cash Act, and the Corporate Transparency Act, which may provide some antidote to foreign influence and disinformation campaigns.

Public Keynote: How Technology Advances Autocracy and What Democracies Can Do About It

This keynote panel presentation opened to the public took place on November 21, 2019, in Fitts Auditorium at the University of Pennsylvania Carey Law School. The keynote panelists were:

David D. Cole is the National Legal Director of the American Civil Liberties Union. Before joining the ACLU in July 2016, he was the Hon. George J. Mitchell Professor in Law and Public Policy at the Georgetown University Law Center from March 2014 through December 2016.

Richard Fontaine is the Chief Executive Officer of the Center for a New American Security (CNAS). Prior to joining CNAS, he worked at the State Department and the National Security Council, and on the staff of the Senate Foreign Relations Committee.

Kara Frederick is a Fellow for the Technology and National Security Program at the Center for a New American Security (CNAS). Prior to joining CNAS, Kara helped create and lead Facebook's Global Security Counterterrorism Analysis Program.

Marwan M. Kraidy is Professor of Communication, the Anthony Shadid Chair in Global Media, Politics and Culture, and the Founding Director of the Center for Advanced Research in Global Communication (CARGC) at the Annenberg School for Communication at the University of Pennsylvania.

Professor Claire Finkelstein, Algernon Biddle Professor of Law and Professor of Philosophy and CERL's Faculty Director, moderated the discussion.

Panelists Richard Fontaine and Kara Frederick co-authored "The Autocrat's New Tool Kit," an article that appeared in the March 15, 2019, issue of *The Wall Street Journal*. The piece brought national attention to the connection between technology and autocracy, stating that "[the technologies] will allow strongmen and police states to bolster their internal grip, undermine basic rights and spread illiberal practices beyond their own borders." This provocative prediction guided the panel discussion.