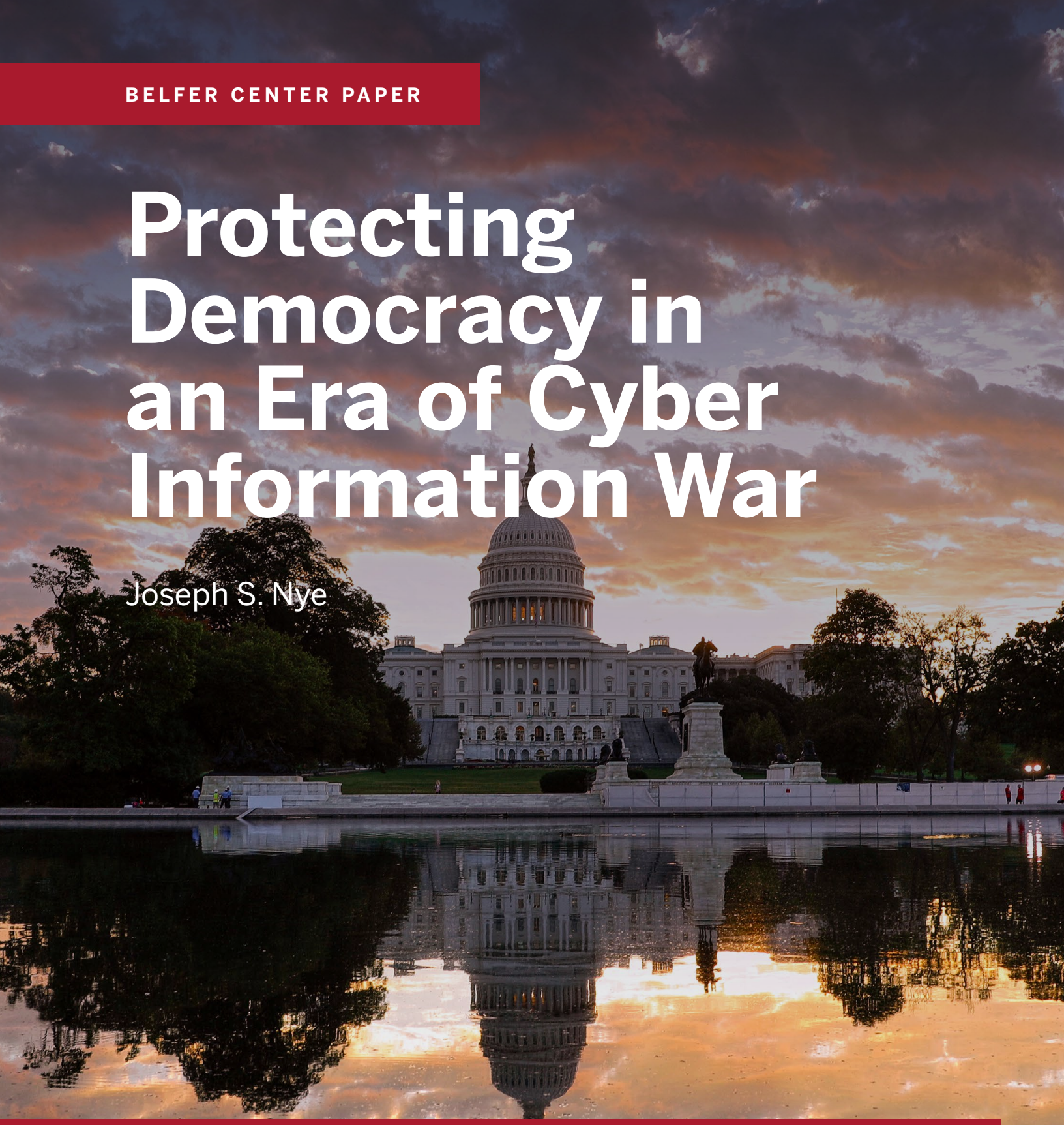
BELFER CENTER PAPER

Protecting Democracy in an Era of Cyber Information War

Joseph S. Nye



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
FEBRUARY 2019

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

www.belfercenter.org

This paper was originally published as a Working Paper by the Hoover Institution's Governance in an Emerging New World Project

www.hoover.org/governanceproject

Layout and design by Andrew Facini

Cover Image: The U.S. Capitol is seen at sunrise, in Washington, October 10, 2017. (AP Photo/J. Scott Applewhite)

BELFER CENTER PAPER

Protecting Democracy in an Era of Cyber Information War

Joseph S. Nye

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
FEBRUARY 2019

除《企业家第一课》、《企业家功成堂》外，其他公众号分享本期资料的，均属于抄袭！

邀请各位读者朋友尊重劳动成果，关注搜索正版号：《企业家第一课》、《企业家功成堂》

谢谢观看！

企业家第一课，专注做最纯粹的知识共享平台

关注官方微信
获取更多干货

加入知识共享平台
一次付费 一年干货

About the Author

Joseph S. Nye, Jr., is University Distinguished Service Professor and former Dean of the Kennedy School of Government at Harvard University. He received his bachelor's degree summa cum laude from Princeton University, studied at Oxford University on a Rhodes Scholarship, and earned a Ph.D. in political science from Harvard where he joined the faculty in 1964. In 2008, a poll of 2700 international relations scholars listed him as the most influential scholar on American foreign policy, and in 2011 Foreign Policy listed him among the 100 leading global thinkers.

From 1977-79, Nye was a deputy Undersecretary of State and chaired the National Security Council Group on Nonproliferation of Nuclear Weapons. In 1993-94 he chaired the National Intelligence Council which prepares intelligence estimates for the president, and in 1994-95 served as Assistant Secretary of Defense for International Security Affairs. He won Distinguished Service medals from all three agencies.

Nye has published fourteen academic books, a novel, and more than 150 articles in professional and policy journals. Recent books include *Soft Power*, *The Powers to Lead*, *The Future of Power*, and *Is the American Century Over?*

He is a fellow of the American Academy of Arts and Sciences, the British Academy, the American Academy of Diplomacy, and an honorary fellow of Exeter College, Oxford. He is the recipient of Princeton University's Woodrow Wilson Award, the Charles Merriam Award from the American Political Science Association, France's Palmes Academiques, and various honorary degrees.

Table of Contents

Cover Image
The U.S. Capitol is seen at sunrise, in Washington, October 10, 2017. (AP Photo/J. Scott Applewhite)

Introduction

The early years of the Internet were marked by a libertarian optimism about its decentralizing and democratizing effects. Information would be widely available and undercut the monopolies of authoritarian governments. Big Brother would be defeated. President Clinton believed that China would liberalize and that Communist Party efforts to control the Internet were like trying to "nail jello to the wall."[1] The Bush and Obama administrations shared this optimism and promoted an Internet Freedom Agenda that included subsidies and technologies to assist dissidents in authoritarian states to communicate.

Today, in the face of successful Chinese control of what citizens can see and say on the Internet and Russian use of the Internet to interfere in the 2016 American election, the United States (and allied democracies) find themselves on the defensive. The expected asymmetries seem to have been reversed. Autocracies are able to protect themselves by controlling information flows, while the openness of democracies creates vulnerabilities that autocracies can exploit via information warfare. Ironically, one cause of the vulnerabilities has been the rise of social media and mobile devices in which American companies have been the global leaders. Citizens voluntarily carry Big Brother and his relatives in their pockets. Along with big data and artificial intelligence, technology has made the problem of defending democracy from information warfare far more complicated than foreseen two decades ago. And while rule of law, trust, truth and openness make democracies asymmetrically vulnerable, they are also critical values to defend. Any policy to defend against cyber information war must start with the Hippocratic oath: first, do no harm.

Information Warfare: What's New and What's Not

The use of information as an instrument of conflict and manipulation in international politics has a long history. Britain manipulated information to move American opinion in the direction of war with Germany both in 1917 and 1941. The United States and the Soviet Union both used broadcasts, covert organizations, and funds to interfere in foreign elections during the Cold War.[2] And more narrowly, in battlefield situations in Iraq or in the campaign against ISIS, information was an important tool. In recent years, Russia's hybrid war against Ukraine has encompassed both cyber attacks and manipulation of information. Information operations are a critical component of modern warfare.[3]

Russia has used propaganda to express preferences for candidates in American elections since at least 1964, but new technologies have amplified their impact enormously.[4] According to former CIA Director Michael Hayden, Russian interference in the 2016 election was "the most successful covert influence campaign in recorded history." [5] For example, Russian operatives used Facebook to publicize 129 staged events, drawing attention of 340,000 users; 10 million people saw ads paid for by Russian accounts; and 126 million Americans saw posts by 470 accounts affiliated with the Russian Internet Research Agency.[6] A study by Twitter reported that 50,000 Russia-linked accounts were automated and tweeted election related content.[7] Reports released by the Senate Intelligence Committee estimate that the Russian campaign reached not only the 126 million people on Facebook but another 20 million more on Instagram.[8] Some Russian messages were crafted to support particular candidates while others were designed to create a general sense of chaos. Still others were micro-targeted to suppress voting by particular demographic groups such as African-Americans or younger voters. While skeptics argue that Russian efforts were a small percentage of the total content on the Internet, "for sub-groups of targeted Americans, the messaging was perhaps ubiquitous."[9]

Before the Internet, such operations involved costly training and movement of spies across borders, establishment of foreign bank accounts, and transfers

of cash. Now similar effects can be accomplished remotely at much lower cost. It is much easier to send electrons across borders than human agents. Ransoming a failed spy can be costly, but if no one clicks on a phishing e mail, it is simple, deniable, and virtually free to send another. In 1983, when the KGB seeded the rumor that AIDS was the product of U.S. government experiments with biological weapons, the rumor started with an anonymous letter to a small New Delhi newspaper and then was propagated globally but slowly over several years by widespread reproduction and constant repetition in conventional media. It took four years to reach full fruition.[10] In 2016, an updated version of the same technique was used to create "Pizzagate," the bizarre rumor that Hillary Clinton's campaign manager ran a child sex ring in a Washington restaurant. It spread instantly on the Internet. What's new is not the basic model; it's the speed with which such disinformation can spread and the low cost of spreading it.

With its armies of paid trolls and botnets, along with outlets such as Russia Today (RT) and Sputnik, Russian intelligence, after hacking into the e-mails of the Democratic National Committee and senior Clinton campaign officials, could distract and disrupt news cycles week after week without setting foot in the United States. And it could also count on the witting and unwitting help of organizations like Wikileaks. Russian messages aimed at priming, framing, agenda setting and contagion were accelerated by US media that were too quick and unreflective in using the Russian phrasing and frames.[11] American voters are subject to many influences, and there were many potential causes of the narrow outcome of the 2016 election. It is far too simple just to blame manipulation of social media. As social scientists say, the outcome was "overdetermined." But whatever its effects on the particular election outcome, Russia was able to accomplish its deeper goal of sowing disruption and discrediting the democratic model. It successfully undercut American soft power.

Soft Power and Sharp Power

Many Russian books and articles claim that "the death blow to the Soviet Union came not from NATO conventional forces but from an imperialist information war that Russia lost."[12] From the Kremlin's perspective, color revolutions in neighboring countries and the Arab Spring uprisings in 2011 were examples of the United States using soft power as a new form of hybrid warfare. "Authoritarian governments do not just fear that their citizens will use the Internet to organize and rebel; they also believe that democracies use the Internet to advance pro-democracy narratives to undermine their regimes."[13] While that may not have been the intention of the Obama Administration in Ukraine, Russia felt it needed to respond. The concept of soft power was incorporated into Russia's 2013 Foreign Policy Concept, and in March 2016, Russian Chief of General Staff Valery Gerasimov stated that since responding to such foreign threats using conventional troops is impossible; they must be counteracted with the same hybrid methods.[14] However, Russian and American views of soft power differ.

Power is the ability to affect others to get what you want, and that can be done through coercion, payment, and attraction. Some think soft power means any action other than military force, but this is wrong. Soft power is the ability to get what you want through attraction and persuasion rather than coercion or payment. While it relies in part on information, it differs from the coercive manipulation of information because it rests on the voluntarism of the subject. The soft power of attraction can be used for offensive purposes but if the degree of manipulation is so deceptive that it destroys voluntarism, the act becomes coercive and is no longer soft power. This manipulative use of information has recently been dubbed "sharp power." [15] Countries have long spent billions on public diplomacy and broadcasting in a game of competitive attractiveness – the "battle for hearts and minds." Soft-power instruments like the Marshall Plan and the Voice of America helped to determine the outcome of the Cold War through attraction. But the US also used deceptive sharp power in the form of covert support for publications and political parties.

After the Cold War, Russian elites believed that European Union and NATO enlargement, and Western efforts at democracy promotion, were

designed to isolate and threaten Russia. In response, they tried to develop Russian soft power by promoting an ideology of traditionalism, state sovereignty, and national exclusivity. This attracted support in countries like Hungary, where Prime Minister Victor Orbán promoted "illiberal democracy," as well as among the diaspora along Russia's borders, in impoverished countries of Central Asia, and among right-wing populist movements in Western Europe. But Russian soft power was quite limited. What Russia lacks in soft power, however, it has made up with its sharp power manipulation of social media.

In 2007, President Hu Jintao told the 17th Congress of the Chinese Communist Party that China needed to increase its soft power, and it has been spending billions on broadcasting, exchange programs and Confucius Institutes to teach Chinese language and culture.[16] In addition China's impressive economic performance has added to its attractiveness. David Shambaugh estimates that China spends $10 billion a year on its soft power instruments, but it has earned a modest return on its investment. The "Soft Power 30" index ranks China 27th (and Russia 28th) out of 30 countries assessed, far below the US and European democracies.[17] But China also goes beyond soft power and tries to exercise discourse control and export censorship beyond its borders by manipulation of visas, threatening loss of access to its markets, control of its information companies, covert broadcasting and payments to foreign groups and politicians. While China has not tried to disrupt the American political process to the extent that Russia has, it has used cyber and other means to intervene in politics in other countries. As Eric Rosenbach and Katherine Mansted point out, democratic civil society actors are often " the primary agents for much of the soft power appeal of the U.S. system of government. This dynamic means that authoritarian states do not just view control of their information environments as a domestic matter; they increasingly believe that offensive action might be required to counter what they perceive as foreign information incursions."[18]

Other authoritarian countries such as North Korea and Iran manipulate information to undercut American power, but Russia and China are the most important. Russian interference in European democracies' domestic politics is designed to reduce the attractiveness of NATO, the embodiment of

Western hard power, which Russia views as a threat. In the nineteenth century, the outcome of contests for mastery of Europe depended primarily on whose army won; today, it also depends on whose story wins.[19] Or as Singer and Brooking argue, "these new wars are not won by missiles and bombs, but by those able to shape the story lines that frame our understanding…" [20] In addition to formal public diplomacy organizations like Russia Today and Sputnik, Russian intelligence units and their proxies generate false information that can later be circulated and legitimated as if it were true. And it is easy and cheap to send such disinformation across borders.

Authoritarian sharp power has disrupted Western democratic processes and tarnished the brands of democratic countries, but it has done little to enhance the soft power of its perpetrators—and in some cases it has done the opposite. For Russia, which is focused on playing a spoiler role in international politics, that could be an acceptable cost. China, however, is a rising power that requires the soft power of attraction to achieve its objectives as well as the coercive sharp power of disruption and censorship. These two goals are hard to combine. In Australia, for example, public approval of China was growing until the revelation of its use of sharp power tools, including meddling in Australian politics, set it back considerably. In other words, Chinese deceptive sharp power undercut its soft power.

Although sharp power and soft power work in very different ways – attraction vs. coercion -- the distinction between them can sometimes be hard to discern in particular instances and that complicates the response to authoritarian sharp power. Attraction and persuasion involve choices about how to frame information. When that framing shades into deception which limits the subject's voluntary choices it crosses the line into coercion. Openness and limits on deliberate deception distinguish soft from sharp power. When RT or Xinhua broadcast openly in other countries, they are employing soft power. Similarly, properly labeled advertising in American media are legitimate exercises of soft power. If their messages are too blatantly propagandistic, they will not attract support and thus fail to produce soft power, but democracies can deal with open information. When the authoritarian states covertly back radio stations in other countries, or secretly promote news on social media, that deception crosses the line into

sharp power. Transparency and proper disclosure is necessary to preserve the principle of voluntarism that is essential to soft power.

As democracies respond to sharp power, we have to be careful not to undercut our own soft power by imitating the authoritarian model. Much of American soft power comes from our civil society—Hollywood, universities, and foundations more than from official public diplomacy efforts—and closing down access or ending openness would undercut our crucial asset. Authoritarian countries such as China and Russia have trouble generating their own soft power precisely because of their unwillingness to free the potential talents in their civil societies – witness Chinese censorship of its film industry or the harassment of the artist Ai Weiwei which undercut its soft power overseas. Moreover, shutting down legitimate Chinese and Russian soft power tools can be counter-productive. For example, if China and the United States wish to avoid conflict, exchange programs that increase American attraction to China, and vice versa, can be good for both countries. And on transnational challenges which pose a shared threat such as climate change, soft power can help build the trust and networks that make cooperation possible. But the programs have to be open and transparent to pass the test of soft power.

It would be a mistake, therefore, to prohibit Russian and Chinese soft power efforts simply because they sometimes shade into sharp power. Congress has required that RT be registered as a foreign entity, but it would be a mistake to go further and ban its broadcasts. At the same time, it is important to monitor the dividing line carefully. Take the 500 Confucius Institutes and 1,000 Confucius classrooms that China supports in universities and schools around the world to teach Chinese language and culture. Government backing does not mean they are necessarily a sharp power threat. Only when a Confucius Institute crosses the line and tries to infringe on academic freedom (as has occurred in some instances) should it be treated as sharp power intrusion and be closed.

Democracies must also be careful about our own offensive information actions. It may make sense to establish an American "political warfare" capability and strategy in an age of hybrid warfare, but a good strategy must be carefully designed and implemented.[21] Public diplomacy and

broadcasting should be public. It would be a mistake to imitate the authoritarians and use major programs of covert information warfare as we did in the Cold War. Such actions will not stay covert for long and when revealed would undercut our soft power as we saw in the 1970s when many CIA covert cultural operations were disclosed. Some argue that in the information struggle against authoritarian systems, democracies should use every weapon available and not worry about nice distinctions between soft and sharp power. However, the two types of power are hard to combine successfully in the long term, and some apparent arrows in the quiver of political warfare may turn out to be boomerangs. In the long term, central manipulation of information can make authoritarian states brittle, and openness may make democracies more resilient.

In the realm of defensive measures, democratic governments must counter the authoritarians' aggressive information warfare techniques (as we shall see below), but openness remains the ultimate defense of liberal societies. The press, academics, civic organizations, government, and the private sector should focus on exposing information warfare techniques, inoculating the public by exposure. Openness is a key source of democracies' ability to attract and persuade. As Henry Farrell and Bruce Schneier point out, information plays a very different role in legitimizing the political order of autocracies than in democracies.[22] Even with the mounting use of sharp power, we have little to fear in open competition with autocracies for soft power. If we succumb to temptation and lower our standards to the level of our authoritarian adversaries, democracies will squander our key advantage.[23]

Technology, New Tools, and Remedies

The authoritarian threat to democracy takes a number of forms ranging from the corruption of election machinery to the manipulation of voters through fake news, through the targeting and destruction of particular candidates, the creation of inauthentic groups to generate or exacerbate conflict, and the creation of chaos and disruption to discredit the democratic model. In the 2016 American presidential election, for example, Russians scanned election systems in at least 22 states; hacked into individual emails and leaked out the contents; and created fake accounts, trolls, and disinformation to disrupt the political process.

Hacking Electoral Systems

The most direct way to corrupt democracy is to manipulate the electoral systems and alter the calculations of voting. This can be accomplished through hacking into voting machines or into the rolls of registered voters. This is a particular problem with older voting machines which do not have a paper backup, but now 80 per cent of Americans vote on machines that incorporate paper ballots or backups. Since 2016, many state voter registration data bases have been hardened against outside attacks. A number of civic organizations have developed programs to alert and train local election officials. State election officials are gaining security clearances to permit access to federal threat information, and in 2018 all 50 states and more than 1000 localities opened a center to exchange data. While hacking election systems remains possible, it is increasingly difficult to rig enough decentralized devices and records to change the outcome of a national election. The Department of Homeland Security has declared that election systems are part of the national critical infrastructure and that makes it now easier to share threat information with state and local officials. Russia does not need to hack into machines to create mistrust about election results. Some of the damage is self-inflicted by American politicians and media, but the press seemed more alert to this danger in the 2018 midterm elections than it had been in 2016. Creating and publicizing a good

process is essential. While important, hacking into machines may be the most straightforward and easiest part of the puzzle to solve.[24]

Disseminating Fake News

The term "fake news" has become a political epithet, but as an analytical term, it describes deliberate disinformation that is presented in the format of a conventional news report.[25] Again, the problem is not completely novel. In 1924, Harpers' Magazine published an article about the dangers of "fake news", but today two-thirds of American adults get some of their news from social media where algorithms can be easily be gamed for profit or malice. What is different about social media is that they rest on a business model which lends itself to outside manipulation. Many organizations, both domestic and foreign, amateur, criminal and governmental are skilled at reverse engineering the ways that tech platforms parse information. To give Russia credit, it was one of the first governments to understand how to weaponize social media.

The Internet has flooded the world with information and when people are overwhelmed with the volume of information confronting them, they find it hard to know what to focus on. Attention rather than information becomes the scarce resource to capture. Friends become pointers and filters. Big data and artificial intelligence allow micro-targeting of communication so that people's information is limited to a "filter bubble" of the like-minded. The so-called "free" services of social media are based on a profit model in which the user or customer is actually the product, and their information and attention is sold to advertisers. Algorithms are designed to learn what keeps users engaged so that they can be served more ads and produce more revenue.

Emotions such as outrage stimulate engagement, and false news which is outrageous has been shown to engage more viewers than accurate news. A study of demonstrations in Germany, for example, found that "YouTube's algorithm systematically directs users toward extremist content… It looks like reality, but deforms reality because it is biased toward watch time."[26] False news is often more outrageous than accurate news, and one

study found that falsehoods on Twitter were 70 percent more likely to be retweeted than accurate news.[27] Fact checking by conventional news media is often unable to keep up in the race for attention, and sometimes can be counterproductive by drawing more attention. The nature of the social media profit model can be exploited as a weapon by states and non-state actors alike.

Recently Facebook chief executive Mark Zuckerberg wrote that "in 2016, we were not prepared for the coordinated information operations we regularly face. But we have learned a lot since then and have developed sophisticated systems that combine technology and people to prevent election interference on our services." Such efforts include automated programs to find and remove fake accounts; featuring Facebook pages that spread disinformation less prominently than in the past; issuing a transparency report on the number of false accounts removed; verifying the nationality of those who place political advertisements; hiring 10,000 additional people to work on security; and improving coordination with law enforcement and other companies over suspicious activity.[28] Even so, the arms race will continue between the social media companies and the states and non-state actors who invest in ways to exploit their systems.[29] Artificial intelligence cannot alone solve this problem. It turns out to be far easier to develop an algorithm that identifies nudity than one that identifies hate speech. In 2018, Facebook reported that only 38 percent of hate speech was flagged by its internal systems compared to 96 percent of adult nudity.[30]

Ironically, because it is often more sensational and outrageous, fake news travels further and faster than real news and that makes it profitable. False information on Twitter is retweeted by many more people and far more rapidly than true information, and repeating false information, even in a fact-checking context, may increase an individual's likelihood of accepting it as true.[31] The Internet Research Agency in St Petersburg "spent more than a year creating dozens of social media accounts masquerading as local American news outlets."[32] Sometimes the reports favored a candidate, but often they were designed to give an impression of chaos, disgust and to suppress voter turn-out.

When Congress passed the Communications Decency Act in 1996, social media companies were treated as neutral telcoms providers where customers could communicate with each other, but this model of pipes that ignores content is clearly outdated. Under political pressure, the major companies have begun to police their networks more carefully and take down obvious fakes, including those propagated by botnets, but the question of limits on free speech is a problem. While machines and foreign governments have no First Amendment rights (and private companies are not bound by the First Amendment in any case), some abhorrent domestic groups and individuals have free speech rights in our democracy and they can serve as intermediaries for foreign influencers. Foreign manipulation of accurate news about polarized American actors may have more impact than fake news. The damage done by foreign actors may be less than the damage we do to ourselves through polarized political rhetoric and tactics.

The social media companies have now encountered political controversy about their censorship of hate speech and conspiracy theorists. Companies want to avoid regulation, but legislators criticize them for both sins of omission and commission. This part of the problem will not be easy to solve because it raises trade-offs among our important values. Experience from European elections suggests that investigative journalism and alerting the public in advance can help inoculate against disinformation campaigns, but the problem of fake news is likely to remain a cat and mouse game between companies and fakers (both foreign and domestic) as part of the continual background noise of elections.[33]

Manipulating False Actors and Creating Astroturf Groups

Artificial actors can be created and manipulated to create chaos, social conflict, and disrupt the political process. Successful infiltration of the political process requires the creation of fake social media profiles that appear to be authentic, and then their coordination into false grass roots groups. For instance, in May 2016 there was a confrontation in Houston between demonstrators for and against a mosque screaming at each other (and being videoed for the Internet) but both the pro and anti-mosque protests had been planned and promoted by trolls in Russia.[34] A Russian-created

account @Blacktivist had 360,000 likes on Facebook – more than the verified BlackLivesMatter account on Facebook. A Russian created group posted authentic video of black and white people hitting each other to exacerbate racial animosity. "Not only did the Kremlin create individuals and organizations on both sides of wedge issues, they also used targeted advertising to reach the audiences that they believed would be most receptive."[35] Other actions were to harass candidates or influential people with organized trolling, including botnets, to the point that they dropped offline. Again, companies can monitor their platforms and public exposure can help, but it is difficult to prevent external manipulation of domestic divisions by analysis of big data and micro-targeting sensitive groups. On the other hand, taking down fake accounts and artificial actors is less likely to encounter the thorny censorship and free speech problems that plague the fake news problem.

Using Artificial Intelligence and Deep Fake Videos

Computers have long been used to generate and manipulate images, but fake images were often detectable by shifts in lighting and voices were often slightly off in cadence or tone. Now with artificial intelligence and deep machine learning, it is "possible to doctor images and video so well that it is difficult to distinguish manipulated files from authentic ones." And with "generative adversarial networks, the algorithm works by getting really good at fooling itself."[36] Distributed ledger technologies may help in verification, but blockchain solutions may not be quick enough to prevent deep damage to political reputations.

When introduced late in a campaign, deep fakes may remain credible for long enough to alter an election result, particularly if they are embedded as brief offhand offensive remarks in otherwise authentic video. While companies are investing in research on counter measures such as digital watermarks, it is far from clear that the defensive technologies of detection will advance as rapidly as the offensive technologies of deception. Nonetheless, artificial intelligence may eventually help the defense as much as the offense if we invest in it.

A Strategy for Response

The defense of democracy in an age of cyber information war cannot rely on technology alone. It will require a strategy with several strands, and will have to involve many government departments, close coordination with the private sector, and will best be coordinated from the White House. The key elements will include domestic resilience and defense; deterrence, and diplomacy.

Domestic resilience

Some steps are underway; others remain to be taken. Progress has been made on training and support of local election officials and upgrading the security of election infrastructure including paper backups.[37] Political parties, candidates and staffs have become more alert to the importance of basic cyber hygiene such as encryption and dual authentication, but phishing is always a danger and volunteers are often untrained. Various civic organizations are focused on the problem and investigative journalism and independent fact-checking has helped to alert the public and inoculate against some of the cruder forms of sharp power.

Laura Rosenberger of the Alliance for Assuring Democracy has suggested a number of further steps such as an honest ads act which would apply the same rules to online political advertising as apply to such ads on TV; a rule requiring social media companies to disclose any bots on their platform, and prohibit candidates and parties from using bots; creating a better legal framework for protection of data privacy; and enhancing better mechanisms for information sharing among government agencies and with the private sector.[38]

The social media platforms are crucial to coping with this problem, but rather than heavy handed regulation a process should be set up for continual consultation and sharing of information between the companies and government. Rather than turn the companies into purely private censors, *The Economist* has recommended making the companies more publicly

"accountable for their procedures: clarify the criteria applied to restrict content; recruit advisory bodies and user representatives to help ensure that these criteria are applied; give users scope to appeal against decisions. They also need to open their algorithms and data to independent scrutiny, under controlled conditions."[39]

Independent bipartisan boards or commissions might enhance algorithmic accountability without revealing proprietary information in a damaging way. Rather than try to break up the companies or deprive them of all autonomy, it would be better to have them monitor their systems more effectively and in a publicly more accountable manner. As Alex Stamos has argued, the companies will "need to act in a quasi-governmental manner, making judgments on political speech and operating teams in parallel to the US intelligence community, but we need more clarity on how these companies make decisions and what powers we want to reserve to our duly elected government."[40] But given the transnational scale of the companies, there will have to be provisions for cultural differences about values like privacy and fairness, and companies will have to obey local laws. Few other countries share American "First Amendment absolutism", and that includes allied democracies like Germany and France.[41]

More generally, a successful strategy would have to focus on raising the general level of cyber hygiene in society and government. This would not solve the problem, but it could remove the most vulnerable low hanging fruit and make the tasks of attackers more costly. Stronger cyber defense measures are like vaccinations in term of creating public goods, and legal frameworks could be developed to encourage this. The 2016 problems of hacking and doxing political e-mails could be made more difficult if dual factor identification and encryption were more widespread. Much could be done to encourage development of higher standards in software by revising liability laws, and encouraging the development of the cyber insurance industry as the number of points of vulnerability to cyber intrusion expands exponentially with the Internet of Things.[42] Similarly, more can be done to improve the quality of cyber security in government agencies both by new investment and by raising standards.

Deterrence

Some skeptics believe that deterrence does not work in cyber conflict, at least not in the gray zone of hybrid warfare below the level governed by the law of armed conflict. They often cite the case of the 2016 election where President Obama personally warned President Putin to desist in September but to no avail, and where American intelligence officials have told the Congress that Russian interference continues. But the case is not definitive because American responses were inhibited by domestic politics in both parties. In September 2018 President Trump signed an executive order enabling sanctions (which include asset freezes and prohibitions from doing business) and defined foreign interference as efforts to "influence, undermine confidence in, or alter the result or reported result" of an election or "undermine public confidence in election processes or institutions." That broad definition would cover anything from state-sponsored social media campaigns to altering vote tallies. Its effectiveness remains to be seen, but deterrence must be a crucial part of a successful strategy.

Understanding deterrence in cyberspace is often difficult because our minds are captured by Cold War images of deterrence as threatening massive retaliation to a nuclear attack by nuclear means. The analogy to nuclear deterrence is misleading, however, because the aim with nuclear explosions is total prevention. In contrast, many aspects of cyber behavior are more like other behaviors, such as crime, that governments strive only imperfectly to deter. Moreover, cyber deterrence need not be limited to cyber responses, but can cross domains. There are four major mechanisms to reduce and prevent adverse actions in cyberspace: threat of punishment, denial by defense, entanglement, and normative taboos. None of these four mechanisms is perfect, but together they illustrate the range of means by which it is possible to reduce the likelihood of adverse acts causing harm. They can complement one other in affecting actors' perceptions of the costs and benefits of particular actions.[43]

Deterrence by defense involves many of the steps we already wish to take to enhance our resilience, and by hardening ourselves as a target, we affect the ratio of costs to benefits that an attacker expects. If the targets are soft and the costs are low, the temptations are greater. That need not be the case.

Deterrence by entanglement refers to situations where an attacker holds back because the interdependence is so great that damaging the target may damage oneself. That level of interdependence does not exist between the US and Russia, Iran or North Korea. And despite some progress in the UN Group of Government Experts that reported in 2015 on development of norms restricting damage to civilian targets, cyber taboos are not as strong as they are, for example, in biological weapons. It is interesting, however, that after the events of 2016, the US added electoral processes to a list of 16 critical civilian infrastructures as a signal.

Deterrence by threat of retaliation remains a crucial but underutilized aspect of deterrence of cyber attack. There has been no attack on our electrical systems despite the reported presence of Chinese and Russians on the grid. Pentagon doctrine has announced that we will respond to damage with any weapon of our choice, and deterrence seems to be working at that level. Presumably it could be made to work in the gray zone of hybrid warfare as well if we had not been so pusillanimous in our responses to 2016 and 2017. Since American intelligence is reported to carry out espionage in Russian and Chinese networks, one could imagine that we discover embarrassing facts about the hidden assets of foreign leaders which we could threaten to disclose or bank accounts we could shut. Similarly, we could go further in applying economic and travel sanctions against authoritarians' inner circles. The diplomatic expulsions and indictments that have occurred thus far are only a first step toward strengthening our deterrent threat of retaliation.

Diplomacy

Negotiating treaties for cyber arms control involves a number of problems, but this does not make diplomacy impossible. In the cyber realm, the difference between a computer program that is a weapon and a non-weapon may come down to a single line of code, or the same program can be used for legitimate or malicious purposes depending on the intent of the user. Thus it will be difficult to anathematize the design, possession, or even implantation for espionage of particular programs. In that sense, cyber arms control cannot be like the nuclear arms control that developed during the Cold War.

Verification of the absence of a stockpile of zero day exploits would be virtually impossible, and even if it were assured, the stockpile could quickly be re-created. Unlike physical weapons, for example, it would be difficult to reliably prohibit possession of the whole category of cyber weapons.

But if traditional arms control treaties are too difficult, it may still be possible to set limits on certain types of civilian targets, and to negotiate rough rules of the road for behavior that limits conflict. For example, the US and Soviet Union negotiated an Incidents at Sea Agreement in 1972 to limit naval behavior that might lead to escalation. The US and Russia might negotiate limits to their behavior regarding each other's domestic political processes, in which we would draw a line between activities that constitute soft power and those that cross the line into sharp power. Even if they cannot agree on precise definitions they could exchange unilateral statements about areas of self-restraint and establish a consultative process to prevent escalation. Such a procedure of exchanging unilateral statements could protect democratic non-governmental organizations' right to criticize authoritarians while at the same time creating a framework that limits governmental escalation.

Skeptics object that such an agreement is impossible because of the difference in values between our two societies, but even greater differences did not prevent agreements related to prudence during the Cold War. Skeptics also say that since elections are meaningless in Russia, they would have no incentive to agree, but this ignores the potential threat of our retaliation across domains as discussed above. Others object to the implied moral equivalence, but since our democracy is more open and we have more to lose in the current situation, that should not hold us back from pursuing our self interest in developing a norm of restraint in this gray area.

As Jack Goldsmith puts it, "The United States needs to draw a strong principled line and defend it. That defense would acknowledge that the United States has interfered in elections itself, renounce those actions and pledge not to do them again; acknowledge that it continues to engage in forms of computer network exploitations for various purposes it deems legitimate; and state precisely the norm that the United States pledges to stand by and that the Russians have violated."[44] This would not be unilateral

disarmament on our part since we would draw the line between soft and sharp power; overt programs and broadcasts would continue to be allowed. We would not object to the content of others' political speech but to how they pursue it through covert coordinated inauthentic behavior. Non-state actors often act as proxies of the state in varying degrees, but the rules of the road would require their open identification. Even if adherence to such rules of the road were imperfect on the part of authoritarian states, a reduction of their level of interference could make our defense of our democracy more feasible.[45]

Conclusions

Democracy depends upon open information that can be trusted. Authoritarian states can exploit and weaponize this openness. Information warfare is not new, and it has always presented a challenge to democracy, but technology has transformed the nature of the challenge. What's new is the speed with which such disinformation can spread and the low cost and visibility of spreading it. The Internet has expanded the information attack surface and the instruments that can exploit it. Electrons are cheaper, faster, safer, and more easily deniable than human spies. What is more, the business models of the large American social media companies can be readily manipulated by malign actors for criminal or political purposes. But as democracies respond to such challenges, they run the risks both of doing too little, but also too much. Measures that curtail openness and trust would become self-inflicted wounds. This will be true of both the defensive and offensive measures that democracies undertake. Imitation of the authoritarian practices would be a defeat.

In the case of Russian interference in the 2016 presidential election, the United States was poorly prepared and inadequate in its response. Different vectors of attack require different measures. Hacking and doxing of political actors requires greater awareness and practice of cyber hygiene. Hacking of electoral machinery and voter rolls requires more robust machines and audit trails as well as improved federal, state and local cooperation. Thwarting and removing false accounts, botnets, sockpuppets and

astroturf actors requires strong action and cooperation among social media companies. Dealing with fake news designed to polarize, disrupt and suppress voting also requires action by the companies but with procedures for protecting transparency in algorithms and processes that reveal difficult trade-offs regarding free speech. None of this will be solved easily. In some cases, artificial intelligence will help the offense, in other cases the defense. The game of cat and mouse does not end; it must be continually monitored.

At a more general level, a national strategy for defending democracy in the cyber age must include all three dimensions of resilience, deterrence and diplomacy. American actions have been inadequate on all three dimensions but some useful steps have begun, and this discussion has suggested more that can be done. We are only at the beginning of a long process of protecting democracy in an era of cyber information war.

Endnotes

I am grateful to Jack Goldsmith, Trey Herr, Alexander Klimburg, Eric Rosenbach and Michael Sulmeyer for comments on an early draft.

1 William J. Clinton, "Remarks at the Paul H. Nitze School," (Washington, March 8, 2000) http://www.presidency.ucsb.edu/ws/index.php?pid=87714

2 Kenneth Osgood, "The CIA's Fake News," *New York Time*s, October 14, 2017, pA19.

3 Herb Lin and Jackie Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation," *Oxford Handbook of Cyber Security,* Paul Cornish ed., Oxford University Press 2018, Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (Rand Corporation 2016).

4 Sir David Omand, "The threats from modern digital subversion and sedition,"*Journal of Cyber Policy*, 2018, pp 1-19

5 Michael Hayden quoted in Davis V. Gioe, "Cyber Operations and useful fools: the approach of Russian hybrid intelligence," Intelligence and National Security. https://doi.org/10.1080/02684527.2018147934
5. Hayden also is reported to have said "I would not want to be in an American court of law and be forced to deny that I never did anything like that as director of NSA." "Suing Spies," The E*conomis*t, September 15, 2018, p29.

6 Suzanne Spaulding, "Countering Adversary Threats to Democratic Institutions: An Expert Report" Washington, Center for Strategic and International Studies, 2018, p 4.

7 Kate Conger and Adam Satariano, "Twitter Clamps Down, But Rogue Accounts Turn the Pressure Up," *New York Times,* November 6, 2018

8 Tony Romm, "New report on Russian disinformation, prepared for the Senate, shows the operation's scale and sweep," *Washington Post*, December 17, 2018. See also Scott Shane, "Five Takeaways from Reports on Russian Campaign, *New York Ti*mes, December 18, 2018, pA14

9 Renee DiResta, "Russia's Information Warfare," *New York Times*, December 18, 2018, pA23.

10 For details of "Operation Infektion", see P.W. Singer and Emerson T. Brooking, *Like War: The Weaponization of Social Media*, New York, Houghton Mifflin, 2018, p104.

11 See Alexander Klimburg, "Hacking the Presidency," Review of Kathleen Hall Jamieson's CyberWar, *Nature*, Vol 562, October 11, 2018. See also Alexander Klimburg, *The Darkening Web*, New York, Penguin, 2017,2018,

12 Tim Maurer and Garrett Hinck, "Russia: Information Security Meets Cyber Security," in Fabio Rugge, ed. *Confronting an Axis of Cyber*? Milano, Ledi Publishing, 2018, p 39.

13 Eric Rosenbach and Katherine Mansted, "Can Democracy Survive in the Information Age," https://www.belfercenter.otg/publication/can-democracy-survive-information-age October 2018

14 Singer and Brooking, cited, p 106

15 Christopher Walker and Jessica Ludwig, *Sharp Power: Rising Authoritarian Influence*, Washington, National Endowment for Democracy, 2017.

16 David Shambaugh, *China Goes Global,* Oxford, Oxford University Press, 2013

17 Portland and USC Center on Public Diplomacy, *The Soft Power 30: A Global Ranking of Soft Power*. London, 2017

18 Rosenbach and Mansted, cited.

19 John Arquilla and David Ronfeldt, The Emergence of Noopolitik: Toward an American Information Strategy. Santa Monica, RAND,1999, pp ix-xii

20 Singer and Brooking, cited, p21.

21 See Charles Cleveland, Ryan Crocker, Daniel Egel, Andrew Liepman and David Maxwell, "An American Way of Political Warfare: A Proposal," *Perspective*, July 2018. Santa Monica,RAND, 2018.

22 See Henry Farrell and Bruce Schneier, "Common-Knowledge Attacks on Democracy." Berkman Klein Center Research Publication No. 2018-7 November 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273111

23 See Suzanne Spaulding and Eric Goldstein, "Countering Adversary Threats to Democratic Institutions," Washington, CSIS. February 2018.

24 Michael Wines and Julian Barnes,"Fear Trolls, Not Hacked Voting Machines," *New York Times*, August 3, 2018, p16

25 David Lazer et. al, "The Science of Fake News," *Science*, March 9, 2018, Vol 359, Issue 6380,

26 Max Fisher and Katrin Bennhold, "Germans, Seeking News, Find You Tube's Far Right Tirades," *New York Time*s, September 8, 2018, pA4.

27 Sheera Frenkel, Mike Isaac, and Kate Conger, "With Growth, Social Media Spread Harm," *New York Times*, October 30, 2018, pA1

28 Sheera Frenkel and Mike Isaac, "Facebook, After Reforms, Is Now Better Prepare to Ward Off Skulduggery," *New York Times*, September 14, 2018, p B2

29 Kevin Roose, "Capitalizing on a Mass Killing to Spread Fake News Online," *New York Times*, October 3, 2017, p19

30 Sheera Frenkel, Mike Isaac and Kate Conger, "With Growth, Social Media Spread Harm," *New York Times*, October 30, 2018.

31 Lazer et al., cited above, p 1095

32 Jared Cohen, "Confronting Hybrid Warriors and the Disinformation Tactics They Use," paper delivered at the Aspen Strategy Group, August 2018.

33 Erik Brattberg and Tim Maurer, "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks," Washington, Carnegie Endowment, 2018. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

34 Farhad Manjoo, "The Drama of Reality TV, Brought to You by Russia," *New York Time*s, November 9, 2017, pB1. See also, Darrell West, "How to combat fake news and disinformation: a report.," Washington, Brookings, December 2017.

35 Jared Cohen, cited above.

36 Chris Meserole and Alina Polyakova, "The West is ill prepared for the wave of 'deep fakes' that artificial intelligence could unleash," Washington, Brookings Institution, May 25, 2018

37 See for example, Defending Digital Democracy Project, *Election Cyber Incident Communications Coordination Guide*, Cambridge, Harvard Kennedy School, February 2018.

38 Laura Rosenberger, "Countering Technologically-Driven Information Manipulation," paper delivered at the Aspen Strategy Group, August 2018. See also Laura Rosenberger and Jamie Fly, "Shredding the Putin Playbook," *Democracy Journal*, Winter 2018, pp 51-63.

39 "Truth and Power," *The Econo*mist, September 8, 2015, p14

40 Alex Stamos, "Yes, Facebook made mistakes in 2016. But We Weren't the Only Ones," *Washington Post,* November 17, 2018.

41 See Frederick Schauer, "The Politics and Incentives of Legal Transplantation," in Joseph Nye and Jack D. Donahue, eds, *Governance in a Globalizing World*. Washington, Brookings,2000, p253

42 Ariel Levite, Scott Kannry, Wyatt Hoffman, "Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance," Washington, Carnegie Endowment, November 2018.

43 J.S. Nye, "Dissuasion and Deterrence in Cyber Space" , *International Security*, 41 (3) 47-71

44 Jack Goldsmith, "Uncomfortable Questions," https://na01.safelinks.protection.outlook.com?url=https%3A%2F%2Fwww.lawfareblog.com. See also Jack Goldsmith, "The Failure of Internet Freedom," *Knight Foundation Emerging Threats Series* (June 2018), available at https://knightcolumbia.org/content/failure-internet-freedom, and

Jack Goldsmith and Stuart Russell, "Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations," *Hoover Institution Aegis Papers, No. 1806* available at https://www.hoover.org/sites/default/files/research/docs/381100534-strengths-become-vulnerabilities.pdf.

45 Alex Grigsby, "Russia Wants a Deal with the United States on Cyber Issues: Why Does Washington Keep Saying No? New York, Council on Foreign Relations. Net Politics. August 27, 2018

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

www.belfercenter.org

Printed in the United States of America