How Artificial Intelligence Will Reshape the Global Order

The Coming Competition Between Digital Authoritarianism and Liberal Democracy

By Nicholas Wright

The debate over the effects of artificial intelligence has been dominated by two themes. One is the fear of a singularity, an event in which an AI exceeds human intelligence and escapes human control, with possibly disastrous consequences. The other is the worry that a new industrial revolution will allow machines to disrupt and replace humans in every—or almost every—area of society, from transport to the military to healthcare.

There is also a third way in which AI promises to reshape the world. By allowing governments to monitor, understand, and control their citizens far more closely than ever before, AI will offer authoritarian countries a plausible alternative to liberal democracy, the first since the end of the Cold War. That will spark renewed international competition between social systems.

For decades, most political theorists have believed that liberal democracy offers the only path to sustained economic success. Either governments could repress their people and remain poor or liberate them and reap the economic benefits. Some repressive countries managed to grow their economies for a time, but in the long run authoritarianism always meant stagnation. AI promises to upend that dichotomy. It offers a plausible way for big, economically advanced countries to make their citizens rich while maintaining control over them.

Some countries are already moving in this direction. China has begun to construct a digital authoritarian state by using surveillance and machine learning tools to control restive populations, and by creating what it calls a “social credit system.” Several like-minded countries have begun to buy or emulate Chinese systems. Just as competition between liberal democratic, fascist, and communist social systems defined much of the twentieth century, so the struggle between liberal democracy and digital authoritarianism is set to define the twenty-first.

DIGITAL AUTHORITARIANISM

New technologies will enable high levels of social control at a reasonable cost. Governments will be able selectively censor topics and behaviors to allow information for economically productive activities to flow freely, while curbing political discussions that might damage the regime. China’s so-called Great Firewall provides an early demonstration of this kind of selective censorship.

As well as retroactively censoring speech, AI and big data will allow predictive control of potential dissenters. This will resemble Amazon or Google’s consumer targeting but will be much more effective, as authoritarian governments will be able to draw on data in ways that are not allowed in liberal democracies. Amazon and Google have access only to data from some accounts and devices; an AI designed for social control will draw data from the multiplicity of devices someone interacts with during their daily life. And even more important, authoritarian regimes will have no compunction about combining such data with information from tax returns, medical records, criminal records, sexual-health clinics, bank statements, genetic screenings, physical information (such as location, biometrics, and CCTV monitoring using facial recognition software), and information gleaned from family and friends. AI is as good as the data it has access to. Unfortunately, the quantity and quality of data available to governments on every citizen will prove excellent for training AI systems.

Even the mere existence of this kind of predictive control will help authoritarians. Self-censorship was perhaps the East German Stasi's most important disciplinary mechanism. AI will make the tactic dramatically more effective. People will know that the omnipresent monitoring of their physical and digital activities will be used to predict undesired behavior, even actions they are merely contemplating. From a technical perspective, such predictions are no different from using AI health-care systems to predict diseases in seemingly healthy people before their symptoms show.

In order to prevent the system from making negative predictions, many people will begin to mimic the behaviors of a "responsible" member of society. These may be as subtle as how long one's eyes look at different elements on a phone screen. This will improve social control not only by forcing people to act in certain ways, but also by changing the way they think. A central finding in the cognitive science of influence is that making people perform behaviors can change their attitudes and lead to self-reinforcing habits. Making people expound a position makes them more likely to support it, a technique used by the Chinese on U.S. prisoners of war during the Korean War. Salespeople know that getting a potential customer to perform small behaviors can change attitudes to later, bigger requests. More than 60 years of laboratory and fieldwork have shown humans' remarkable capacity to rationalize their behaviors.

As well as more effective control, AI also promises better central economic planning. As Jack Ma, the founder of the Chinese tech titan Alibaba, argues, with enough information, central authorities can direct the economy by planning and predicting market forces. Rather than slow, inflexible, one-size-fits-all plans, AI promises rapid and detailed responses to customers' needs.

There's no guarantee that this kind of digital authoritarianism will work in the long run, but it may not need to, as long as it is a plausible model for which some countries can aim. That will be enough to spark a new ideological competition. If governments start to see digital authoritarianism as a viable alternative to liberal democracy, they will feel no pressure to liberalize. Even if the model fails in the end, attempts to implement it could last for a long time. Communist and fascist models collapsed only after thorough attempts to implement them failed in the real world.

CREATING AND EXPORTING AN ALL-SEEING STATE

No matter how useful a system of social control might prove to a regime, building one would not be easy. Big IT projects are notoriously hard to pull off. They require high levels of coordination, generous funding, and plenty of expertise. For a sense of whether such a system is feasible, it's worth looking to China, the most important non-Western country that might build one.

China has proved that it can deliver huge, society-spanning IT projects, such as the Great Firewall. It also has the funding to build major new systems. Last year, the country's internal security budget was at least $196 billion, a 12 percent increase from 2016. Much of the jump was probably driven by the need for new big data platforms. China also has expertise in AI. Chinese companies are global leaders in AI research and Chinese software engineers often beat their American counterparts in international competitions. Finally, technologies, such as smartphones, that are already widespread can form the backbone of a personal monitoring system. Smartphone ownership rates in China are nearing those in the West and in some areas, such as mobile payments, China is the world leader.

China is already building the core components of a digital authoritarian system. The Great Firewall is sophisticated and well established, and it has tightened over the past year. Freedom House, a think tank, rates China the world's worst abuser of Internet freedom. China is implementing extensive surveillance in the physical world, as well. In 2014, it announced a social credit scheme, which will compute an integrated grade that reflects the quality of every citizen's conduct, as understood by the government. The development of China's surveillance state has gone furthest in Xinjiang Province, where it is being used to monitor and control the Muslim Uighur population. Those whom the system deems unsafe are shut out of everyday life; many are even sent to reeducation centers. If Beijing wants, it could roll out the system nationwide.

To be sure, ability is not the same as intention. But China seems to be moving toward authoritarianism and away from any suggestion of liberalization. The government clearly believes that AI and big data will do much to enable this new direction. China's 2017 AI Development Plan describes how the ability to predict and "grasp group cognition" means "AI brings new opportunities for social construction."

Digital authoritarianism is not confined to China. Beijing is exporting its model.The Great Firewall approach to the Internet has spread to Thailand and Vietnam. According to news reports, Chinese experts have provided support for government censors in Sri Lanka and supplied surveillance or censorship equipment to Ethiopia, Iran, Russia, Zambia, and Zimbabwe. Earlier this year, the Chinese AI firm Yitu sold "wearable cameras with artificial intelligence-powered facial-recognition technology" to Malaysian law enforcement.

More broadly, China and Russia have pushed back against the U.S. conception of a free, borderless, and global Internet. China uses its diplomatic and market power to influence global technical standards and normalize the idea that domestic governments should control the Internet in ways that sharply limit individual freedom. After reportedly heated competition for influence over a new forum that will set international standards for AI, the United States secured the secretariat, which helps guide the group's decisions, while Beijing hosted its first meeting, this April, and Wael Diab, a senior director at Huawei, secured the chairmanship of the committee. To the governments that employ them, these measures may seem defensive—necessary to ensure domestic control—but other governments may perceive them as tantamount to attacks on their way of life.

THE DEMOCRATIC RESPONSE

The rise of an authoritarian technological model of governance could, perhaps counterintuitively, rejuvenate liberal democracies.How liberal democracies respond to AI's challenges and opportunities depends partly on how they deal with them internally and partly on how they deal with the authoritarian alternative externally. In both cases, grounds exist for guarded optimism.

Internally, although established democracies will need to make concerted efforts to manage the rise of new technologies, the challenges aren't obviously greater than those democracies have overcome before. One big reason for optimism is path dependence. Countries with strong traditions of individual liberty will likely go in one direction with new technology; those without them will likely go another. Strong forces within U.S. society have long pushed back against domestic government mass surveillance programs, albeit with variable success. In the early years of this century, for example, the Defense Advanced Research Projects Agency began to construct "Total Information Awareness" domestic surveillance systems to bring together medical, financial, physical and other data. Opposition from media and civil liberties groups led Congress to defund the program, although it left some workarounds hidden from the public at the time. Most citizens in liberal democracies acknowledge the need for espionage abroad and domestic counterterrorism surveillance, but powerful checks and balances constrain the state's security apparatus. Those checks and balances are under attack today and need fortification, but this will be more a repeat of past efforts than a fundamentally new challenge.

In the West, governments are not the only ones to pose a threat to individual freedoms. Oligopolistic technology companies are concentrating power by gobbling up competitors and lobbying governments to enact favorable regulations. Yet societies have overcome this challenge before, after past technological revolutions. Think of U.S. President Theodore Roosevelt's trust-busting, AT&T's breakup in the 1980s, and the limits that regulators put on Microsoft during the Internet's rise in the 1990s.

Digital giants are also hurting media diversity and support for public interest content as well as creating a Wild West in political advertising. But previously radical new technologies, such as radio and television posed similar problems and societies rose to the challenge. In the end, regulation will likely catch up with the new definitions of "media" and "publisher" created by the Internet. Facebook Chief Executive Mark Zuckerberg resisted labeling political advertising in the same way as is required on television, until political pressure forced his hand last year.

Liberal democracies are unlikely to be won over to digital authoritarianism. Recent polling suggests that a declining proportion in Western societies view democracy as "essential," but this is a long way from a genuine weakening of Western democracy.

The external challenge of a new authoritarian competitor may perhaps strengthen liberal democracies. The human tendency to frame competition in us versus them terms may lead Western countries to define their attitudes to censorship and surveillance at least partly in opposition to the new competition. Most people find the nitty-gritty of data policy boring and pay little attention to the risks of surveillance. But when these issues underpin a dystopian regime in the real world they will prove neither boring nor abstract. Governments and technology firms in liberal democracies will have to explain how they are different.

LESSONS FOR THE WEST

The West can do very little to change the trajectory of a country as capable and confident as China. Digital authoritarian states will likely be around for a while. To compete with them, liberal democracies will need clear strategies. First, governments and societies should rigorously limit domestic surveillance and manipulation. Technology giants should be broken up and regulated. Governments need to ensure a diverse, healthy media environment, for instance by ensuring that overmighty gatekeepers such as Facebook do not reduce media plurality; funding public service broadcasting; and updating the regulations covering political advertising to fit the online world. They should enact laws preventing technology firms from exploiting other sources of personal data, such as medical records, on their customers and should radically curtail data collection from across the multiplicity of platforms with which people come into contact. Even governments should be banned from using such data except in a few circumstances, such as counterterrorism operations.

Second, Western countries should work to influence how states that are neither solidly democratic nor solidly authoritarian implement AI and big data systems. They should provide aid to develop states' physical and regulatory infrastructure and use the access provided by that aid to prevent governments from using joined-up data. They should promote international norms that respect individual privacy as well as state sovereignty. And they should demarcate the use of AI and metadata for legitimate national security purposes from its use in suppressing human rights.

Finally, Western countries must prepare to push back against the digital authoritarian heartland. Vast AI systems will prove vulnerable to disruption, although as regimes come to rely ever more on them for security, governments will have to take care that tit-for-tat cycles of retribution don’t spiral out of control. Systems that selectively censor communications will enable economic creativity but will also inevitably reveal the outside world. Winning the contest with digital authoritarian governments will not be impossible—as long as liberal democracies can summon the necessary political will to join the struggle.

Published in “Foreign Affairs”