7

GOVERNANCE FROM AN INTERNATIONAL PERSPECTIVE

William Drozdiak

Disruptive technologies pose a pervasive challenge to democracies around the world. These engines of human progress bring vast benefits. But they also pose risks to fundamental values of democracy. In some cases, new technologies that offer a great leap forward for humanity—instant communications around the globe or the creation of driverless cars that curtail deadly accidents—can also be viewed as potential threats to political order, shared prosperity, and stable communities.

The internet was once regarded as a powerful weapon of democracy, an ingenious way to circumvent government censorship and empower the voices of common people. The Arab Spring rebellions that toppled dictators in Tunisia, Libya, Egypt, and Yemen heralded this new era. Yet now many autocracies have learned to employ digital tools to further suppress their people by blocking access to free information or by distorting the news that they receive. As they have in the past, autocracies claim such actions are justified to ensure the security of society over individual freedoms. They argue that in spite of rampant corruption and human rights abuses, the relative stability that prevails under autocrats is a better state of affairs than the violent anarchy that would follow their overthrow. Only now they can unleash new electronic tools of surveillance and repression of dissent. And as seen by Russia's meddling

in Western elections, autocrats are also willing to distort information as a tool of hybrid warfare against democratic societies as a way to wage aggression without declaring war.

Criminal gangs have also learned how to exploit the internet. In February 2016, digital bank robbers infiltrated SWIFT, the global banking payments system, and stole $81 million from the central bank of Bangladesh, which was the largest hack ever of an international financial institution.[1] Later that year, Yahoo revealed a breach of more than one billion user accounts—about one-third of the global population of the internet at the time—in which passwords and encrypted security questions were stolen. And the Mirai botnet attack, which targeted household devices and electronic products, disabled the internet's domain name system and brought down sites including Twitter, Netflix, and CNN in an attack that was twice as powerful as any previous disruption on record.

The number of devices connected to the internet now exceeds our global human population of 7.5 billion. By 2020, according to the digital technology company Cisco, there will be more than fifty billion devices and sensors connected to an internet of things that will link smartphones, parking meters, thermostats, bank accounts, cardiac monitors, cars, supermarket shelves, and nearly every aspect of human life. The world has barely begun to grapple with the security and economic implications of building out this vast and vulnerable global network, involving billions of points of interconnection that could be disrupted by criminals, warlords, or mad dictators controlling a small army of hackers.

Our societies are becoming more diverse than ever, even as we wrestle with the forces of globalization. Successive waves of immigration have deepened our cultural, political, economic, and historical connections with the rest of the world. This growing diversity, coupled with the rise of digital social media, has created many fault lines and vulnerabilities within democracies that can be exploited by possible aggressors, whether they are based in Moscow, Beijing, Pyongyang, or Tehran, or have no fixed address, such as criminal syndicates.

Once-marginalized elements—from alt-right white supremacists in America to the Islamic State in the Middle East to hacker groups in Russia and Eastern Europe—can now rapidly cultivate a degree of social and political influence once deemed unthinkable. With about one-quarter of the world's population now on Facebook, the possibilities of extremist or hateful groups exploiting political grievances and cultural resentments in ways that cannot be controlled now threaten our democratic way of life.

Just as governments need to become more vigilant about unconventional forms of warfare, the public needs to be educated to become more discerning about the quality and credibility of information in the digital age. A promising development is the creation of popular news literacy courses for civil society that instruct young people how to navigate the maze of social media networks and to be discriminating in finding the truth by questioning the sources of what they read. Critical thinking skills have always been important, but they have become a vital necessity in the twenty-first century as people struggle to deal with information overload and to separate fact from fiction.

But fake news is only part of the story. The dangers posed by perverted or biased information are just a symptom of a larger truth now dawning on the world: with billions of people glued to Facebook, WhatsApp, WeChat, Instagram, Twitter, Weibo, and other popular services, social media is rapidly becoming perhaps the world's most dominant cultural and political force, to the point that its effects can alter the course of global events. Yet our democracies have not even come close to gaining a clear understanding of this explosive trend, let alone developing the means and methods to tame its power and ensure our values are protected.[2]

Political parties are being disrupted by radical reformers with no traditional power base who build their support online, as seen in the recent candidacies of Bernie Sanders in the United States and Emmanuel Macron in France. In the future, insurgent candidates will become more common as voters embrace politicians and policy prescriptions once viewed as outside the mainstream.

Besides the need to protect our political process and civic institutions from being disrupted by fake news and false information, the threat to our national security interests may be even more urgent. Following the failure to prevent Russian hackers from intervening in the election process, the United States needs to shore up its defenses against future intrusions. Rapid responses by Estonia, France, and Germany to thwart Russia's apparent efforts "to wage war without going to war" offer salutary lessons for the United States about the importance of stronger cyberdefenses in protecting vital infrastructure and raising vigilance levels during election campaigns. After neglecting the rising importance of cyberattacks in recent years, the NATO alliance now recognizes that "nonkinetic" weapons of hybrid warfare like hacking, subversion, espionage, and fake news pose serious threats to our security. Following Estonia's lead, Germany's new cybercommand was launched in April to help safeguard last September's election. Berlin's defense ministry has declared that cyberspace will now be considered the sixth branch of its armed forces.

The Western allies together need to develop a more sophisticated international strategy to block cyberattacks while still preserving democratic principles. NATO managed to win the Cold War with an effective deterrence strategy that contained Soviet aggression short of engaging in a nuclear conflict. As part of a new deterrent strategy to thwart cyberattacks, the Western alliance may need to consider whether it should deploy counterpropaganda programs against fake news and media manipulation by foreign countries in the way Voice of America and Radio Free Europe were used to counter *dezinformatsia* campaigns waged against the West by the Soviet Union.

During the Cold War, we had Radio Liberty and Radio Free Europe. All of the archival material came to our archive here at Hoover, so we had some people study it. And there were two questions. Did anything work? Number two, what did we learn? It was clear that everybody thought there really was a huge impact, and we learned a lot about how to do this effectively.—George P. Shultz

---

The Future of Employment and Social Order in Western Democracies

How Europe and the United States respond to the transformation of work and society by new technologies has already become an acute concern about how we can sustain our democracies in the twenty-first century. If, as recent research suggests, every industrial robot absorbs up to six jobs, that could mean up to six million jobs could be lost over the coming decade. This trend will also affect the problem of income inequality, since the poor and the young will suffer most. According to a White House economic report, there is more than an 80 percent chance that automation will take a job with an hourly wage below $20.

John Kasich, the Republican governor of Ohio, is one public official who worries about the impact of this rapid technological change on the health of our democracies if ever larger numbers of the poor, the young, and the less educated are thrown out of work. Speaking over dinner at the Munich Security Conference in early 2017, Kasich predicted that, by 2030, many truck drivers could find their jobs obsolete as driverless vehicles take over the roads.

"If truck drivers are one of the largest sources of jobs in my state, what do I or my successors need to do to prevent mass unemployment and all the social turmoil that goes with it?" Kasich asked. "If you think our society is polarized today, what will happen when you have an even greater disparity between rich and poor two decades from now? What happens when massive numbers of blue-collar workers have lost all hope for earning a decent living? It is a question that could make or break our democracy."[3]

Technological developments are forcing European politicians and business executives to reexamine their assumptions about labor markets, welfare benefits, and the now politically explosive subject of immigration. For example, Germany's interior ministry has for years warned in annual reports that because of its aging population and low birth rates the country should be prepared to accept as many as 400,000 migrants a year over the next quarter century to sustain the structure of

its export-driven economy and generate enough income taxes to pay for a generous health and welfare system. But in February this year, the ministry scaled down that assessment to 300,000 immigrants per year over the next forty years. One factor was the rapid growth of automation and artificial intelligence and the reduction in the labor force they make possible.

But perhaps even more important was the rise of xenophobic nationalists who have gained popularity by arguing against an influx of Muslim or African immigrants. And foreign adversaries seem ready to seek to exploit these tensions through fake news and social media. During the exodus of Syrian war refugees into Europe, Russia helped disseminate rumors on right-wing websites about alleged rapes and other crimes by immigrants as a way of stoking internal political divisions in Germany and elsewhere.

Chancellor Angela Merkel cited Germany's shrinking population as a reason to open the country's borders to more than one million refugees fleeing Syria's civil war in 2015. The immigrants were initially welcomed into Germany as Merkel and many commentators hoped they could rejuvenate the country's population and fill many of the job vacancies created by Germany's booming economy. But efforts to integrate so many Syrian, Afghan, Albanian, and North African immigrants have proved more difficult than imagined. And the startling rise in support for the right-wing Alternative for Germany party, which rose as high as 15 percent in some polls after demanding that Germany shut its doors to immigrants, forced Merkel to backtrack and adopt a less tolerant approach. The chancellor's tougher stance reassured some of her more conservative supporters and helped deflate right-wing gains in the weeks before the September vote.

Indeed, some European governments are now placing a greater priority on ensuring that their existing populations are capable of adapting to new jobs in a changing global economy rather than recruiting workers from abroad. Denmark's center-right government, supported by the right-wing Danish People's Party, has strongly discouraged the influx of immigrants and refugees by threatening to confiscate jewelry and valu-

ables worth more than $1,000 (ostensibly to pay for their food, lodging, and health care). At the same time, it has expanded efforts to help retrain and reeducate all Danish citizens who want to learn digital skills as a pathway to find better jobs and maintain unemployment levels at some of the lowest in Europe.

The Danish government seeks to ensure that as many people remain employed as possible in order to pay for a generous welfare state that offers free health service, up to five years of university education without cost, and subsidized care for children and the elderly. To persuade those without jobs and living on welfare stipends to return to the labor force as quickly as possible, the government makes extraordinary efforts to prepare its citizens to accept different kinds of employment and not focus on a lifelong career.

France's new president, Emmanuel Macron, has said his goal in seeking to cut his country's 10 percent unemployment rate (as high as 25 percent among young people) is to create a "Scandinavian-style economy" by reproducing many of the programs carried out in Denmark. And in the United States, former Democratic presidential candidate Bernie Sanders often declared during his campaign that his ideal vision for America would be to see his country become more like Denmark.

One out of four Danish workers changes jobs every year, more frequently than any labor force in the developed world. Employers are given great leeway in terms of hiring and firing workers to adapt to a highly competitive global economy—and worker training programs that keep adult citizens engaged in active work as often as possible are vital to sustain Denmark's enviable affluence. Denmark spends proportionately almost eighteen times as much as the United States on worker training, according to the Organisation for Economic Co-operation and Development.

Europe's worker training programs are considered much more advanced than in the United States, which may help the continent adapt better to the disruptions caused by the digital age. Germany's highly successful *Berufschule* program offers young people who do not go to university the chance to enroll in vocational training schools in which

the weekly schedule involves three days of classroom work combined with two days gaining hands-on experience in a company. This enables Germany to adapt vocational training to the modern needs of industry so that students can go straight into jobs. Some community colleges in the United States have shown an interest in emulating the German model, but for cultural and other reasons the American programs have failed to make a big impact in helping young people who do not go to university to learn the advanced skills that will lead to well-paying, sustainable jobs.

Other countries in the European Union are also pursuing labor policies designed to boost local employment in ways that may reduce dependence on immigrants. In the case of Poland, the country's right-wing government has shut the door to virtually all Muslim immigrants but welcomed Ukrainians who share the same Catholic faith. Poland's paramount leader Jaroslaw Kaczynski has spread false reports in the media claiming immigrants from the Middle East and Africa would bring "parasites and strange diseases" to Poland and must be kept out. Meantime, Germany and Scandinavian countries have placed a new emphasis on language skills before immigrants can expect to acquire good jobs.

Some European politicians believe the era of high-tech transformation will require democratic societies to think beyond questions like whether to accept more immigrants or how to fund the welfare state. They say that encouraging the moral benefits of work is critical to sustaining a healthy society—something that will become a vital issue for democracies as technology eliminates more jobs.

Former French prime minister Michel Rocard, who spent his last years promoting an education revolution from his seat in the European Parliament, became convinced that the emergence of digital technologies should require universities to become lifelong bastions of learning and thinking for people of all ages, not just the young.

Rocard, who died in 2016, believed it should become customary in Western democracies for people to return to universities every two decades to reinvent themselves and create new careers that would last

ten to twenty years. "Nobody should think of spending forty years at a single trade or profession and then go into retirement," he told me. "You should engage in phases of study and reflection in your twenties, in your forties, and again in your sixties, in order to prepare yourself for two, three, or four different careers."

The global economy will change so fast under the influence of new technologies, Rocard predicted, that people will need to go back to school regularly in order to learn new skills, or they will be left behind, leading to greater political and social alienation in Western society. On that score, his forecast is proving accurate.

There's a segregation going on; globalization is retreating. But now we're seeing there are important reasons why we need to have ways of getting together and talking on a global basis.—George P. Shultz

---

America and the World: The Clash over Data Privacy

The spectacular success of America's social media giants is often cited abroad as a principal reason why the United States remains the dominant force in the global economy. The powerful forces of innovation and entrepreneurial energy in Silicon Valley are both admired and feared in Europe, which is often accused of trying to obstruct the growth of American companies and protect the interests of the continent's homegrown enterprises.

The European Union has asked Ireland to seek $13 billion in back taxes from Apple, claiming it has unfairly exploited Ireland's low corporate tax rate while doing business in the twenty-eight-nation union. Apple has vowed to fight the EU demand. Airbnb is another company that has attracted the ire of European governments for escaping high taxes. Even though it has more than ten million users in France, Airbnb paid less than 100,000 euros in taxes last year in France.

Finance Minister Bruno Le Maire has vowed that the new French government under Macron will join Germany in pushing for the European Union to set a new global standard in imposing much higher tax assessments against the American digital giants. "All companies need to pay their fair share in tax in all the countries they operate in," Le Maire said. "That's not the case today. It's time to change gear. . . . We want the EU to take the lead in tackling this global issue."[4]

The American tech giants complain they are being unfairly targeted because of their overwhelming success. They say that punishing their performance will stifle innovation and ultimately hurt the quality of products offered to local users. Such actions, they claim, are designed to prop up weaker local rivals to the detriment of the consumer and amount to a new form of European protectionism.

But there are deeper forces at work in Europe besides competitive jealousy. Europe is genuinely worried that the untrammeled influence of American social media giants could shatter their cultural traditions of data privacy, encourage the spread of libelous rumors or "fake news," and generally erode civic democratic values. The horrible history of totalitarian abuses under Nazi, Fascist, and Communist regimes during the past century has made Europeans much more sensitive to the vast accumulation of personal data in the hands of the state or corporations.

Rather than seeing social media as a liberating force, Europeans tend to look toward the dark side and see a dystopian vision that could eventually dominate many aspects of human activity. "For us, big data equals big brother," a prominent Central European politician told me. "In the communist days, we used to worry about informers telling the government about the details of our private lives. Yet now, we inform on ourselves to the world at large through Facebook and Google."

Such distrust is spreading in Europe and making policy-makers uneasy about allowing social media to acquire enormous power and influence under the guise that free speech must remain a fundamental right in any democracy. Many Europeans feel that limits on hate speech, child pornography, and terrorist propaganda may be necessary in a modern democracy to find the right balance between freedom and security.

"Social media can challenge the basic principles of democratic life," said Margrethe Vestager, the EU's antitrust chief who has waged fierce battles against Facebook, Google, Apple, and other social media titans.[5] "If we are not careful, social media could let us down. Because despite all the connections it allows us to make, social media can also lock us up in our own worlds. . . . And we can't have an open debate from inside separate worlds."

"Lately, politicians have been learning a lesson that business has known for a long time," Vestager told a Brussels conference about democracy in the digital age. "The information that social media companies collect about their users can transform the way you advertise. It can help you put your message in front of exactly the people who are likely to buy it. But when you apply that to politics, it could undermine our democracy."

As one of Europe's most influential policy-makers, Vestager said she believes that the digital age presents serious challenges to basic rights such as personal privacy. She has been instrumental in pushing through new rules on data privacy across the European Union that will take effect in 2018 and are designed to protect the EU's five hundred million citizens from unwelcome intrusions that can be exploited by business.

She said, "More than four-fifths of Europeans feel that they don't have control over their personal information online. So we need rules to give them back that control."[6] She said an important part of new EU legislation is "data protection by design"—a principle that means "when you come up with a new digital service, you have to think from the start about how to protect people's privacy, so that treating people fairly isn't just an afterthought."

Many politicians across Europe share Vestager's view that digital technology companies must be held accountable for any unwanted exploitation of personal information. The United States has favored a softer approach, reflecting an aversion to putting too many limits on free enterprise and free speech. But in Europe, as in Asian democracies like South Korea and Japan, there is a greater willingness for the state to enforce tighter controls on abuses, such as hate speech and fake news,

including the imposition of harsh penalties against companies that convey such information on internet platforms.

Vestager is reshaping antitrust law for the digital age. This year, she slapped a 2.42 billion euro penalty ($2.76 billion) on Google for abusing its dominant position in Europe as a search engine. The European Union also approved a pan-European digital privacy law that could have profound effects on the way social media companies use personal information. After four years of negotiations, the EU agreed to a common legal approach protecting digital privacy rights that will empower EU regulators to impose fines up to 4 percent of a company's worldwide revenue. This could lead to record penalties against American social media giants and other large corporations that have become data-dependent in the way they conduct business.

The purpose of the European law is to invest greater power in the hands of consumers and force large companies to respect their wishes when it comes to data-mining practices. The law will require these companies to seek additional consent every time they want to use such information. Online advertisers and data analytics firms say their business could be devastated and the EU approach will hurt innovation. They claim it shifts the burden of proof and could drag their companies into constant litigation to prove they are not at fault in any privacy violations. The law will also enshrine the controversial "right to be forgotten," which allows people to request deletion of personal data from online platforms like Facebook or Google.[7]

The EU claims it is upholding basic democratic values by protecting the rights of its citizens to control the most personal aspects of their lives. Privacy advocates believe the EU approach may soon become a model for the rest of the world. As Japan, South Korea, and other Asian nations consider adopting the tougher EU standards on data privacy, American companies will need to accept those rules or risk being excluded from lucrative markets. And the United States could find that it may have to adapt its own privacy laws in order to conform to the new global standard, at least among free-market democracies. US civil liberties advocates see digital privacy as a growing issue in the United States, and the European experience may be relevant here. Meantime, American

companies will need to abide by Europe's judgments or find themselves hit with huge penalties that will hurt their reputation and ultimately erode their market presence there.

Some countries are taking even stricter measures to shield their citizens from growing abuses in the internet age. In Germany, where privacy fears are particularly acute because of repressive surveillance practices by the Nazi and Communist regimes, the federal parliament has passed legislation making social media companies responsible for eliminating objectionable content that is posted online. As of October 1, 2017, companies like Facebook and Google can be subject to penalties up to fifty million euros ($57 million) if they fail to delete within twenty-four hours any material construed to be hate speech, libel, terrorist propaganda, or other content deemed as "clearly illegal" by German authorities.

The new German law was approved months ahead of the September 24, 2017, federal elections, just as the anti-immigrant Alternative for Germany party had surged to more than 15 percent support—well above the threshold to qualify for seats in the federal parliament. A spate of xenophobic threats against immigrants carried on right-wing websites was believed to have encouraged hostile acts that included burning down housing for refugees. In addition, German authorities detected a sharp increase in online terrorist recruitment sites, which they feared could radicalize some of the more than one million refugees, many of them young Arab males from Syria and Iraq who have settled in Germany since 2015.

German police warned that an increasing number of false online reports were inciting hostile acts against immigrants. A Breitbart News report carried on the German internet claimed more than one thousand young immigrants had attacked police in Dortmund, waving Islamic State and al-Qaeda flags and setting fire to Germany's oldest church. In fact, a few men had simply set off firecrackers to celebrate New Year's Eve, there were no attacks on police, and a small fire on a piece of scaffolding had been quickly extinguished.[8]

Social media companies and civil rights groups claimed the new German law could suppress freedom of speech and be exploited by authoritarian regimes to justify their crackdowns on political opponents.

It could also stifle innovation to such an extent that many companies may question whether the risks of litigation or huge fines are worth the effort of doing business in Europe.

Anders Ansip, a former prime minister of Estonia who now serves as the EU's digital affairs chief, says the growing plague of fake news and its impact on elections in Western democracies drove the European Union to take action that would compel social media companies to assume greater responsibility in policing the internet. He denies that Europe's governments are engaging in de facto censorship of online content by threatening to inflict heavy penalties against companies that do not take active measures.

As somebody who grew up under communism, Ansip said that while some limits are necessary, he has no desire to see Orwellian media controls imposed on digital technologies introduced in Europe. "Fake news is bad but the ministry of truth is even worse," he said.[9]

A trendy new discussion is that this is the new Gilded Age and one has to "break up the Carnegie Steel Corporation." This is the wrong analogy. . . . Breaking up Google or Facebook would be a futile endeavor because as network economics predicts, these are pretty natural monopolies that have emerged. The real issue is that if social network platforms have become broadcast networks or publishers or giant media groups, they need to be regulated as such.

—Niall Ferguson

Disinformation, Cyberattacks, and Election Meddling

The revelations that Russia was involved in multiple efforts to influence the 2016 American presidential election in favor of Donald Trump came as no surprise to many Europeans. Indeed, despite the intense spotlight focused on Russia's interference in the 2016 US presidential

election, Europe has become arguably the world's most active battleground in modern cyberwarfare. Since 2014, many European governments, including Germany, France, Latvia, Estonia, Sweden, and Montenegro, have been subjected to waves of mysterious cyberattacks and malicious falsehoods spread through the internet by what is presumed to be a Russia-directed onslaught.

Last January, a report released by US intelligence agencies confirmed what many people across the continent already assumed: Russia was actively seeking to influence elections across Europe, in what appears to be a much larger strategy of Russian covert actions designed to destabilize Western democracies. At the Munich Security Conference a month later, Russian foreign minister Sergey Lavrov, while denying any interference in US or European elections, spelled out Russia's ambitions to create conditions for what he described as "a post-Western era."

Russia's blueprint for a cyberwarfare strategy against the West was first outlined in a 2013 article in a professional military journal by General Valery Gerasimov, chief of staff for Russia's General Staff and a close adviser to President Vladimir Putin. Gerasimov claimed the huge military superiority of the United States could be effectively countered in cyberspace, which he said "opens wide asymmetrical possibilities for reducing the fighting potential of the enemy."[10]

He said Russia should learn lessons from the Arab Spring, when social media played a key role in mobilizing protests that brought down several entrenched dictatorships across North Africa and the Middle East. "We witnessed the use of technologies for influencing state structures and the population with the help of information networks," Gerasimov wrote. "It is necessary to perfect activities in the information space, including the defense of our own objects."

Gerasimov emphasized that Russia's military services needed to hone their hacking skills to serve as a surreptitious extension of conventional warfare and political conflict. He suggested that the use of disinformation, hacking, and deception through social media channels would be a way "to fight a war without fighting a war" against the West. Since the

article appeared, Russia has greatly accelerated its political warfare campaign against Western democracies.

Last February, Russian defense minister Sergei Shoigu confirmed the existence of "information troops" that had long been denied by Moscow. "Propaganda must be smart, literate, and effective," Shoigu told Russia's lower house of parliament. According to the *Kommersant* business newspaper, Russia's military devotes about $300 million a year to a "cyber army" of about one thousand highly trained hackers. At their Warsaw summit in July 2016, NATO leaders adopted a Cyber Defense Pledge and vowed to make a top priority of protecting their digital networks and infrastructure. Since then, Britain has announced it would invest more than $2 billion in a national cybersecurity program and France has dedicated more than $1 billion to upgrading its cyberdefenses.

While Russia has engaged in spreading propaganda for decades, its intelligence services have greatly escalated their conflict with the West within the past three years by deploying the tools of digital technology in the ways that Gerasimov proposed. Kremlin specialists say Moscow's cyberoffensive against the West was likely triggered by the Maidan revolution in Ukraine, which Putin viewed as a Western-orchestrated effort that posed a direct threat to his own regime.

One of Russia's most important priorities has been Germany. Chancellor Merkel's staunch criticism of Russia's annexation of Crimea and its armed support for separatists in eastern Ukraine as well as her dominant leadership role in rallying support across Europe for sanctions against Moscow have made her government a primary target for cyberdestabilization efforts.

In December 2016, the German government informed the federal parliament, or Bundestag, that computer networks were being struck at least once a week by foreign intelligence services, mostly Russian. The Interior Ministry said in its annual report on security threats that "it is assumed that Russian state agencies are trying to influence parties, politicians and public opinion, with a particular eye to the [September 24] 2017 election."

Hans-Georg Maassen, the head of Germany's domestic intelligence service, said the intention might be "to damage trust in and the functioning of our democracy so our government should have domestic political difficulties and not be as free to act in its foreign policy as it is today."[11] He said it was initially assumed that Russia wanted to help Donald Trump in the US presidential election and that the cyberattacks were now seen as having "damaged American democracy."

Maassen said his agency was convinced that Russia would escalate its intrusions over the course of Germany's election campaign. He said a massive theft of electronic data from the Bundestag occurred during a 2015 cyberattack and that material might be released via WikiLeaks or other conduits before the September election. German officials believe the operation was carried out by the Russian hack group APT 28, also known as Pawn Storm, Fancy Bear, Sofacy, or Strontium. The hackers are believed to be controlled by Russia's military intelligence arm, or GRU.

The Russian government denies any connection to the hackers, but experts say there are hundreds of past incidents and suspicious connections that point to Russia. APT—for advanced persistent threat—was first identified by the global cybersecurity company FireEye. APT 28 has developed masterful "phishing" methods, using sophisticated fake emails with realistic but infected attachments that implant malware in foreign networks and can provide access to classified or sensitive materials.[12] These tools were used in the hacking of the emails of the Democratic National Committee ahead of the American presidential election in 2016. German officials claim that sensitive documents on US-German intelligence cooperation, presumably obtained through the Bundestag hack, were also published on WikiLeaks.

German security officials say the cyberattack on the Bundestag, which targeted the parliament's intelligence control committee, triggered the creation of a new cyberprotection department with more than ten thousand operatives to be run out of the defense ministry. Merkel also ordered a complete overhaul of the parliament's computer systems and deployed more sophisticated defenses to thwart any future

cyberattacks aimed at sabotaging government institutions or key utilities such as power plants.[13]

Merkel's government was outraged by Russia's manipulation of the so-called Lisa case in 2016, when reports circulated about a thirteen-year-old Russian-German girl named Lisa who had been missing for two days and was allegedly raped by three refugees. The German police quickly learned the girl had not been raped and was merely staying with friends. But pro-Russian media sites kept insisting the girl had been raped by refugees, stirring up right-wing protests in Germany against the influx of Syrian refugees. Russia's foreign minister even accused Merkel of staging a cover-up of the truth.

The chancellor knows Russia will continue to deploy its arsenal of social media weapons to exploit the West's democratic traditions like freedom of expression, in contrast to the suppression of dissent in Russia and other autocracies. Again, this is nothing new. In the 1980s, Soviet disinformation efforts designed to split the Western alliance sought to persuade Europeans that the CIA was responsible for inventing the AIDS virus as part of an American biological weapons program.

Besides the loss of sensitive data and manipulation of fake news, the German government believes new dangers include the planting of delayed-action malware that could trigger "silent, ticking digital time bombs" in government computers and the nation's critical infrastructure. "This now belongs to normal daily life. . . . We must learn how to manage this," Merkel said in ordering the complete overhaul of government computers. She also insisted that industry help devise more effective ways to prevent sabotage of power plants, electrical grids, and other key parts of the national infrastructure.

Germany is not alone in Europe in finding its political process under attack through new digital technologies. Social media has helped make extremist candidates and causes seem more plausible, and not just in the United States, where Trump's victory took pundits by surprise. In the Philippines, Rodrigo Duterte cultivated a vast army of online supporters to help him win the presidency even though the crude, tough-

talking mayor was heavily outspent by his mainstream opponents. In Britain, the once unlikely cause of leaving the European Union won an outright majority of votes in the June 2016 referendum thanks to an effective mobilization of supporters on Facebook and other forms of social media.

Russia has consistently sought to exploit extremist groups on the right and left to destabilize Western democracies. Moscow is finding stronger resonance for its support of extremist messages in European politics, in part because of the expanding impact of social media. In Hungary, the once-marginal far-right extremist group Jobbik has emerged as the leading opposition party, forcing conservative Prime Minister Viktor Orban to move sharply to the right. Both Jobbik and Orban's ruling Fidesz party have cultivated close ties with Putin's Russia, causing consternation among NATO allies.

This year, Russia acquired control of a far-right website in Hungary called Hidfo, or The Bridgehead, that now operates from a server in Russia and provides a platform for Russian disinformation. Orban, who has befriended Putin and shares his scorn for liberal democracy, also accepted Moscow's offer of a $10 billion loan for Hungary to pay for construction by Russia of a nuclear power plant. Elsewhere, Russia has tried to disrupt the normal functions of democracy in Scandinavia by nurturing far-right groups such as Nordic Resistance, which has formed an alliance with the Russian Imperial Movement.[14]

In Central and Eastern Europe, Russia's ambition to secure political control of its periphery by exercising greater influence through the acquisition of local radio and television stations, newspapers, and social media sites recently helped elect pro-Moscow candidates in presidential elections held in Bulgaria and Moldova. Just months after joining NATO, Montenegro's government was besieged by a wave of cyber-attacks, presumably as a consequence of becoming a member of the Western military alliance against Moscow's wishes. The attacks came after twenty people, including two Russians, were arrested and charged with planning a coup.

But Russia's most important priorities appear to be centered on the larger countries in Europe. Besides Germany, Moscow has been particularly active in Italy and France. In Italy, where Putin once enjoyed a close friendship with billionaire former prime minister Silvio Berlusconi, Russia has sought to build ties with the anti-immigrant Northern League, which strongly opposes sanctions against Russia and whose leader, Matteo Salvini, has paid numerous visits to Moscow.

Russia is also courting Italy's populist Five Star Movement, which was launched less than a decade ago as an online movement to promote transparency in government. It is now leading in polls as the country's most popular party with about 30 percent support and aspires to head the next government after national elections are held, probably in early 2018.

The Five Star Movement was cofounded in 2009 by the comedian Beppe Grillo and the internet publishing entrepreneur Gianroberto Casaleggio, who died of a brain tumor in 2016. They have attracted a lot of support from Italian voters disillusioned with government corruption by promising that major policies and programs will be subject to public approval through online referendums. Five Star describes frequent online votes as its preferred format for ensuring transparent democracy and direct citizen participation in government. Casaleggio's son, Davide, who has inherited his father's internet business, has further honed the movement's use of online tools to raise funds and recruit candidates for public office.

Part of Five Star's appeal is to engage people directly through its online tools in proposing and drafting legislation. Despite the movement's naïve populism, Five Star has capitalized on a new desire in Italy for greater citizen empowerment as a way to help bridge the gap of distrust that evolved between political parties and the citizens they aspire to help. In that sense, they have become the country's leading political party because they are perceived as a fresh hope of restoring democracy.

Casaleggio's company also controls several popular websites that often publish sensational and distorted reports found on Sputnik Italia, an Italian version of the Kremlin-backed website that espouses Putin's

views on the world. Luigi di Maio, a likely prime minister if Five Star wins the next elections, rejects sympathy with Moscow and says the movement is aligned with neither Russia nor the United States. But some Five Star members of parliament back Italy's departure from NATO and endorse Moscow's views on issues like the Syrian civil war.[15]

Russia was also deeply involved in meddling with France's 2017 presidential election campaign, seeking to bolster support in favor of the right-wing National Front candidate, Marine Le Pen. The First Czech Russian Bank, now in bankruptcy, loaned about $10 million to Le Pen's party, and Putin met with her in Moscow during the campaign to burnish her foreign policy credentials. She, in turn, has advocated the lifting of all sanctions against Russia and promised to pursue a new policy of greater Western cooperation with the Kremlin.

Moscow tried repeatedly to sabotage the candidacy of Emmanuel Macron and his *En Marche!* political movement by spreading rumors that Macron was a closet homosexual and "an agent of the big American banking system" because of his past employment as an investment banker with Rothschild. Macron's campaign websites and computer networks were targeted frequently in the months ahead of the presidential election, with hundreds if not thousands of attacks coming from hackers believed to be located in Russia, according to Richard Ferrand, the national secretary of Macron's party.

On the eve of the French presidential election, Macron's campaign staff members discovered they had been struck again, this time by a massive and coordinated operation unlike any of the others. The digital attack involved a dump of campaign documents including emails and accounting records in the hours just before a legal prohibition on campaign communications went into effect.[16] Macron's digital campaign director, Mounir Mahjoubi, told journalists the hackers had mixed fake documents with authentic ones "to sow doubt and misinformation." He said the operation, coming just before France's most consequential election campaign in decades, was "clearly a matter of democratic destabilization, as was seen in the United States during the last presidential campaign."

> *How can government structures and decision-makers take advantage in a big data era of decision-support mechanisms that are provided by technology such as AI? How do we bring into the governance process the exploitation of these new capabilities? That's something that I think governments don't do very well today.* —Christopher Stubbs

What Can the West Do to Thwart Cyberattacks?

Shortly after his election, President Macron welcomed Putin to a huge cultural exhibition held in Versailles celebrating French-Russian relations. During a joint press conference, with an uncomfortable Putin at his side, Macron described RT and Sputnik as "agents of influence which on several occasions spread fake news about me personally and my campaign through lies and propaganda." He noted with evident satisfaction that Russia's disinformation efforts had proved in vain, as he won a convincing 67 percent of the vote in the final round against Le Pen.

RT and Sputnik had repeatedly released false voter surveys during the campaign, claiming Macron was running well behind Le Pen and Francois Fillon, the former conservative prime minister who had also cultivated friendly relations with Putin. Mahjoubi told journalists the main objectives of Russia's state-funded media outlets were to foment uncertainty about the election and spread chaos as a way of diverting attention from Fillon's legal problems. Fillon was the one-time favorite in the presidential race, but his standing plummeted when he became embroiled in a corruption investigation after putting his wife and children on the parliamentary payroll for doing little or no work.

Mahjoubi believes the principal reason that Russian attempts failed to disrupt the French election was because the campaign had made meticulous preparations to defend against potential cyberattacks. Macron's campaign team and French government authorities had anticipated a

Russian onslaught, not just because of what they saw occur during the US presidential campaign. In 2015, a massive cyberattack nearly shut down the world's largest francophone broadcaster, TV5Monde. Only a last-minute intervention by a TV technician, who ripped wires from a targeted server, prevented the collapse of the network. The hackers sent false messages to make it appear that the Islamic State was behind the attack, but French technicians later traced its origins to APT 28, or Fancy Bear, which turned out to be the same address that carried out attacks against the Democratic National Committee in 2016.

The fact that Macron's team and French authorities had drawn lessons from previous attacks and were bracing for a fresh wave of cyberassaults clearly helped mitigate the damage. As early as October 2016, the French national cybersecurity agency summoned all political parties involved in the campaign to raise their awareness about the risks of manipulation and outside interference that could impinge on national sovereignty in such a high-stakes election. In the months before the May 2017 election, France's defense ministry created a cyber command center composed of 2,600 experts knowledgeable in the ways of repulsing hack attacks. France's painstaking defenses clearly paid off.

France's success in blocking Russia's hacking operations—aided by French laws that prohibited the media from disseminating information in the final forty-eight hours before the election—showed that while open, democratic societies may be vulnerable, they are not helpless in thwarting such attacks. An open society can encourage its public to be alert and informed about the nature and intentions of forces seeking to disrupt the proper functioning of democratic processes, like free elections. While the murky nature of cyberoperations makes it difficult to trace the identity of actual culprits, there are hopeful signs that Western countries may be able to develop a more effective shield against channels of information warfare.

Over the past decade, the Estonian government has developed some of the world's most advanced and sophisticated defenses in countering cyberattacks. In 2007, the small Baltic nation of 1.3 million people was

overwhelmed by a spate of cyberattacks, believed to originate in Russia, that nearly crippled its banking system and digital infrastructure. The websites of leading newspapers, political parties, and government ministries were also disabled. The attacks came shortly after Estonia removed a Soviet-era memorial to World War II from the center of its capital.

In early 2017, NATO Secretary General Jens Stoltenberg declared that Western alliance networks were being subjected to an average of five hundred attacks a month, up 60 percent from the previous year. While the Russian government consistently denies meddling in foreign elections and waging cyberattacks against the West, many of the intrusions are believed by NATO intelligence experts to have been conducted by Russian hackers operating with tacit, if not active, support from Moscow.

Since the 2007 attacks, Estonia has transformed itself into a highly valued Western ally that has erected NATO's most advanced cybersecurity defenses.[17] A recent alliance joint exercise called Locked Shields 2017 took place in the Estonian capital of Tallinn with nine hundred security experts from across Europe and the United States. They were challenged to defend against simulated attacks such as hackers breaking into an air base's fueling system and fake news reports accusing NATO of developing drones with chemical weapons.

Estonia has encouraged direct involvement by the private sector in helping fortify the nation's cybersecurity defenses. Under former president Toomas Hendrik Ilves, Estonia set up a program that enlisted volunteers who donate their free time, much like a national guard, to learning how to protect the nation's digital infrastructure, including everything from online banking to electronic voting systems. The program has already been emulated in neighboring Latvia. In the United States, the state of Maryland is consulting with Estonia about setting up a cyberdefense unit within its own national guard.

Despite such efforts, Russia-directed hacking threats continue to escalate in both Estonia and Latvia, the two Baltic nations that feel most

highly exposed to such intrusions, in part because they have large ethnic Russian populations. Early this year, Marko Mihkelson, chairman of the Estonian parliamentary foreign affairs committee, received a suspicious email, allegedly from NATO, offering a link to an analysis of a North Korean missile launch. He did not click on the link but alerted some of Estonia's top cyberexperts. They found, yet again, that the message contained the same malware as that used against the Democratic National Committee during last year's presidential campaign by APT 28, alias Fancy Bear.

Developing better defenses and making Russia aware that further attacks traced back to Moscow will result in serious damage to relations with the West may be the best formula for an immediate, effective Western deterrent. When Merkel met with Putin and demanded that he personally halt Moscow's campaign of falsehoods in the Lisa case or face further escalation of economic sanctions and permanent damage to Russia's relations with Germany, Putin finally backed off. Since Merkel's direct warning to Putin, Russia has ceased making inflammatory comments about the Lisa case.

And when the United States challenged China about its cyberespionage efforts in 2008, China deflected blame and insisted it had done nothing wrong. Later, as Western defenses became stronger, China realized an escalating crisis with the West and the likelihood of economic sanctions were not worth the risk of conducting further cyberattacks for military or commercial purposes.[18] The prospect of diminishing returns and growing costs persuaded Chinese president Xi Jinping to agree to halt Chinese commercial cyberespionage, first against the United States and then against the United Kingdom and all G20 nations.

These examples suggest that the shield of stronger defenses and the stick of harsh sanctions can help contain the danger of cyberattacks spinning out of control. Even if Russia persists in its belligerent attitude toward the West and its aggressive efforts to destabilize its neighbors, a combination of smarter and stronger Western cyberdefenses along with

punitive retaliatory measures may form the most effective basis for deterrence in a new age of hybrid warfare.

The Chinese story on cyber industrial espionage is the one that gives me hope too because they really did go from being the poachers to being gamekeepers. They started to understand, "Hey, we have IP. We're starting to innovate. This stuff is going to start hurting us." —Niall Ferguson

---