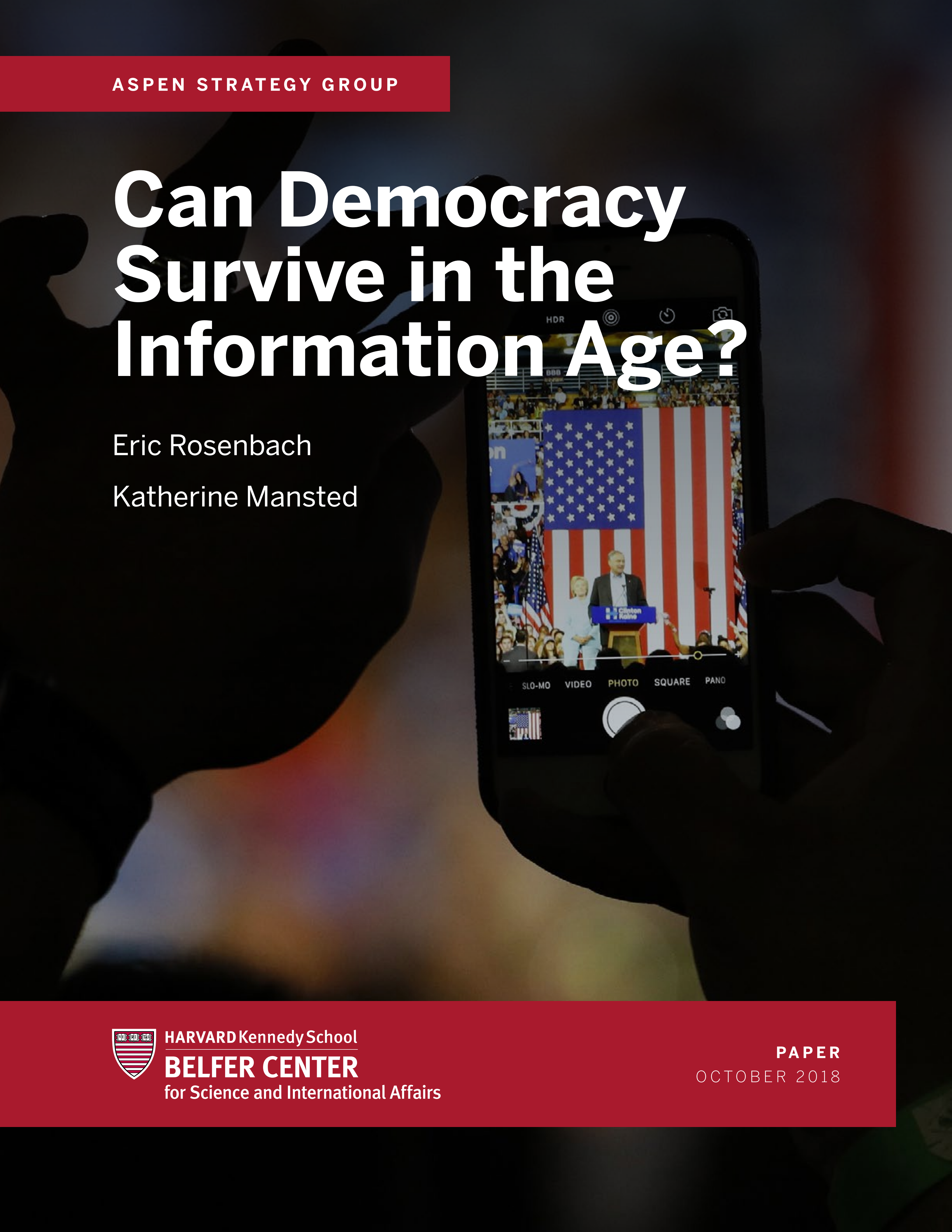

ASPEN STRATEGY GROUP

Can Democracy Survive in the Information Age?

Eric Rosenbach

Katherine Mansted

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
OCTOBER 2018

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

www.belfercenter.org

Statements and views expressed in this report are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Layout by Andrew Facini

Cover photo: An attendee shoots a photo on a cell phone of Democratic U.S vice presidential candidate Senator Tim Kaine speaking as he appears with Democratic U.S. presidential candidate Hillary Clinton during a campaign rally in Miami, Florida, U.S. July 23, 2016. (REUTERS/Scott Audette)

ASPEN STRATEGY GROUP

Can Democracy Survive in the Information Age?

Eric Rosenbach

Katherine Mansted

This paper is adapted from an article for a forthcoming Aspen Strategy Group series on Technology and National Security to be published this Fall.

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
OCTOBER 2018

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 Nonresident Fellow at the Belfer Center and a Senior Research Officer at the Australian National University's National Security College.

Table of Contents

HDR
Clinton Kaine
SLO-MO
VIDEO
PHOTO
SQUARE
PANO

Introduction

States have always used a combination of diplomatic, military, economic, and informational measures to advance their national interests, and technological change has altered each of these levers of power. The Information Revolution, however, has most radically reinvented the way in which states wield information power, ushering in changes to the nature of state competition, conflict, and international relations in the 21st century. Today's digitally-enabled information operations bear no resemblance to the mass letter drops and radio broadcasts of the Cold War. Even the counter-messaging campaigns focused on Al-Qaeda during the decade following 9/11 now seem anachronistic: the United States had little control over who tuned in to its messages, struggled to segment the audience or create customized content, and relied on expensive, yet imprecise, infrastructure.

Democracy is built on the crucial compact that citizens will have access to reliable information and can use that information to participate in government, civic, and corporate decision-making. The technologies of the Information Age were largely built on the assumption that they would strengthen this compact. However, as typified by Russia's ongoing use of information operations against the United States and Europe, key information technologies have evolved quickly over the past five years and been weaponized against democracies. The trajectory of data-driven technologies, including machine learning and other aspects of artificial intelligence, will increase the scale, complexity and effectiveness of adversary information operations. As technology advances, and as geopolitical and ideological tensions between democratic and authoritarian states rise, information operations are likely to become more numerous, insidious, and difficult to detect. Democracy is resilient: few, if any, democracies will crumble under the coming wave of information warfare. But absent a new national security paradigm and real action, the weaponization of information technologies threatens to jeopardize democracies' ability to govern and protect their national security, and to undermine people's trust in democracy as a system of government.

This paper explores both the politics and technologies that are changing the face of information power in the 21st century. In Part 1, we explain why states, especially those with authoritarian forms of government, are increasingly seeking to 'game' democracy's strengths by using information operations.[1] We also highlight that authoritarian governments—and China in particular—have largely succeeded in controlling their domestic information environments. This affords them a degree of impunity to engage in information operations, but in the long run may make them more brittle in the face of conflict and dissent in the Information Age. As an antidote to the national security community's tendency to 'fight the last war' (in this case Russian information operations) we then explain why China is also capable and increasingly likely to engage in information operations to advance its national goals. In Part 2, we assert that advances in artificial intelligence, coupled with the growing abundance and importance of data, will turbocharge the scale and effectiveness of adversary information operations. Information operations to date are only prototypes of the sophisticated platforms and messages that non-democratic states will weaponize in coming years. This points to the urgency of reorienting America's national security strategy to focus on the emerging information operations threat.

In Part 3, we set out steps that the United States can take to build a whole-of-nation strategy to defend itself in the Information Age. By mobilizing action across civil society, the private sector and government agencies, a whole-of-nation approach will play to the strengths of democracy. The linchpin of any strategy must be a clear national deterrence posture that explicitly includes the option of counterattacks, which would threaten adversaries' control of their own information environments.

[1] We use the term 'information operations' to refer broadly to the use of information to "influence, disrupt, corrupt, or usurp" decision-making within a state, especially via the Internet and related information technologies. While the phrase in quotation marks comes from U.S. Joint Publication 3-13 (Information Operations), we are not using the current military definition of the term—which focuses on exploiting adversary information flows, and protecting our own, during extant military operations.

1. Democracy and Security in the Information Age

In the 1990s, as the Internet started to be commercialized, it was widely assumed that technology would accelerate the global spread of democracy. The design of the Internet itself—a decentralized network that empowers individuals to freely associate and share ideas and information—reflected liberal principles. As an American innovation, the Internet, and the Information Revolution that followed, attested to the merits of democracy and appeared to cement the United States' position as world superpower. During the 1990s and early 2000s, governments that sought to co-opt the Internet to serve the state were seen to be resisting an immutable, democratizing force. In March 2000, President Bill Clinton expressed the dominant view in the United States when he derided China's nascent attempts to censor the Internet as "like trying to nail Jell-O to the wall."[2] However, contrary to predictions of the futility of control in the Information Age, China ultimately developed the most sophisticated national-level system of censorship in history: the Great Firewall. Other non-democratic states have also invested significant resources in protecting and controlling their domestic 'information environments.' About eight years ago, authoritarian governments began to reap rewards from their investment in information control, and in mastering the tools of the Information Age. Actions by Russia, China, and terrorist networks like the Islamic State upended the conventional wisdom of the preceding two decades and demonstrated that information technologies can be used to exploit the vulnerabilities of democracy to advance nefarious interests.

[2] 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.

The Vulnerabilities of Democracy

In the same way that island building in the South China Sea, or 'little green men' in Ukraine enable our adversaries to achieve foreign policy objectives without triggering thresholds that would invite a significant U.S. response, information operations permit less powerful states to challenge core U.S. national interests. Our adversaries are emboldened because they see technologically-advanced democracies like the United States as digital 'glass houses' with four specific vulnerabilities: (i) weak mechanisms for distinguishing facts from fiction; (ii) the long, media-driven nature of elections; (iii) the tech sector's profit-oriented culture; and (iv) the inability of the government to oversee and coordinate issues related to the information environment.

First, free speech is a core value of democracy. However, with the advent of social media platforms, the Internet is no longer just a static bulletin board, but a place where any individual (or bot) can participate in the public debate, in real time. The nexus between the Internet and social media means that, without resorting to diplomacy or conflict, adversaries can change a democracy's behavior by influencing its citizens at scale and in real time. The institutions democracies previously relied upon to provide objective facts have not adapted to the reality of the Information Age. Now, the information that citizens use to inform how they vote, protest, and debate in the public square is distributed via a largely unmediated social media environment and frenetic 24/7 news cycle. By contrast, authoritarian states often control the media, censor the Internet, and in many cases shield their citizens from outside information through national firewalls.

Second, elections, the heart and soul of a democracy, are vulnerable to both information operations and cyberattacks. The Internet, social media, and data analytics will be the center of gravity for future political campaigns. All three played a key role in the Obama campaigns' ability to mobilize grassroots support,[3] while the Trump campaign established a new paradigm for presidential campaigns, using social media and big data analysis to both drive media coverage and to mobilize probable voters. The length of campaigns in the United States provides adversaries with a luxurious amount of time to plan, execute, and adapt information operations. Conversely, authoritarian states restrict the ways in which the public square can influence national decision-making. Most obviously, their leadership does not hinge on genuine elections that can be disrupted by manipulating public opinion.

Third, healthy democracies rely on the private sector to drive economic growth and prosperity in a way that is compatible with the overall public good. Over the past decade, profit-focused technology firms, especially Facebook and Twitter, have amassed an enormous amount of valuable data and honed the capability to drive citizens' decisions and opinions. This power has not been matched by a sense of public purpose, much less a sense of responsibility to contribute to national security. Although there are some early indications of change, their indifference remains a vulnerability. Conversely, authoritarian states closely align their industrial policy for the tech sector and national security priorities.[4] A state like China has unfettered access to domestic communications, rules against online anonymity, and can instantly order shutdowns of websites or designated accounts.

Fourth, in democracies, the executive and legislative branches perform the "inherently governmental functions" of national security and regulation. However, in the United States, government has not kept pace with adversaries' strategies of exploiting information technologies. Moreover, information operations (by design) fall into the seams between the public and private sectors. For example, ahead of the 2016 presidential election, there was ample evidence of Russia's intent and capability to meddle in

[3] In 2013, Google published a case study, *Obama for America uses Google Analytics to Democratize Rapid, Data-driven Decision Making*, explaining how Google Analytics had been critical to Obama's 2012 "data-driven re-election campaign." Claiming that digital marketing and analytics were responsible for "providing much of the winning margin" for the campaign, the case study outlines how Google Analytics was used to understand voter motivations, and to shape the information voters were served when they searched to verify claims made during debates, or as they considered how to vote. See: https://analytics.googleblog.com/2013/08/obama-for-america-uses-google-analytics.html.

[4] This alignment between industrial and national security policy is most obviously reflected in the Chinese government's use of cyberattacks to steal U.S. commercial secrets, an effort which continues despite a 2015 U.S./China bilateral agreement to cease industrial espionage.

U.S. politics. The Intelligence Community knew that Russia had been publicly signaling an increasingly aggressive political warfare posture from at least 2013,[5] and had tested many of the information tools it used in 2016 against Ukraine's presidential election in 2014. Researchers had also reported use of similar tools by the Syrian Government during the Syrian Civil War as early as 2012.[6] Many campaign staffers and technologists knew that in 2012 and 2015, respectively, Google and Facebook had promoted their platforms' abilities to influence voter behavior.[7] We also know now that Russian operatives stationed in the United States began laying the groundwork for the 2016 campaign as early as 2014, and purchased advertisements on Facebook and Google.[8] However, researchers, government officials, and tech platforms failed to work together in a way that let them connect the dots and anticipate—or even detect the full extent of—Russia's actions.

[5] For a summary of these public signals see: Linda Robinson et al., "Modern Political Warfare: Current Practices and Possible Responses" (Santa Monica, CA: RAND Corporation, 2018), 42–48, https://www.rand.org/pubs/research_reports/RR1772.html.

[6] Norah Abokhodair, Daisy Yoo, and David W. McDonald, "Dissecting a Social Botnet: Growth, Content and Influence in Twitter," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (New York, 2015), 849, http://doi.acm.org/10.1145/2675133.2675208.

[7] Ashley Parker, "Facebook Expands in Politics, and Campaigns Find Much to Like," *The New York Times*, July 29, 2015, https://www.nytimes.com/2015/07/30/us/politics/facebook-expands-in-politics-and-campaigns-find-much-to-like.html.

[8] Robert S. Mueller, "United States of America v Internet Research Agency & Ors. Indictment by the Grand Jury for the District Court of Columbia." (Case 1:18-cr-00032-DLF, February 16, 2018).

The Authoritarian Information Paradox

Authoritarian states have recently deployed information operations to advance their foreign policy, but propaganda and censorship have always been essential tools for maintaining control and power at home. For authoritarian governments in the Information Age, however, the Internet and related technologies are also a major vector for instability—since they make news and ideas accessible, and allow people to mobilize in ways that can threaten the ruling party.[9] Consider this stark observation in China's 2017 Cybersecurity Strategy: "If our party cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term."[10] Authoritarian governments do not just fear that their citizens will use the Internet to organize or rebel; they also believe that democracies use the Internet to advance pro-democratic narratives to undermine their regimes. Russia's president has derided the Internet as a "CIA project,"[11] while China's president characterized the competition between major powers as "rivalry for ideology, for the power of discourse."[12] It is easy to dismiss these statements as a diversionary tactic. However, while democratic governments generally do not engage in information operations to undermine their competitors, commercial and civil society actors do actively promote democratic and liberal principles—indeed, they are the primary agents for much of the "soft power" appeal of the U.S. system of government.[13] This dynamic means that authoritarian states do not just view control of their information environments as a

[9] For example, when President Xi Jinping came to power, a memo referred to as 'Document No.9' was allegedly distributed to senior party leaders which listed seven "perils" to the Chinese Communist Party's leadership. These included "Western constitutional democracy;" promotion of "universal values" like human rights, media independence, and civic participation; and "nihilist" criticisms of the CCP's past. See Chris Buckley, "China Takes Aim at Western Ideas," *The New York Times*, August 19, 2013, http://www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hard-line-in-secret-memo.html.

[10] Translated by Elsa Kania et al., "China's Strategic Thinking on Building Power in Cyberspace," New America, September 25, 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

[11] Ewen MacAskill, "Putin Calls Internet a 'CIA Project' Renewing Fears of Web Breakup," *The Guardian*, April 24, 2014, http://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia.

[12] Quoted in Fergus Ryan, "Money Talks in China's Cloistered Internet," *The Strategist* (blog), December 15, 2017, https://www.aspistrategist.org.au/money-talks-in-chinas-cloistered-internet/.

[13] Weatherhead Center for International Affairs, "Hard Times for Soft Power: A Q&A with Joseph Nye," Harvard University, May 30, 2017, https://epicenter.wcfia.harvard.edu/blog/joseph-nye-qa.

domestic matter; they increasingly believe that offensive action might be required to counter what they perceive as foreign information incursions.

Centralized control of the Internet does, however, make authoritarian states brittle. In democracies, a plethora of decentralized non-government actors play a role in disseminating trusted information and debunking propaganda. Even a small chink in the armor of authoritarian states' information control systems may have existential ramifications for those in power. This helps explain why authoritarian governments are prepared to engage in hostile information operations to defend their information environment, including to suppress liberal ideas and to discredit alternative systems of government. It also explains why most efforts to create international 'norms' against state information operations are bound to fail. Thus, in the long-run, authoritarian states, not democracies, may be proved to be the real glass houses.

The China Example

Russia's ongoing interference in U.S. democracy is the most politically salient instance of an information operation, but we should not assume that Russia is the only actor in this space. We should also not assume that all information operations will employ similar tools and tactics or share similar objectives. For example, researchers have observed that China is increasingly embracing "sharp power," which centers on using information for the purposes of distraction, manipulation, and intimidation.[14] China's domestic propaganda and censorship capabilities provide it with a powerful vehicle for information operations, particularly as the popularity of Chinese platforms like WeChat and Internet penetration in countries with large Mandarin-speaking populations both continue to rise. China's use of government operatives (colloquially known as '50-centers') to flood social media with an estimated 488 million posts annually to advance pro-government narratives and drown out negative stories is well-documented.[15] Additionally, China has been increasingly implicated in spreading 'fake news' stories designed to foment civil unrest and distrust in democracy in Taiwan.[16] Even if China confined propagandistic content to its domestic platforms, the borderless nature of the Internet means that this content will inevitably spill over to other countries.

China's cyber agencies are also increasingly using offensive operations to advance China's regional foreign policy interests—particularly in connection with China's territorial disputes. Chinese hackers blocked or vandalized Japanese websites in response to tensions over the disputed Senkaku (Diaoyu) Islands.[17] And they took down Philippines government

[14] Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence," *Foreign Affairs*, November 16, 2017, https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.

[15] See, for example, David Wertime, "Meet the Chinese Trolls Pumping out 488 Million Fake Social Media Posts," *Foreign Policy,* May 19, 2016, https://foreignpolicy.com/2016/05/19/meet-the-chinese-internet-trolls-pumping-488-million-posts-harvard-stanford-ucsd-research/.

[16] See, for example, David Spencer, "Why the Risk of Chinese Cyber Attacks Could Affect Everyone in Taiwan," *Taiwan News*, July 13, 2018, https://www.taiwannews.com.tw/en/news/3481423.

[17] Bill Gertz, "U.S. Officials Say China behind Cyber Attacks on Japan," *Washington Free Beacon* (blog), September 25, 2012, http://freebeacon.com/politics/cyber-blitz/.

websites[18] and hacked Vietnam Airlines systems[19] following the 2016 UN Permanent Court of Arbitration ruling on the South China Sea. Perhaps most concerning of all is that China's cyber agencies also have a history of hacking government, political, and media networks in the lead up to democratic elections in its region: most recently in Taiwan[20] and Cambodia.[21] At this stage, it is not clear whether this activity is limited to intelligence-gathering or could be in preparation for information operations.

Chinese information operations within the Asia Pacific region threaten U.S. allies and interests. It is also increasingly conceivable that China might use information operations to directly target the United States, or other Western democracies. As China's power grows, it is increasingly using influence and intimidation tactics, for example against media companies, civil society, and academia in Europe, the United States, Australia, and New Zealand, to suppress information contrary to the interests of the Chinese Communist Party.[22] To this point, these tactics are executed by human operatives, rather than as part of information operations exploiting information technologies.

Currently, China predominantly uses its extensive cyber capabilities for government and commercial espionage; however, it could easily repurpose these capabilities, or information it has collected, for use in information operations against Western targets. Instead of using its access to a penetrated network to exfiltrate data, China could easily use that position to poison government datasets, seed false content into the information environment, or obtain and leak sensitive documents. Recalling that China was responsible for the 2015 data breach of the U.S. Office of Personnel Management—resulting in the theft of sensitive information on 4 million

[18] Janvic Mateo, "68 Gov't Websites Attacked," *The Philippine Star*, July 16, 2016, https://www.philstar.com/headlines/2016/07/16/1603250/68-govt-websites-attacked.

[19] Charlie Osborne, "Chinese Hackers Take down Vietnam Airport Systems," ZDNet, August 1, 2016, http://www.zdnet.com/article/chinese-hackers-take-down-vietnam-airport-systems/.

[20] Scott Morgan, "Taiwan Prepares for Spike in Chinese Cyber-attacks in Lead-up to Elections," Taiwan News, July 9, 2018, https://www.taiwannews.com.tw/en/news/3477568.

[21] FireEye, "Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 20148 Elections and Reveals Broad Operations Globally," July 10, 2018, https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html.

[22] Thorsten Benner et al., "Authoritarian Advance: Responding to China's Growing Political Influence in Europe" (Berlin: Global Public Policy Institute, February 5, 2018), http://www.gppi.net/publications/rising-powers/article/authoritarian-advance-responding-to-chinas-growing-political-influence-in-europe/.

people who had undergone U.S. government security checks—it is apparent that China already controls large troves of sensitive information that could be strategically leaked or used for highly-targeted information operations. China also has the technical tools to launch 'blunt force' attacks. The Great Firewall can be repurposed into an offensive weapon (which researchers have dubbed the 'Great Cannon') that can launch massive cyberattacks to shut down websites or to inject false or misleading content into targeted systems.[23] The potential of the Great Cannon, and China's willingness to use it against Western democracies, was demonstrated in 2015, when Chinese hackers launched a massive distributed denial-of-service against U.S.-headquartered website GitHub.[24] GitHub, the world's biggest repository of open source code, had hosted content that provided technology to subvert Chinese online censorship. As the 'authoritarian information paradox' discussed above predicts, China is willing to use offensive measures to suppress information that challenges its domestic control of information.

[23] Bill Marczak et al., "China's Great Cannon" (Munk School of Global Affairs, University of Toronto: The Citizen Lab, April 10, 2015), https://citizenlab.ca/2015/04/chinas-great-cannon/.

[24] Lorenzo Franceschi-Bicchierai, "China Is Behind DDoS Attack on GitHub, Activists Say," *Motherboard*, March 30, 2015, https://motherboard.vice.com/en_us/article/8qx7wz/china-is-behind-ddos-attack-on-github-activists-say.

2. The Coming AI Wave

To this point, information operations have relied on human operatives to generate content and used a combination of human 'trolls' and basic automated algorithms to disseminate that content. Social media companies currently have the capacity (if not always the will) to defend against most of the tools that today's information adversaries employ. Most automated algorithms can be identified because they exhibit predictable 'bot-like' patterns. Similarly, after public and political pressure, Facebook, Twitter, and Google have announced efforts to update their algorithms to deemphasize 'fake news.' Facebook has also introduced labeling requirements for electoral advertisements, and advertisements on topical political issues,[25] while Twitter has taken action to shut down bot networks and delete inauthentic accounts.[26] These are all positive steps, but advances in artificial intelligence (AI) technologies in coming years may allow adversaries to outpace our abilities to defend against them using technology alone.

The Data Explosion

The primary driver of advances in AI is the growing abundance of data. The amount of data in the world is growing at an exponential rate (around 90 percent of the data in the world today was created in the last two years). By 2020 there will be some 20 billion 'Internet of Things' sensors embedded around the world—collecting data from wearable devices, home appliances, and city infrastructure. Parallel developments, including rising use of geotagging by phone apps, smart cars and financial services firms; improvements in facial recognition technology; and the rise of affective computing (whereby machines can discern human emotions from text, facial expressions, and voice patterns[27]) will add to increasingly rich sets of data. The data explosion is overwhelmingly driven by economics. Data enables firms—whether they are online platforms, traditional bricks and

[25] "Making Ads and Pages more Transparent," *Facebook*, April 6, 2018, https://newsroom.fb.com/news/2018/04/transparent-ads-and-pages/.

[26] See, for example, "Confidence in Follower Counts," *Twitter,* July 11, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/Confidence-in-Follower-Counts.html.

[27] See, for example, the Affective Computing research group at the MIT Media Lab: https://www.media.mit.edu/groups/affective-computing/overview/

mortar retail chains, financial companies or insurance brokers—to better target consumers.

Access to data also has a multiplying effect, due to advances in machine learning (a subset of AI). Firms with more data can serve their customers more effectively: for example, Netflix's personalization algorithms have made it more valuable than Disney.[28] Firms with more data are also able to create better AI software: for example, Facebook trained its algorithms to recognize faces by learning from billions of users 'tagging' pictures of their friends. Today, nearly every industry is either using or exploring machine-learning applications. Erstwhile titans of the industrial age, like GE, market themselves based on their ability to aggregate and process customer data.[29] The rapid pace of data collection is only likely to accelerate. By some estimations, up to 80 percent and up to 60 percent of the current 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.[30]

AI Will Give Adversaries a Technological Edge

The rise of data is underwriting a new wave in the development of AI technologies. These advances will benefit those who defend against information operations (for example by helping to train algorithms to detect and filter propaganda). In the short term, however, they are likely to magnify the scale and effectiveness of adversary information operations. With China articulating a national plan to be the world leader in AI investment and research,[31] we can no longer assume that the benefits of Information Age advancements will accrue to American interests. Likewise, while the

[28] "Netflix is Moving Television Beyond Time-slots and National Markets," *The Economist,* June 28, 2018.

[29] For example, GE's "Predix Platform" promises to extract value from the "massive amounts of data" generated by customers' industrial operations. See: https://www.ge.com/digital/predix-platform-foundation-digital-industrial-applications.

[30] 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/.

[31] Cade Metz, "As China Marches Forward on AI, the White House is Silent," *The New York Times,* February 12, 2018, https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligencre.html.

research and development costs of cutting-edge AI are high, breakthroughs are likely to spread quickly and widely, equipping both state and non-state adversaries with a technological edge.

Hyper-personalized content

Data is valuable commercial information; but in the hands of adversaries, it can be extraordinarily dangerous. Russia has a long history of exacerbating divides on fractious social issues by targeting susceptible identity groups: for example, its operatives posted divisive content to Facebook groups affiliated with Black Lives Matter supporters and detractors, and to individuals who "liked" content related to race.[32] With advances in machine learning, adversaries will be able to build, buy, or steal detailed profiles on nearly every citizen. These profiles will not just be based on known data inputs (like whether a person is a member of a racial justice group), but also on inferences from machine learning tools that predict with increasing accuracy people's personality and preferences, political and religious beliefs,[33] real-time emotions, and even identity characteristics like sexual preference.[34] Social media micro-targeting is already one of the more difficult information operation tactics to counter—since messages are only seen by select individuals or groups and for a short time. As machines begin to know us better than we know ourselves, adversaries will increasingly be able to identify and target those who are most susceptible to influence. They will then be able to deliver highly-personalized content that achieves maximum effectiveness by exploiting individuals' unique characteristics, beliefs, needs and vulnerabilities.[35]

[32] Russian operatives also attempted to stoke divides on hot button issues including the Black Lives Matter movement, gun control, Islamophobia, immigration, and police violence.

[33] For example, Google offered political interest targeting to advertisers in the 2016 U.S. election cycle, based on whether users had been identified as "left-leaning" or "right-leaning". See Google, "Security and Disinformation in the U.S. 2016: What We Found," October 30, 2017, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/google_US2016election_findings_1_zm64A1G.pdf.

[34] For example, researchers at Stanford have created an AI system able to predict person's sexual orientation from a photograph with up to 91% accuracy.

[35] Matt Chessen, "The MADCOM Future," *Atlantic Council*, September 26, 2017, 10, http://www.atlanticcouncil.org/publications/reports/the-madcom-future.

Taking humans out of the loop

Humans, such as China's '50-centers' and the hundreds of Russian 'troll farm' operators, are currently needed to develop content for information operations. Bots are often used to amplify the content but do not create it. However, the next wave of AI research—which is focused on creating tools that are better able to understand human language and to process it in the right context[36]—may put bots in the driver's seat. Today's AI tools can only interact with humans in highly circumscribed contexts, but they are constantly improving their ability to generate original and dynamic content, to persuade, and to tailor their content to appeal to their interlocutor's mood. As AI becomes better at mimicking human behavior, fake, automated online personas will become harder to detect. Additionally, once a certain piece of AI software exists 'in the wild,' the marginal cost of using it to create one additional bot or to influence one additional citizen will be almost zero.[37] Finally, AI tools are by nature learning systems. AI-enabled bots will be able to conduct experiments and learn from successes and failures in real time to recalibrate their methodologies for maximum impact. As a result, once an adversary sets an objective for an online information operation, it may become most effective and economical to take humans out of the loop at the tactical level.

Deep fakes

Advances in AI are also making digital manipulation of audio and video cheaper and harder to detect. Currently, high-quality audio or visual material is considered highly reliable evidence in factual and legal disputes and is largely taken at face value by the media and individuals to be legitimate.[38] However, according to expert predictions, researchers are a matter of several years or even months away from being able to produce realistic video forgeries that will fool the human eye. Already, user-friendly software

[36] Venkat Srinivasan, "Context, Language, and Reasoning in AI: Three Key Challenges," *MIT Technology Review,* October 14, 2016, https://www.technologyreview.com/s/602658/context-language-and-reasoning-in-ai-three-key-challenges/.

[37] Matt Chessen, "The MADCOM Future," *Atlantic Council*, September 26, 2017, 4, http://www.atlantic-council.org/publications/reports/the-madcom-future.

[38] Future of Humanity Institute et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," February 2018, 46, https://maliciousaireport.com/.

exists online to produce realistic fake audio, provided there is a sufficiently large training dataset of the particular voice.[39] Adversaries will soon be able to create entirely false audiovisual content, or even more insidiously, they will modify existing content to create highly effective information operations.[40] Some analysts have also pointed to the risk that increased use of digital forgeries by both legitimate and illegitimate actors could pose a more systemic risk to democracy by eroding people's trust in even completely truthful information.[41]

We are more sanguine about this risk. Just as the Internet has evolved to require security certificates for trusted websites, it is likely that, over time, audiovisual certificate systems will become increasingly sophisticated. Blockchain technologies could also be used to ensure these certificates are authentic. In the short-term however, adversaries will be able to take advantage of the gap between the emergence of better forgery technology and new authentication norms. Even once that gap closes, forged audiovisual content is likely to remain a significant concern on particularly contentious issues such as international crises or fraught political issues—where news will spread fast, and quick decisions will need to be taken.

[39] See, for example, the Canadian company Lyrebird: https://lyrebird.ai/.

[40] Matt Chessen, "The MADCOM Future," *Atlantic Council*, September 26, 2017, 10, http://www.atlanticcouncil.org/publications/reports/the-madcom-future.

[41] Robert Chesney and Danielle Citron, "Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?" *Lawfare,* February 21, 2018, https://www.lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy.

3. A Whole-of-Nation Security Strategy for the Information Age

Our response to Vladimir Putin's ongoing attempts to undermine the strength of American democracy will be a defining issue of the Information Age. The most important lesson the United States should internalize from Russia's interference campaign in 2016 is the price of complacency: we ignore continued cyberattacks and information operations at our own peril. Adversaries are able to turn our democratic system against itself because we lack a coherent national security strategy for the Information Age. A whole-of-nation approach that recognizes and harnesses the expertise of academia, civil society, companies, and across government agencies will play to the strengths of democracy and, at a minimum, should contain four elements we outline below.

Establish a clear deterrence posture against information operations and cyberattacks that begins with explicit declaratory policy and includes the threat of offensive information and cyber counterattacks.

Strategic signaling matters as much in the Information Age as it did to the nuclear threat during the Cold War. Failures by both the Obama and Trump Administrations to confront Russia will lead our adversaries to continue to believe that the United States will hope to weather the blows of information operations and cyberattacks. This puts us in an invidious position: the scale, potency, and likely impact of future information operations will not be determined by how prepared we are to combat them; we are instead leaving it up to our adversaries to determine when their ends justify the means of deploying an information operation against us. As highlighted earlier in this paper, authoritarian governments recognize that they exist in a brittle information environment. This fact makes them particularly susceptible to the threat of information and cyber operations against key elements of their media, technology and government ecosystems. With that in mind, the United States, led by the President and other senior political leaders in the executive and legislative branches, must explicitly state that information (and cyber) attacks against the United

States and our allies will result in counteraction. The counterpunch should use all available levers in the foreign policy toolkit but should always include some aspect of an incisive information operation.[42] Looking over the horizon, it is particularly important that the United States signal to China that information operations against democracies will result in significant strategic risk to China's core national interests.

Recalibrate the Intelligence Community to provide the United States and its allies with the intelligence necessary to detect and expose sources and content related to information operations.

During the run-up to the 2016 presidential election, the U.S. Intelligence Community provided impressive, clear, and unique intelligence about Putin's intent to interfere in the presidential election. The Intelligence Community provided relatively little intelligence, however, on some of the specific operations that the Russian intelligence services used to influence American voters. Understandably, the Intelligence Community simply was not postured to provide indications and warnings about manipulation of social media via botnets and false personas. The Intelligence Community cannot shift its full attention away from more existential threats to the country, but it must invest and innovate to bolster the 'early warning' system of attribution for information operations which target U.S. democratic institutions. This will require better collaboration and information sharing with Silicon Valley firms, which in turn need to shed a post-Snowden reluctance to cooperate with government on pressing national security issues. Additionally, the government should enlist the support of private sector threat intelligence firms, which have excellent capabilities and will be key to any information sharing arrangement.

Attribution is not only a requirement for an effective deterrence strategy, but also a core aspect of the best antidote to information operations: public shaming and fact-based counter-messaging. The United States can learn from and follow the examples set by both the French and German governments, which used intelligence about probable Russian information

[42] The United States is currently not organized and lacks important capability for this mission. Thus, implementation of this recommendation would likely require the establishment of a national joint task force that combines the unique skills, capabilities and authorities of CIA, NSA, SOCOM, CYBERCOM and DHS.

operations to warn their citizens and publicly call out the Russians. Just hours after a massive online leak of emails, the 2017 Macron campaign issued a statement blaming the leaks on hackers intent on "sow[ing] doubt and disinformation."[43] After receiving intelligence from her national intelligence organization, Chancellor Merkel warned the German public of possible Russian interference in Germany's elections, a course of action which many experts believe influenced Russia not to leak data stolen in a 2015 hack of the Bundestag.[44]

Enact national legislation that requires social media platforms to increase transparency about their algorithms and political, bot-driven content.

Social media companies are an essential aspect of American economic power in the Information Age, but they have also created tools and systems which can be used to subvert democracy. Ensuring that social media is not gamed by our adversaries cannot be left to self-regulation but needs to be incentivized and in some cases mandated by government. In particular, citizens have a right to know when they are seeing paid political advertisements and, in some cases, why they are being targeted by certain political or social campaigns. While Facebook has recently introduced internal requirements for displaying disclosures on political advertisements, this issue is too important to be left to the discretion of individual companies. Congress should enact legislation that mandates at a minimum the same disclosure for political advertisements on social media as for traditional media.

Additionally, Congress should pass laws that require platforms to identify and label foreign actor-driven bots and to provide users with the option to block them. Researchers have already developed tools which can screen for and identify bots; social media companies should now provide their users with more protection from them.[45] While as we noted earlier in

[43] Adrian Croft and Geert De Clercq, "France Fights to Keep Macron Email Hack from Distorting Election," *Reuters,* May 6, 2017, https://www.reuters.com/article/us-france-election/france-fights-to-keep-macron-email-hack-from-distorting-election-idUSKBN1820BO.

[44] See, for example, Alina Polyakova and Spencer P. Boyer, "The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition, *Foreign Policy at Brookings,* March 2018, 18, https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/.

[45] Zi Chu et al., "Who Is Tweeting on Twitter: Human, Bot, or Cyborg?" (Proceedings of the 26th Annual Computer Security Applications Conference, 2010), https://dl.acm.org/citation.cfm?id=1920265.

this paper, bot-spotting is likely to become more difficult with advances in AI, a requirement to label accounts which should be reasonably able to be identified as bots will force social media firms to keep ahead of the technological curve and to adopt the latest best practices on bot identification from researchers and the security community. Private-sector led bot-spotting also supports the whole-of-nation ethos. Bot labelling does not silence speech or censor content but equips citizens with tools to better understand the content they are engaging with and to judge its veracity for themselves.

Finally, social media companies must adjust their algorithms to reflect their role in democracy. Because of their market dominance, platforms like Twitter, Facebook, and YouTube do not just house public discourse; they shape it. Currently, social media algorithms are optimized for user engagement because clicks, views, and 'likes' maximize profit. As a result, social media platforms often promote and prioritize controversial information—something that Russian trolls and bots have exploited to great effect. It is technically uncomplicated, and necessary for the overall public good, to adjust these algorithms.

Enact national legislation that establishes a high level of protection for citizens' private data.

As the Information Age advances, the United States needs to recognize that data is a precious commodity that warrants a much higher national security priority. Data protection has historically been viewed as a niche issue relevant only to consumer privacy, but recent incidents, such as the hacks of the Office of Personnel Management and credit reporting agency Equifax, illustrate that data is a high priority target.

Looking over the horizon, adversaries will greatly increase operations to steal sensitive and valuable information from the private sector. Given the richness of data held by companies like Google, Amazon, Facebook, and the financial and healthcare sectors, it is highly likely that adversary intelligence services will expand their traditional targets to include corporate datasets that could be used to train AI systems and to hone information operations. We should not be surprised if Facebook eventually confirms that Russian intelligence services accessed and operationalized the same private user data acquired by Cambridge Analytica.[46]

National data protection legislation is necessary because even the serious repercussions that arose from the Equifax data breach, including costly litigation and reputational damage, have not sufficiently changed most corporate perspectives on data protection. While Europe's General Data Protection Regulation is by no means a perfect model and in some respects is inconsistent with other U.S. values,[47] 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 it establishes important principles that could serve as the foundation for national legislation.[48]

[46] For a relatively good summary, see: https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.

[47] Perhaps most notably in its codification of a 'right to be forgotten.'

[48] See Daisuke Wakabayashi, "California Passes Sweeping Law to Protect Online Privacy," *The New York Times,* June 28, 2018, https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html.

4. Conclusion

Information technologies have not just revolutionized lives, societies, and economies; they are also reshaping the nature of 21st century politics and conflict. In many respects, our adversaries have learned and adapted to this reality more quickly. As technology continues to advance, and as our adversaries learn from the successes of Russian information operations, democracies should brace themselves for increasingly sophisticated and aggressive information attacks. Leaders in democracies must also realize that they can no longer advance and defend their national interests through conventional military, economic, and diplomatic means. For America, there remains a narrow window in which a coherent whole-of-nation strategy can be devised to combat the threats of the Information Age.

The integrity, and legitimacy, of our system of government may depend on it.

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

www.belfercenter.org