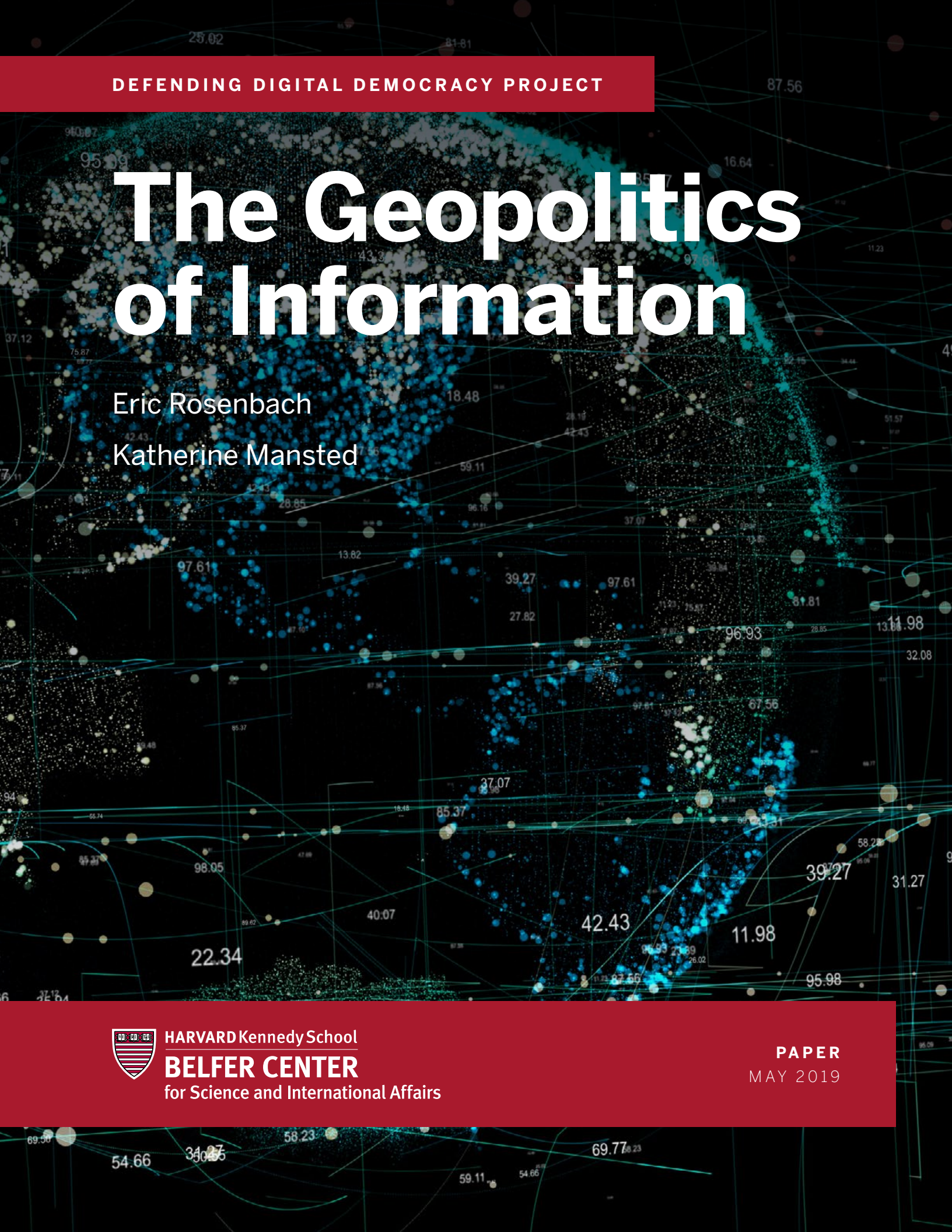


DEFENDING DIGITAL DEMOCRACY PROJECT

The Geopolitics of Information

Eric Rosenbach

Katherine Mansted

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2019

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Design and layout by Andrew Facini

Cover photo: Adobe Stock

Printed in the United States of America

DEFENDING DIGITAL DEMOCRACY PROJECT

The Geopolitics of Information

Eric Rosenbach

Katherine Mansted

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
MAY 2019

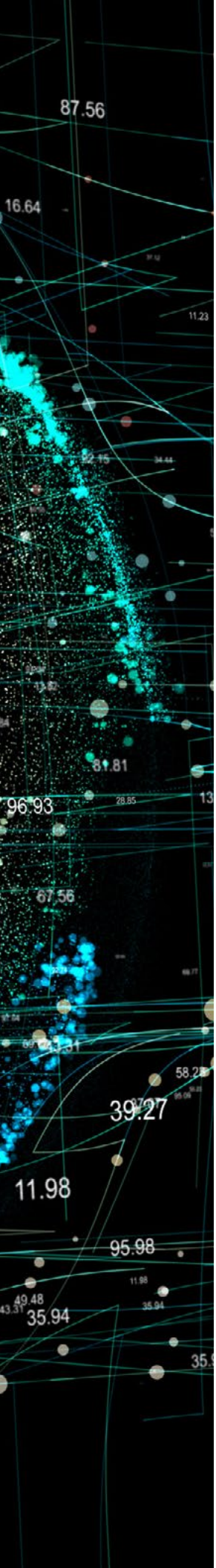
About the Authors

Eric Rosenbach is Co-Director of the Belfer Center and a Harvard Kennedy School Public Policy Lecturer. He also heads the Center's Defending Digital Democracy project.

Katherine Mansted is a Fellow at the Belfer Center and a Senior Adviser at the Australian National University's National Security College.

Table of Contents


35.94
22.34
25.02
81.81
35.94
97.04
85.37
40.07
98.53
26.02
96.16
49.48
59.11
95.09
85.37
58.23
32.08
97.61
43.31
97.61
97.04
95.98
22.34
37.12
75.87
97.04
18.48
42.43
42.43
59.11
39.27
69.77
98.53
28.85
96.16
13.82
37.07
13.82
18.48
97.61
39.27
97.61
18.48
27.82
98.53
75.87
35.94
34.44
85.37
37.07
98.05
40.07
42.43
75.23
22.34
13.82
63.66
35.94
85.37
43.31
58.23
69.77
54.66
59.11
54.66



Introduction

Information is now the world's most consequential and contested geopolitical resource. The world's most profitable businesses have asserted for years that data is the "new oil." Political campaigns—and foreign intelligence operatives—have shown over the past two American presidential elections that data-driven social media is the key to public opinion. Leading scientists and technologists understand that good datasets, not just algorithms, will give them a competitive edge.

Data-driven innovation is not only disrupting economies and societies; it is reshaping relations between nations. The pursuit of information power—involving states' ability to use information to influence, decide, create and communicate—is causing states to rewrite their terms of engagement with markets and citizens, and to redefine national interests and strategic priorities. In short, information power is altering the nature and behavior of the fundamental building block of international relations, the state, with potentially seismic consequences.

Authoritarian governments recognize the strategic importance of information and over the past five years have operationalized powerful domestic and international information strategies. They are cauterizing their domestic information environments and shutting off their citizens from global information flows, while weaponizing information to attack and destabilize democracies. In particular, China and Russia believe that strategic competition in the 21st century is characterized by a zero-sum contest for control of data, as well as the technology and talent needed to convert data into useful information.

Democracies remain fundamentally unprepared for strategic competition in the Information Age. For the United States in particular, as the importance of information as a geopolitical resource has waxed, its information dominance has waned. Since the end of the Cold War, America's supremacy in information technologies seemed unassailable—not least because of its central role in creating the Internet and overall economic primacy. Democracies have also considered any type of information strategy to be largely unneeded: government involvement in the domestic information

environment feels Orwellian, while democracies believed that their "inherently benign" foreign policy didn't need extensive influence operations.

However, to compete and thrive in the 21st century, democracies, and the United States in particular, must develop new national security and economic strategies that address the geopolitics of information. In the 20th century, market capitalist democracies geared infrastructure, energy, trade, and even social policy to protect and advance that era's key source of power—manufacturing. In this century, democracies must better account for information geopolitics across all dimensions of domestic policy and national strategy.

Information as a Source of Power

Information is more important to world affairs today than at any previous point in history as a result of recent advances in data-driven technologies. These advances have revolutionized each of the four key facets of information power: to influence the political and economic environment of other actors; to create economic growth and wealth; to enable a decision-making edge over competitors; and to communicate quickly and securely.

First, the global penetration of the Internet has revolutionized the potential for information ***to influence*** other actors. Propaganda is as old as war itself, and has been used by advertising firms and PR experts to drive consumer behavior for at least a century.[A] But, as Russia's ongoing use of digital disinformation to interfere in American politics demonstrates, digital networks and the widespread adoption of social media platforms have dramatically expanded the scale, scope and geographic reach of state influence operations. Russian influence campaigns are, however, only prototypes of the sophisticated and insidious influence operations states will soon be able to deploy. In the next five years, advances in automation and artificial

A Father of public relations, Edward Bernays, explained in 1928 that it was "the astounding success" of the mass broadcast propaganda of World War I that opened his eyes to the immense commercial and political possibilities of "regimenting the public mind." His how-to manual, *Propaganda*, set the blueprint for 20th century ad firms, politicians, and even social activists on how they could shape popular tastes and ideas to advance their interests.

intelligence (AI) will enable propagandists to effectively run mass influence campaigns on auto-pilot, to micro-target those individuals and groups most vulnerable to manipulation, to continuously improve their tactics and messages based on real-time digital feedback, and to cheaply and quickly computer-generate fake audio and visual material.[1]

Second, advances in machine learning (a subset of AI) are enabling entities with access to significant amounts of raw data ***to make better decisions***. The value of data to humans has always been limited by the "information overload" problem: that is, there are limits to how much information humans can feasibly collect and, the more information we have, the harder it becomes to make sense of it. The 1880 U.S. census, for example, asked just 26 questions but took eight years to process.[B] Even 20th century machines struggled to process information quickly—meaning that decisions often hinged on limited datasets, gut feelings, or a combination of both. Today, advances in computer processing power and machine learning are solving the information overload problem. Indeed, machine learning systems work best when confronted with vast datasets, since huge amounts of initial "training" data and ongoing "feedback" data enable them to refine their algorithms over time to produce better outputs. At the same time, billions of powerful computer sensors are now embedded in Internet-connected personal, household and industrial devices around the world. In a phenomenon big data gurus Viktor Mayer-Schönberger and Kenneth Neil Cukier call "datafication," information that was once lost or simply unobserved is now meticulously collected and catalogued.[2] Increasingly, the full range of human, business, and societal activities will be transparent to machine analysis.

Third, data and information now play a central role in nations' ability ***to create*** the wealth and prosperity essential to developed economies. When in May 2017 *The Economist* argued that data had replaced oil as "the world's most valuable resource,"[3] the magazine was capturing a powerful zeitgeist. Since then, world leaders from Narendra Modi[4] to Shinzo Abe[5] and Angela Merkel[6] have declared that data will be the 21st century's most important driver of economic growth. Some analysts go further—Viktor Mayer-Schönberger predicts that "data capitalism" will eventually replace finance capitalism as the global

B The challenges of that census helped to prompt Herman Hollerith to invent the punched card tabulating machine, and with it the origins of 20th century automated data processing and computing giant IBM.

economy's organizing principle.[7] Certainly, companies whose core business involves acquiring, processing and using data now almost exclusively make up the top ten of the world's most valuable listed firms.[C] Data enables firms to better target their consumers and, via advanced data analytics, to improve business processes and products, discover new knowledge, and build new business models. Today, nearly every industry sector in advanced economies is using or exploring data-driven machine-learning applications.[D] But while companies have bet big on data analytics, the McKinsey Global Institute estimates that they have realized only a small fraction of the many hundred-billion dollars of the economic opportunity.[8] Most of the potential for value creation in data analytics remains open to capture and, in coming years, as technology and in particular machine learning software advances, will continue to expand,[E] positioning data at the center of global economic competition for decades to come.

Fourth, it is axiomatic to observe that advances in Internet, mobile, and related technologies have revolutionized the speed, scale, and scope of actors' ability ***to communicate*** information. For most of history, the ability to communicate quickly and securely was the most important facet of information power. During the Napoleonic Wars, the Royal Navy's Admiral Lord Cochrane famously destroyed French semaphore towers along the Mediterranean coastline—seizing the initiative for Britain. The Internet itself was invented to insulate America's nuclear command and control communications system from similar acts of sabotage. Lines of communication are not just important for militaries. In the 19th century, the Rothschild family's pan-European network of business agents and couriers provided the then-world's wealthiest business empire with a peerless

C Around 37% of the rise in the value of all firms in the S&P 500 index since 2013 is due to six information giants: Alphabet (Google's parent), Amazon, Apple, Facebook, Microsoft and Netflix. About 28% of the rise in Chinese equities over the same period is due to two Chinese information conglomerates: Alibaba and Tencent: *The Economist,* November 1, 2018, https://www.economist.com/business/2018/11/03/big-techs-sell-off.

D Even erstwhile titans of the industrial age now market themselves based on their ability to aggregate and process data. See, for example, GE's "Predix Platform," which promises to extract value from the "massive amounts of data" generated by its customers' industrial operations: https://www.ge.com/digital/iiot-platform.

E This assessment also appears to be backed by investor behavior. By some estimations, up to 80 percent and up to 60 percent of the share price of Facebook and Google, respectively, is attributable to future growth projections—indicating that the market is confident in their ability to collect and monetize increasingly vast tranches of data. See: Rod Sims. "Don't Rely on Amateur Journalists," *The Mandarin*, July 4, 2018, https://www.themandarin.com.au/95208-rod-sims-dont-rely-on-amateur-journalists/.

competitive advantage: exclusive access to financial and political information.[F] In the 21st century, the ability to establish and protect, or disrupt, information flows will continue to play a decisive role in world affairs.

The New Great Game

The rising economic and political importance of information is impacting states' policy choices and priorities and, in turn, how they wield power, compete and prepare for conflict in the 21st century. There are four ways that the rising importance of information has ushered in an era in which information geopolitics drives world affairs.

All information is strategic

Writing in *Foreign Affairs Magazine* in 1998 about the rising geopolitical significance of information, Robert Keohane and Joseph Nye[9] drew a distinction between three types of information: free, commercial, and strategic. They defined free information as the personal information individuals willingly gave up in online interactions; while commercial information such as intellectual property (IP) was only relevant to businesses. Only one narrow category of information— "strategic information" such as state secrets—would be of interest to governments, and relevant to world affairs. Today, the categories set out by Keohane and Nye are blurring. Every piece of information now has the potential to be strategic.

The strategic importance of business IP to governments today is relatively self-evident. The same advancements in machine learning that enable Facebook to better recognize your friends and tag them in photos can be adapted by militaries to identify and target combatants. The self-driving algorithms that pilot a Tesla can be adjusted to operate an autonomous tank. Significantly, it is not just commercial software that states have an interest in. Raw

F News of Wellington's victory at Waterloo famously reached the Rothschilds in London a full day before official messengers; the family's early access to information made them better investors, not to mention politically valuable: Niall Ferguson. *The House of Rothschild: The World's Banker, 1849-1999*, 2000.

data held by myriad types of corporate entities also has strategic value. Machine learning is now at a stage of development that a technical wunderkind is no longer needed to write a good learning algorithm. Instead, what developers most require are troves of high-quality data to train and optimize algorithms over time. Data about the natural and built environments, as well as human behavior and psychology held by logistics, health, manufacturing, financial services and consumer goods companies will train the algorithms that empower states to dominate the physical, electronic and intellectual terrain of the future. As a result, states have a strong interest in accessing (or stealing) the commercial information that Keohane and Nye once classified as relatively disconnected from geopolitics.

Personal information can also be strategically significant. The personal lives of political and military leaders have always been of interest to spies and saboteurs. But these activities have historically been limited by the need for human operatives to collect and interpret intelligence. Digitization has dramatically increased the breadth and depth of information available to intelligence agents. Fitbits, GPS-linked phones, Internet-connected pacemakers and myriad other devices weave a rich tapestry that in the wrong hands can be used to blackmail, discredit or outwit decision-makers. In 2018, state-sponsored hackers targeted and successfully stole the Singaporean Prime Minister's digital health records, for purposes as of yet unrevealed.[10] Moreover, with computers now able to make sense of huge datasets, all people linked to the government, not just senior leaders, are potential foreign intelligence targets. In 2015, China hacked into the U.S. Office of Personnel Management, stealing sensitive personal information on four million people who had undergone U.S. Government security checks—acquiring a tremendous resource for espionage and future blackmail and influence operations.

States also have a strategic interest in acquiring information about foreign private citizens. Information about an individual's emotional state, beliefs, preferences, and social relationships can be used to influence how they think and act. At a domestic level, political campaigns invest heavily in personal information about voters and use data analytics software to micro-target their campaign messages.[11] Google and Facebook have built two of history's most successful business empires based on their ability to

harvest and monetize consumers' personal information in order to change online behavior and real-world decisions.[12] Of course, if democratic political parties and companies can use personal information to change citizens' beliefs and decisions, so too can states. In its disinformation campaign during the 2016 U.S. presidential election, Russia used social media information to identify and then target those people who were most vulnerable to its divisive narratives.[G] The coming wave of AI research will help computers to interact with humans in increasingly "natural" and persuasive ways, at scale and in real-time. As a result, computational propaganda is likely to become a more prevalent, and potent, tool of state influence, and everyday citizens' personal information—once of scant relevance to world affairs—will become an even more strategically valuable resource.

The rise of information mercantilism

Increasingly, governments protect and control their information-related companies and infrastructure. This is a trend most pronounced in authoritarian states, but is by no means limited to them. At a minimum, given the role that data plays in creating economic growth and wealth, all states have a clear economic interest to create regulatory settings that will help their data-rich economy segments thrive. Additionally, despite data's intangibility, the ability to acquire data and use it effectively is strongly associated with traditional geopolitical factors—like population size. As one Indian politician put it: "India has no coltan or rare earths, little oil, and not enough water. What it does have is people… that makes India potentially very rich in what has been called the 'new oil'".[13] Similarly, Lu Qi, a former chief operating officer of Baidu (known as "China's Google," although the analogy is imperfect), predicts that China's vast, digitally immersed population will provide his country with the raw data needed to become the world's preeminent technological power.[14]

Increasingly many states also believe that they are in a zero-sum race to acquire and use data. Certainly, the biggest commercial success stories of

G For example, Russian operatives pushed divisive content to Facebook users who had previously "liked" posts related to race, or who belonged to groups either supporting or opposing the Black Lives Matter movement.

the Information Age—Alphabet (Google's parent), Facebook, Amazon, Alibaba, and Tencent—are monopolists. One explanation for this is that access to data tends to be a virtuous cycle: more data lets companies build better applications and technologies, which accelerates their profitability and popularity, and in turn ability to harvest and use even more data. Transposing this commercial reality to geopolitics, Indian Prime Minister Narendra Modi believes that "whoever acquires and controls" data will attain "hegemony."[15] In his recent book *AI Superpowers*, venture capitalist Kai-Fu Lee predicts that China's widening lead in AI (at essence, a blanket term for computer programs that convert data to decisions[H]) will not only ensure the "economic balance of power tilts in China's favor," but will tilt "political influence and 'soft power,' toward China," and cement its "cultural and ideological footprint around the globe." Russia's Vladimir Putin also subscribes to this zero-sum view, declaring in 2017 that "whoever becomes the leader in [AI] will become the ruler of the world."[16] Most developed economies now have national AI strategies.[17] None are more mercantilist than China's "Development Plan for a New Generation of Artificial Intelligence," which aims through a combination of government subsidies and incentives to push China into leading the world in AI by 2030.

This winner-takes-all ethos means that states do not just want to generate data; they also have an interest in limiting or excluding other countries from accessing it. In November 2016, China enacted a comprehensive cybersecurity law that allows the government to surveil nearly every aspect of its citizen lives while also limiting the access that foreign firms have to data in the country. Tough "data localization" laws have also been introduced in Russia and India, requiring that significant amounts of personal and commercial data can only be stored and in some cases processed inside their territory.

More perniciously, in a zero-sum game, data theft also pays. States have an incentive to sponsor, or at least turn a blind eye to, data grabs by their companies. Just as privateers in the Age of Discovery enriched themselves while serving the strategic objectives of their state sponsors, corporate data

H In this paper, we are limiting our discussion of AI to "narrow AI" systems which take data from a specific domain, and apply it to a particular problem, to optimize for a specific outcome. All AI technologies that exist today are narrow AI. "General AI," the name for all-purpose systems able to perform any intellectual task a human can, is unlikely to eventuate within the authors' lifetimes: see, for example, James Vincent. "This is when AI's Top Researchers Think Artificial General Intelligence will be Achieved," *The Verge,* November 27, 2018, https://www.theverge.com/2018/11/27/18114362/ai-artificial-general-intelligence-when-achieved-martin-ford-book.

thieves can create win-win outcomes for data-hungry states. Consider the massive data breach of credit reporting giant Equifax in 2017, in which hackers stole the financial and personal information of at least 143 million Americans. Evidence suggests that the hack was state-sponsored, that it emanated from China, and that[18] an aspiring world AI-leader like China had strong motive for being involved in the breach. As Kai-Fu Lee writes, China's digitally immersed consumers are providing oodles of data to Chinese e-commerce giants, but China's banking, insurance and healthcare industries lag behind their more established American counterparts, which have been collecting, labelling, and monetizing business and consumer information for decades.[19] There's also evidence that state-sponsored hackers have been behind major hacks against some of the world's biggest health insurance, legal, and other traditional services industries,[20] a trend that is likely to accelerate.

Protecting and investing in their information industries may not just be an economic choice for states; but a strategic imperative. Technological innovation now predominantly comes from the private sector before it has military or intelligence applications. Since around 2015, these dynamics have fueled an accelerating pace of legal and policy changes in advanced economies. The U.S. Congress recently reformed its existing foreign investment regime to make it even more difficult for Chinese and other foreign investors to acquire sensitive technologies and access to Americans' personal data, and further reforms are likely. Beginning in 2015, the U.S Department of Defense recognized that in order to remain the world's most potent military it would need to "rebuild bridges" with Silicon Valley and the tech sector. Led by Secretary Ash Carter, the Pentagon established new outposts in U.S. tech hubs focused on finding new ways for the military to leverage big data and AI-enabled technologies. China's approach is more muscular. Under Xi Jinping's "civil-military fusion" doctrine, any technologies held in the private and academic sectors—whether locally developed or imported—must be shared with the Chinese military.[21]

The rise of information theft, manipulation, and sabotage

The rising importance of information to world affairs is exacerbating old and creating new vectors for state conflict. We have already seen that the economic and strategic importance of data is an incentive for states to sponsor cyberattacks and industrial espionage against rival countries' companies.

Additionally, technological advances in computing, especially machine learning, are allowing states to use information to influence, manipulate and coerce with unprecedented scale and effect. This particular aspect of information geopolitics jumps out in the 2017 U.S. National Security Strategy, which devotes an entire chapter to "information statecraft," and the risk posed by countries like Russia and China.[22] One practical consequence of both trends is that competitors, like the United States and China, are increasingly taking measures to decouple aspects of their economy—reversing, or at least checking, the globalization that has been the dominant ordering principle of the economic world order since the end of the Cold War.[23] Even the United Kingdom's Ministry of Defense has flagged that democracies may need to more carefully balance digital openness and control in the future, including by considering "national or regional cyber borders" to defend against threats in the information space.[24] China has already pivoted heavily to control, with its extensive system of Internet censorship and propaganda, and restrictions on market access for foreign media and technology companies. In 2019, Russian Internet service providers will test a "disconnect" of Russia's Internet from the global Internet; part of a national strategy that also aims to ensure that by 2020, 95 percent of its domestic Internet traffic never needs to leave Russia's borders.[25] American lawmakers are also mulling further action to insulate Americans from foreign disinformation. The powerful, bipartisan Senate Intelligence Committee has heaped public pressure on Facebook, Google, and Twitter to detect and exclude foreign manipulation on their platforms.[26]

Digital sabotage is also emerging as a new and expanding vector for interstate conflict. To this point, most state-sponsored cyberattacks have been for the purposes of stealing information, or impairing the availability

of communication or computing systems. However, as technological advances rapidly improve our ability to turn data into decisions, and more entities adopt these types of technology, we should expect a sharp rise in cyberattacks against the integrity of data itself. Today, more and more decision-making, from what is shown on news and social media feeds, to insurance, lending and investment assessments, and preliminary government and judicial decisions are machine-assisted via automation and / or AI agents.[27] Decision-assistance systems rely on data to operate, making them weak targets for data "food poisoning" attacks. Disrupt or manipulate the data diet they feed on, and their outputs will be corrupted—perhaps unbeknown to the individuals or institutions that depend on them. The Stuxnet malware, which infected computers controlling nuclear centrifuges at Iran's Natanz nuclear plant, is an early example of this type of data integrity attack. The malware not only caused Natanz's centrifuges to malfunction, but fed monitoring software bogus data so that the attack could progress unseen. Stuxnet affected a limited number of industrial control devices at a site linked to a nuclear weapons program. As more of the world's political, commercial and personal decisions become machine-assisted, the target for data integrity attacks will become much wider, and the potential scale and magnitude of them far greater. Through data integrity attacks, a state adversary could advance its agenda or damage a competitor by subtly changing the decisions made by markets, militaries, governments and courts. A data integrity attack need not be successful in order to be damaging. Even the perception that data inputs into machine-assisted decisions have been corrupted could seriously undermine confidence in the market, a government, or democracy itself.

The rise of information authoritarians

The pursuit of information power is not only directly changing how states compete and conflict with each other; it is also changing governments' relationships with their own citizens. In turn, this is likely to alter the behavior of states to each other.

Chinese, Russian, and many Middle Eastern citizens experience the Internet differently than their peer citizens in western countries. At the network level,

their governments block, censor, and re-route "inappropriate" traffic; at the content level, the platforms they use to search, socialize, and obtain news are flooded with government-orchestrated messaging. China in particular under President Xi's leadership has become an information authoritarian that seeks to manipulate and control its population through data-driven technologies. China's emerging social credit system collects vast amounts of social and economic data about citizens to assess whether or not they are "good" Chinese Communist Party members, and rewards (or punishes) accordingly. Its rapidly expanding AI-assisted surveillance system means that Chinese citizens' real and digital lives are increasingly policed.[28] Access to citizens' data, and use of machine learning systems to analyze it, are increasingly offering centralized governments the opportunity to shape the real-time behaviors, and even thoughts, of their own citizens in ways that would "make George Orwell blush and the East German Stasi salivate."[29] Ethical issues aside, the prospect of authoritarian governments being able to consolidate control over their citizens' experiences and interactions, to identify and punish dissenters, and even re-educate wrongdoers in real time, could have three significant implications for international relations.

First, as their regime legitimacy becomes increasingly dependent on censorship and manipulation, information authoritarians are likely to consider information control as a core national interest—equivalent to even economic and physical security interests. This dynamic increases the risk of diplomatic deadlock and inadvertent escalation. For example, what democracies perceive as private activities by their media organizations, companies, education and civil society networks may be perceived by an information authoritarian as a national security threat or deliberate provocation, and responded to as such. China has already demonstrated that it is willing to use offensive cyber measures against American companies that help Chinese citizens evade Internet censorship.[I] Russian strategists believe that the grassroots movements and social media protests of the Arab Spring and "color revolutions" reflect a form of western irregular warfare;[30] a perception that the United States enabled similar uprisings within Russia itself, for example, is likely to be treated as a security threat, and major provocation. Democracies will need

I In 2015 Chinese hackers launched a massive distributed denial-of-service against U.S.-headquartered website GitHub, the world's biggest repository of open source code, after GitHub hosted content on how to subvert Chinese online censorship.

to learn to ensure their foreign and defense policies account for states with very different hierarchies of national interests to their own.

Second, information authoritarians may be more likely to engage in coercive or aggressive behaviors. Authoritarians' tightening control over their information environment decouples their citizens' experience from the reality of world events. If the cadre of leaders are in favor of aggression, there could be less space for public debate to question, deliberate on, or otherwise put a brake on their leaders' decisions. Moreover, democratic governments already tend to view unelected governments as illegitimate and unpredictable,[31] but given the tightening control they exercise over citizens and dissenters, information authoritarians could be perceived as even less trustworthy than their "analog" counterparts. Thus, even if they are not more aggressive in fact, information authoritarians may be *perceived* as such, increasing the chances of strategic miscalculations or even outright conflict with democracies. In particular, as China trends even further toward totalitarianism, the United States is likely to become less willing to accommodate its desire for greater global influence—since Americans will not trust that this influence will be used responsibly.[32] This sets the conditions for competition and increased friction in relations between the two countries.

Third, at least in the short term, the information authoritarian model may appeal to less powerful states, causing the spread of information authoritarianism and shifts in alliance structures. States facing internal discord may find the social control offered by the information authoritarian model attractive, and look to stronger information authoritarians as potential partners. As Samuel Huntington argued, increases in political, economic or military power can make an ideology (in this case, a model of government) more attractive, while fueling self-doubt in states with models that produce comparatively less successful results.[33] Perceptions that information authoritarianism produces a more harmonious society and boosts economic productivity could create a sense of determinism about the strength of its leading adopters. In turn, this could cause even democracies to seek closer ties with authoritarians; while increasing internal disillusionment and unrest within democracies themselves. We should note that we believe that the risk of information authoritarians outperforming democracies is a short-term

one only; we firmly believe that in the long-run, democracy will prove best equipped to adapt to the social and economic disruptions of the Information Age. The risk, however, is that perceptions and expectations trump this reality, and that unsustainable short-term gains by information authoritarians cause changes to world affairs that are more lasting.

Toward a National Information Strategy

The United States must treat information as a strategic resource. Leaders must incorporate the new realities of information geopolitics into policy-making across the full spectrum of economic, social and security issues.

Putting information at the center of U.S. policy and strategy will require a significant, whole-of-nation pivot. To this point, successive administrations have shrunk from addressing the challenges of the Information Age.[J] In large part, this has been because they assumed—wrongly—that advances in information technologies would inevitably benefit American actors and interests, and therefore did not merit close watch, or policy action. For example, there has been a persistent belief that the Internet and related technologies are inherently democratizing. Writing in 1996, Joseph Nye and Admiral William Owens hypothesized that better communications and data processing technologies would increase accountability and transparency, and thus truth in the international system.[34] This would benefit states with benign intentions, and disadvantage the greedy and the rule breakers.[K] For decades, American strategists also assumed that digital information is simply not susceptible of state control or manipulation—and so would tend to empower non-government entities, and transnational

J For example, America's recent National Security Strategy lamented that "efforts to counter the exploitation of information by rivals have been tepid and fragmented" and hampered by a lack of "sustained focus" and "properly trained professionals": The White House. *National Security Strategy of the United States of America*, December 2017, 35.

K It was also perpetuated by the libertarian "techno-optimists" who built or funded most of the early Internet technologies in what they thought was their political image. In 1996, cyberlibertarian John Perry Barlow immortalized this techno-optimist zeitgeist in his *Declaration of the Independence of Cyberspace*, which began: "Governments of the Industrial World, you weary giants of flesh and steel… On behalf of the future, I ask you of the past to leave us alone…You have no sovereignty where we gather": *Electronic Frontier Foundation*, January 20, 2016, https://www.eff.org/cyberspace-independence.

networks, again to the disadvantage of authoritarian regimes. It was this belief that caused President Bill Clinton in 2001 to deride China's then-nascent Internet censorship system as like "nailing Jell-O to the wall."[35]

These assumptions have proved enduring. In introducing America's 2011 Cyberspace Strategy,[36] President Obama highlighted what he saw as a core opportunity of cyberspace: the way it empowers "all people to help make their governments more open and responsive." The strategy went on to announce the United States as a "tireless advocate" for activists and journalists using digital technologies to challenge foreign regimes,[37] apparently blind to the reality that just as the Internet can magnify democracy advocates' influence, it can also be co-opted by information authoritarians for purposes of manipulation and subversion. The Obama strategy also underestimated the extent to which a commitment to empower the digital voices of foreign activists would be perceived by information authoritarians as a direct threat to their core national interests.

Contrary to the approach of previous decades, U.S. interests are no longer best served by allowing the future of the information sphere to be determined by other actors—be they authoritarian regimes with a mercantilist, control-centric approach to information, or technology companies focused primarily on generating more data to further bolster their profits. In the absence of a national strategy to protect Americans' data, promote the competitiveness of American firms, and secure our information and technology infrastructure assets, the United States risks ceding its leadership role in future economic, military, and political landscapes. In our view, the United States must adopt a national strategy guided by four principles:

1. **Security and economic strategy must be data-centric.** America's network-centric approach to national security is failing. Focus on the threat of a low probability catastrophic attack on critical infrastructure networks, for example, has distracted leaders from the reality that we are not defending the nation's most precious resource: information. Likewise, the government has done very little to prioritize the centers of gravity for an economy powered by data-driven innovation.

2. **Privacy is a national security priority.** Policies aimed at bolstering U.S. national security and promoting U.S. economic competitiveness must go hand-in-hand with consumer protection. Information authoritarians may ignore consumer rights in pursuit of acquiring information power, but democracies must not. Bolstering the global competitiveness of American companies should remain a top priority, but not at the expense of allowing these companies to collect, use, and sell information without user consent or while under-investing in cybersecurity. This is not just a values-based argument. We should expect that adversary intelligence services will attempt to expand their traditional targets to include the United States' high-quality corporate, research, and consumer datasets in order to train AI systems, and to hone their propaganda and influence operations. Accordingly, in the age of information geopolitics, data protection is not just a matter of individual rights or of protecting business secrets. It is a national security imperative.

3. **A whole-of-government strategy for information competitiveness is required.** Information geopolitics cuts across all aspects of the economy, society and state security apparatus. Authoritarian governments have adopted a highly centralized, mercantilist approach to protecting, acquiring and using information. Centralization will not be the answer for democracies, but coordination must be. Unprecedented cooperation is required across economic, social, defense, intelligence, state department and homeland security portfolios. For example, the American government cannot keep regulatory decisions about information-related companies siloed from foreign policy decisions concerning cyberspace.

4. **Prioritize coordination with the private sector.** The private sector is on the front-lines of information geopolitics. The intelligence community needs to share threat information with the social media platforms that so directly influence Americans' economic and political decisions. Policymakers must be willing to work with private actors to ensure regulatory red tape does not stand in the way of innovation, that public-private partnerships continue to create incentives to accelerate technology development, and that competition settings are correctly calibrated. At the same time, U.S.

technology firms need to understand, and be held accountable for, their role in protecting national security interests.

These principles should be combined with forward-leaning policy action. Specifically:

- **Pass national data security and privacy legislation.** Information is and will be the nation's most import strategic resource for the next century. Yet, even in the face of inadequate data protection practices and damaging data breaches, the United States continues to muddle along with a complex web of state-based and industry-specific requirements. American consumers are worse off because their data is unprotected and, in the event of a personally costly data breach, their rights and access to legal recourse are unclear. American companies are left to deal with competing and possibly contradictory requirements, in particular impacting early innovators and small businesses without the resources to navigate the complex regulatory environment. U.S. policymakers urgently need to pass a national law that will protect user data, reduce regulatory complexity, and spur innovation by reconciling differences in state and federal requirements. While Europe's General Data Protection Regulation (GDPR) is by no means a perfect model and in some respects is inconsistent with other U.S. values, it has been effective at driving corporate investment in data protection. Data protection legislation passed in California in June 2018 will need fine-tuning before taking effect in 2020, but establishes principles that could serve as the foundation for national legislation.
- **Promote competitiveness of U.S. firms in critical sectors.** The U.S. can do a lot more to reduce regulatory red tape, attract top talent, and create incentives to spur innovation in data-driven technologies.
    - *Expedite deployment of next-generation broadband infrastructure.* Broadband infrastructure has been a key driver of the Information Age. If it does not reduce regulatory red tape to expedite deployment of next-generation broadband infrastructure, the United States risks falling behind.

Nationwide 5G deployment is a massive effort requiring equipment installation and associated permits and approval processes across thousands of localities. Policymakers must drive toward regulation that standardizes and fast-tracks local approvals, while giving local authorities the opportunity to provide implementation guidance.

- *Continue public-private partnerships that support advanced technology development*. Within the framework of robust national data privacy and security laws, the U.S. Government should promote more partnerships with civilian companies and academic institutions to make progress on high-priority AI initiatives. The Defense Innovation Unit provides a model for this approach.

- *Win the race for talent.* The United States has a history of prizing and nurturing openness, creativity, and innovation. Our university system is a springboard for raw talent; our legal and government institutions allow new businesses to thrive; and our sophisticated financial system enables the best ideas to be successful. To maintain a competitive edge, the United States needs a foundation of policies and practices that continue to attract top talent, like the heads of AI at Apple, Facebook, Microsoft, and Google's cloud computing division, who were all born outside the United States At a minimum, Congress should ensure that more highly skilled workers are able to obtain H-1B visas. Policymakers should further consider special programs for students and experts in AI and related fields.

- *Consider new anti-trust legislation to reinvigorate American innovation in data-driven information technologies.* Despite the zero-sum mindset of many authoritarians, democracies should not fall into the trap of thinking that bigger must always be better. Getting the balance right between enabling scale, and ensuring competition in data-rich industries will be vital. In the age of information geopolitics, market concentration may have many negative consequences—not least because monopolists, and their products, are single

points of failure. As 2016 showed in stark terms, Facebook's market dominance meant that the business decisions of one single company became the only bulwark between a widespread Russian disinformation campaign, and the American people. Similarly, if only a handful of companies are involved in creating decision-assistance algorithms, there is a risk that their software could become an attractive target for data saboteurs; one accident or breach could result in system-level failure.

- **Protect U.S. information and infrastructure assets.** Promoting U.S. competitiveness in data-driven technologies must be coupled with strong defense that protects key companies and sectors from foreign attacks and takeovers.

    - *Incentivize use of strong encryption.* Making America the world leader in encryption technology could advance both economic and national security interests. Protecting the nation's most important resource will require a significant expansion in use of encryption. The nation's defense and security agencies have relied on encryption to protect their most precious secrets for many decades—the Department of Defense is the largest user of encryption in the world. The U.S. Government must clarify legal questions around encryption and also develop real incentives to promote the development and use of encryption products and platforms to allow individuals and organizations to protect their data.

    - *Limit foreign ownership and provide resources to support firms in key information sectors.* Over the past decade China has systematically targeted investment in and ownership of firms developing data-driven technologies like AI. Congress has increased limitations and oversight of foreign ownership and involvement in data-rich sectors. While important, this should be supplemented with new incentives to sustain American tech firms whose technology does not have an immediate commercial application.

- **Craft and promote genuine narratives.** Since the end of the Cold War, liberal strategists have tended to believe that liberal democracies "sell themselves." Hence the emergence of concepts such as "soft power"—predicated on the power of attraction, rather than coercion. The United States has been particularly arrogant in this way: leaders of all political stripes assume that actions will be interpreted by other states as largely benign, obviating a need to explain or defend the merits of Washington's strategic view of the world. The rise of information authoritarians, and nationalistic governments like those in Turkey, Poland and the Philippines, demands that democracies proactively engage the world with authentic narratives that highlight the intrinsic value of democracy and liberal values. In general, democratic governments lack the ability and sophistication to advance these narratives; thus, a well-resourced fund administered by a new federally-funded research and development center (FFRDC) should lead this effort.

- **Bolster proactive defensive operations in cyberspace.** Democracies, and the United States in particular, cannot sit back and watch the incoming volleys of attacks from information authoritarians. The national security community must mount a proactive defense that includes cyber operations to defang the adversary networks used to manipulate democracies and steal valuable information. These operations must be consistent with American values and international law and should focus on disrupting and degrading adversary technical capabilities and IT systems rather than relying on counter-propaganda or manipulation.

- **Articulate a clear posture on deterrence in the age of information geopolitics.** The nations controlled by information authoritarians are brittle—they are very susceptible to information and cyber operations against their otherwise tightly controlled information environments. Leaders of democracies, and the United States in particular, should explicitly signal that information attacks against democracies will result in significant risk to information authoritarians' control of their information environment—but should also be aware that this is not a course of action to be pursued lightly. Work is required to understand thresholds and escalation dynamics in information-based contests.

Conclusion

Key technological advancements have ushered in a new era of information geopolitics. This is changing how states engage with their citizens and with each other, define their national interest and strategic priorities, and project power onto the world stage. In particular, the belief that the data-driven economy is a winner-takes-all environment is pushing states and their domestic industry much closer together. To maintain power into the future—while protecting the institutions and values that have guided them in the past—the United States and similar democracies must adopt a coordinated national information strategy. This is not an easy path, and it is one that is strewn with difficult balances. Democracies must build their capacity to produce, refine, and protect information; but avoid the temptations of protectionism and monopolism. They must defend the information environment from subversion and manipulation; but redouble efforts to protect institutions, rights, and democratic values from information authoritarians who are seeking to subvert and undermine them. The difficulty of the task must not deter us from attempting it. Anything less could strike a serious blow to national security, internal stability, and democracy itself.

Endnotes

1 Eric Rosenbach and Katherine Mansted. "Can Democracy Survive in the Information Age?," *Belfer Center*, October 2018, https://www.belfercenter.org/publication/can -democracy-survive-information-age.

2 "The Rise of Big Data," *Foreign Affairs,* May/June 2013.

3 "The World's Most Valuable Resource is No Longer Oil, But Data," *The Economist*, May 6, 2017.

4 "Data is Real Wealth: PM Modi in Davos," *Business Standard,* January 23, 2018, https://www.business-standard.com/article/news-ani/data-is-real-wealth-pm-modi-in-davos-118012300923_1.html.

5 *World Economic Forum,* January 23, 2019, https://www.weforum.org/agenda/2019/01/abe-speech-transcript/ ("it is no longer capital but data that connects and drives everything").

6 *World Economic Forum,* January 24, 2018, https://www.weforum.org/agenda/2018/01/angela-merkel-at-davos-we-need-global-cooperation-not-walls/ ("Data will be the raw material of the twenty first century").

7 *Reinventing Capitalism in the Age of Big Data*, 2018.

8 McKinsey Global Institute. "The Age of Analytics: Competing in a Data-driven World," December 2016, https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world.

9 "Power and Interdependence in the Information Age," *Foreign Affairs,* 77(5), September/October 1998.

10 The cyberattack also saw 1.5 million SingHealth patients' data stolen. See *Straits Times,* July 20, 2018, https://www. straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

11 "Obama for America uses Google Analytics to Democratize Rapid, Data-driven Decision Making," *Google,* 2013, https://analytics.googleblog.com/2013/08/obama-for-america-uses-google-analytics.html.

12 For a critical review of this business model, see Shoshana Zuboff, *The Age of Surveillance Capitalism,* 2019.

13 Shashi Tharoor. "India's Big Leaky Data," *The Daily Star*, April 14, 2018, https://www.thedailystar.net/opinion/awakening-india/indias-big-leaky-data-1562422.

14 Sarah Dai. "'China's Google' says Government Support and Population Size Matters in Global AI Race," *South China Morning Post,* January 9, 2018.

15 "Data is Real Wealth: PM Modi in Davos," *Business Standard,* January 23, 2018, https://www.business-standard.com/article/news-ani/data-is-real-wealth-pm-modi-in-davos-118012300923_1.html.

16 James Vincent. "Putin says the Nation that Leads in AI 'will be the Ruler of the World'," *The Verge*, September 4, 2017, https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world.

17 For a fairly comprehensive tour, see: https://futureoflife.org/national-international-ai-strategies/.

18 Michael Riley, Jordan Robertson & Anita Sharpe. "The Equifax Hack has the Hallmarks of State-Sponsored Pros," *Bloomberg Businessweek,* September 29, 2017, https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros.

19 *AI Superpowers: China, Silicon Valley, and the New World Order,* Houghton Mifflin Harcourt, 2018.

20 Lily Hay Newman. "If China Hacked Marriott, 2014 Marked a Full-on Assault," *Wired,* December 12, 2018, https://www.wired.com/story/marriott-hack-china-2014-opm-anthem/.

21 Michele Flournoy and Josh Hochman. "How Big Tech Can Work With China But Protect U.S. Secu-

rity," *Bloomberg,* January 31, 2019, https://www.bloomberg.com/opinion/articles/2019-01-31/u-s-tech-companies-should-embrace-export-controls-to-china.

22 The White House. "National Security Strategy of the United States of America," December 2017, 34-35.

23 Anthea Roberts, Henrique Choer Moraes & Victor Ferguson. "Geoeconomics: the U.S. Strategy of Technological Protection and Economic Security," *Lawfare,* December 11, 2018, https://www.lawfareblog.com/geoeconomic-world-order.

24 United Kingdom Ministry of Defence. "Global Strategic Trends: The Future Starts Today," 2018, 6th ed., 20, 134.

25 Catalin Cimpanu. "Russia to Disconnect from the Internet as Part of a Planned Test," *ZDNet*, February 11, 2019, https://www.zdnet.com/article/russia-to-disconnect-from-the-Internet-as-part-of-a-planned-test/.

26 Katy Steinmetz. "Lawmakers Hint at Regulating Social Media During Hearing with Facebook and Twitter Execs," *TIME Magazine*, September 5, 2018, http://time.com/5387560/senate-intelligence-hearing-facebook-twitter/.

27 Osonde Osoba and William Welser IV. "An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence," RAND Corporation, 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1744/RAND_RR1744.pdf.

28 See Samantha Hoffman. "Managing the State: Social Credit, Surveillance and the CCP's Plan for China," *China Brief* 17(11), August 17, 2017, https://jamestown.org/program/managing-the-state-social-credit-surveillance-and-the-ccps-plan-for-china/.

29 Viktor Mayer-Schönberger and Thomas Ramge. *Reinventing Capitalism in the Age of Big Data*, Basic Books, 2018.

30 See, for example, Michael Kofman's summary of the perspective of Chief of the General Staff of the Russian Armed Forces General Gerasimov: "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks,* March 11, 2016, https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

31 See, for example, Hal Brands. "Democracy vs Authoritarianism: How Ideology Shapes Great Power Conflict," *Survival,* 60(5), October-November 2018, 67.

32 By contrast, in *Safe Passage: The Transition from British to American Hegemony,* 2017, Harvard University Press, Kori Schake explores how ideological convergence was an important factor in smoothing history's only peaceful transition of hegemonic power, from Britain to America.

33 Samuel P. Huntington. *The Clash of Civilizations and the Remaking of World Order,"* 1996, Simon & Schuster, 92.

34 "America's Information Edge," *Foreign Affairs,* 75(2), March/April 1996.

35 William J. Clinton, "Remarks at the Paul H. Nitze School of Advanced International Studies," Washington,

D.C., March 8, 2000, http://www.presidency.ucsb.edu/ws/index.php?pid=87714.

36 White House. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, foreword.

37 White House. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, 23-24.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P

Printed in the United States of America