The Unhackable Election

What It Takes to Defend Democracy

Michael Chertoff and Anders Fogh Rasmussen

Russia's invasion of Ukraine in 2014 marked a sharp break with the past: the post–Cold War interlude, a time when peace and democracy spread across the globe, was over, and a new, more aggressive era, had begun. Since then, Western governments have had to relearn the forgotten art of deterring attacks and protecting their countries' borders. They have failed to see, however, that the attacks can also be aimed at their democratic institutions. Liberal democracy may remain the world's preferred model of governance, but it is under debilitating pressure from threats both internal and external.

A poll released by Dalia Research in 2018 highlighted just how much citizens of democracies have lost faith in their governments. Sixty-four percent of respondents living in democracies said their governments rarely or never act in the public interest, whereas only 41 percent of those in autocracies said the same. Politicians in democracies are partly to blame: there is more than a grain of truth to the view that they have ignored concerns about such issues as living standards and immigration and that they often say one thing and do another.

But malign foreign powers—led by Russia—have worsened the problem, by weaponizing the infrastructure that underpins democratic societies. They have hacked the Internet, media, and even voting databases to sow discombobulation, discontent, and disunity. From the 2016 Brexit referendum, to the 2016 U.S. presidential primaries and general election, to the 2017 French presidential election, foreign meddlers have systematically sought to skew the democratic debate.

MICHAEL CHERTOFF is Co-Founder and Executive Chair of the Chertoff Group. He was U.S. Secretary of Homeland Security from 2005 to 2009.

ANDERS FOGH RASMUSSEN is Founder and Co-Chair of the Alliance of Democracies Foundation. He was Prime Minister of Denmark from 2001 to 2009 and Secretary-General of NATO from 2009 to 2014.

They are Co-Chairs of the Transatlantic Commission on Election Integrity.

The Kremlin has been testing its interference playbook in countries throughout eastern Europe, and especially Ukraine, ever since those states escaped Soviet rule in the early 1990s. Only in recent years has it begun following that playbook in western Europe and the United States. The attacks are an assault on every citizen's fundamental right to elect his or her own representatives. Yet even though democracies on both sides of the Atlantic have been targeted, their responses have lacked urgency and coordination. Meddlers have sought to undermine mainstream political parties on both the left and the right, but the question of what to do about this interference remains a partisan issue, especially in the United Kingdom and the United States. Meanwhile, governments and technology companies keep talking past each other, with the former preferring overzealous state edicts and the latter inadequate self-regulation.

In the next two years, more than 20 elections will take place across Europe and North America. Many of them will offer voters a stark choice between candidates who support openness and multilateralism and those who advocate isolationism, populism, and nationalism. Russia and other autocratic regimes have a clear stake in these elections, and there is every indication that they will continue to interfere in them. Individual countries and political campaigns can do more to protect themselves, but ultimately, a collective effort to defend democratic institutions is necessary—a bipartisan, transatlantic response to foreign meddling. Countries must work together to undertake broad assessments of the vulnerabilities of their electoral systems. Foreign governments and civil society groups should provide direct support to help protect countries that are particularly vulnerable to foreign meddling, such as Ukraine. Policymakers should collaborate with technology companies to give citizens the tools they need to inoculate themselves against false information. And politicians, finally, should work to address the root causes of the societal cleavages that Russia and other malign actors are trying to exploit.

THE NEW INFORMATION WARFARE

Foreign meddling in elections is not a new phenomenon. During the Cold War, both superpowers relied heavily on information warfare. The Kremlin spread false conspiracy theories claiming, for example, that the CIA was the source of HIV, the virus that causes AIDS, and that it assassinated U.S. President John F. Kennedy. The United States and the United Kingdom both developed sophisticated intelligence campaigns to spread anticommunist propaganda in Chile, Haiti, Italy, and elsewhere.

The fall of communism led many Western countries to believe that Russian interference had been consigned to history. But in the past several years, the Kremlin—faced with an expanding democratic world and Russia's diminishing status as a global power—has dusted off its old playbook and wielded its strategies against the source of the Western world's strength: its unity.

The new Russian meddling combines tried-and-true methods with modern technology. Some tactics are familiar from the Soviet era: supporting factions sympathetic to Russia's interests, promoting media outlets that peddle fake news, sponsoring coups, stirring up diaspora communities. But now, the Kremlin has new tools for manipulating social media, such as armies of robotic accounts and paid trolls. Because the Internet and automation enable aggressors to act anonymously on a large scale, technology has significantly reduced the costs and risks of election meddling.

The scope of Russia's social media disinformation campaigns is staggering.

Adding to the difficulties of preventing interference, foreign meddling operations tend to be carried out in an operational gray zone. This makes it hard to attribute responsibility to one specific government agency. In Russia, the military intelligence agency (GRU) is responsible for both human intelligence, which includes information gathering and carrying out physical missions, and digital spying, which includes fabricating websites. Meanwhile, hacking collectives and criminal networks, such as Fancy Bear, or APT28, actually develop and deploy the malware used in election meddling. There are some links between the intelligence agencies and the hacking collectives, but their exact nature remains unclear.

The scope of Russia's social media disinformation campaigns is staggering. In the lead-up to the Italian election in March 2018, bots were responsible for 15 percent of Twitter activity promoting far-right candidates. Fake Twitter accounts generated 30 percent of the tweets and retweets about the August 2018 assassination of Alexander Zakharchenko, a pro-Russian rebel leader in Ukraine. In Macedonia, there was a surge in new accounts about 40 days before the September 2018 referendum on whether to change the country's name, a move that Russia opposed because it would ease the way for Macedonia to join NATO. Automated accounts mostly encouraged voters to boycott the referendum, suggesting that they were part of a Russian-sponsored voter suppression effort. Similar spikes in bot activity occurred in the lead-up to elections in Sweden in September and Bosnia and Herzegovina in October.

In some cases, foreign meddlers have tried to directly boost whichever candidate or party was most likely to adopt a soft stance on Russia. However, in most cases, their strategy is simply to discredit the entire democratic process. In the 2016 U.S. presidential primaries, for example, Russian operatives supported both the Republican candidate Donald Trump and the Democratic candidate Bernie Sanders, with the goal of radicalizing the political debate.

Election meddling can have unintended consequences. In France, hackers' repeated efforts to thwart French President Emmanuel Macron's campaign undoubtedly hardened his stance toward Moscow. In the United States, meddling in the 2016 election caused Congress to strong-arm the Trump administration into adopting a more aggressive posture toward Russia, including providing Javelin antitank missiles to Ukraine, introducing new sanctions against Russia, and increasing funding for U.S. troops in Europe.

But there is growing evidence that other states are gravitating toward Russia's high-impact, low-cost strategy. In Mexico, two weeks before the country's July 2018 presidential election, there was a surge in bot accounts on Twitter sharing stories that cast doubt about the presidential candidate Andrés Manuel Lopéz Obrador's grasp of economics and spreading news that his opponents had already lost. The majority of the news sources shared by these bots originated not in Mexico but in Argentina, Iran, and Venezuela (as well as Russia). In August, John Bolton, the U.S. national security adviser, announced that there was a "sufficient national security concern about Chinese meddling, Iranian meddling, and North Korean meddling" and said that the U.S. government was working to crack down on it. That same month, Twitter suspended 284 fake accounts with apparent links to Iran, and Facebook discovered 76 fake Instagram accounts originating in Iran. The discourse surrounding the Catalan independence referendum in 2017 saw an unprecedented level of trolling on social media and spreading of distorted facts, all originating in Venezuela. A study by the scholar Javier Lesaca showed that Venezuela likely allowed

Russia to operate its disinformation campaign against the referendum using Venezuelan networks.

For now, foreign meddling operations remain largely the preserve of state actors and their proxies, but other actors will enter the fray in the near future as new technology and artificial intelligence lower the barriers to entry. So-called deepfake videos or audio files—artificial video or audio material generated by an algorithm rather than a video production team—are fast becoming the new frontier in information manipulation. Right now, producing deepfakes requires sophisticated video-editing skills and software and a convincing voice actor. But within a few years, new technologies could enable a programmer to feed a computer a public figure's speeches to synthesize voice patterns and create a convincing fake video. According to a test carried out by ASI Data Science, using two hours of recordings over five days of work, an algorithm could produce a credible audio file of Trump declaring nuclear war against Russia. The prospect is chilling: a teenager in his bedroom could force the world's most powerful individuals to say anything he wants.

A WEAK RESPONSE

Given the scale of the threat posed by foreign meddling, the response of the transatlantic community has been woeful. In the United States and Italy, denial at the highest levels of government has impeded progress. Trump has spent considerable energy denying any interference in the 2016 U.S. presidential election out of fear that recognition of Russian meddling in his favor may be interpreted as a tacit admission of collusion between Russia and his campaign team. Italy's Matteo Salvini, the deputy prime minister and head of the governing right-wing party, Lega Nord (Northern League), has similarly denied Russian meddling in Italy's March 2018 election or fundraising for Lega Nord. In the case of Salvini, his publicly avowed appreciation for Russia has stymied any progress in fortifying Italy's electoral infrastructure. Across Europe, leaders have approached the challenge through the outdated and simplistic 2016 lens of fake news. When they have taken action, their efforts have been uncoordinated and often geared toward fighting the last pattern of interference rather than the next one.

The result is a patchwork of remedies that have either come up short or been overzealous. Although progress has been made, leaders in the United States, for their part, made insufficient preparations to protect November's midterm elections. As of October, eight election-related bills, many of them bipartisan, were still languishing in Congress. Inadequate electoral infrastructure is also a problem: decentralized voting systems preclude uniform security measures, leaving them more vulnerable to manipulation or attack. For example, the electronic voting systems in some U.S. states could be easily infected with malware simply by someone inserting a USB drive into a voting machine, thereby enabling attackers to stuff virtual ballot boxes. Local officials' resistance to what they perceive as federal interference in their states hampers uniform planning.

The European response has also been patchy. The EU's team tasked with countering propaganda and disinformation in eastern Europe is limited by its miserly budget of $1.3 million per year. The European Commission (the EU's executive body) has proposed a code of conduct for social media platforms that would commit them to taking prescribed action to fight fake news and has required EU-funded, pan-European political parties to follow a common set of practices designed to protect against interference. Some member states have taken individual measures: the United Kingdom created a national security unit to combat fake news; France banned electronic voting for citizens living abroad; the Netherlands banned it entirely; and the Czech Republic, Ireland, and Sweden are considering legislation to fight fake news. Others may have gone too far, ending up curbing freedom of speech: France and Germany have passed legislation that civil society and the media have criticized as overzealous. In typical EU fashion, each country has taken its own piecemeal actions and failed to coordinate with its allies.

Meanwhile, lawmakers have criticized technology companies for their inaction and de facto complicity in spreading highly partisan narratives and outright fake news. Some companies have now begun to accept responsibility for reducing the amount of disinformation on their platforms. In April 2018, Microsoft launched the Defending Democracy Program in order to prevent hacking, increase advertising transparency online, and explore technological solutions to protect elections and identify cyberattacks.

In response to significant pressure from lawmakers and the public, Facebook, Google, and Twitter have also stepped up their efforts to police their platforms. They have made some progress, removing more fake accounts, taking more domains offline, and thwarting more hacking efforts. Yet these efforts remain largely voluntary. Protective of their business models, these companies are releasing too little information about the extent of the problem, such as the number of fake accounts. Furthermore, politicians' lack of understanding about how technology platforms work impedes collaboration with the private sector. Earlier this year, for example, Mark Zuckerberg, the CEO of Facebook, appeared before the U.S. Congress for a hearing on Facebook's treatment of user data. At the hearing, senators asked Zuckerberg simplistic questions about Facebook's business model instead of diving deep into the company's sophisticated data practices, revealing the limits of their understanding of the technology.

The advent of artificial intelligence offers an array of possible solutions to the threats posed by meddling. Machines are able to scan the Internet more accurately and faster than humans, processing and synthesizing macro-level patterns in a way humans cannot. But without cooperation between politicians and entrepreneurs to enact laws and build security measures into such software, new technologies themselves will remain vulnerable. This could exacerbate the challenges that new technologies pose rather than solve them.

SAFEGUARDING DEMOCRACY

With the future of democracy in the United States and Europe at stake, it's time to start developing a more forward-thinking strategy for dealing with foreign interference. Prevention starts with political campaigns themselves. As they head into election season, they must understand that foreign meddlers are systematically targeting them through phishing attacks (fraudulent attempts to obtain sensitive information by impersonating a trusted entity) and server hacks. All it takes to bring down an entire campaign is a single employee clicking on one malicious link. Smart cyberdefense is as critical to today's political parties as clever campaign slogans and billboards.

But individual countries, let alone parties and organizations, can do only so much to protect themselves. What is required is a collective, bipartisan, transatlantic response to foreign meddling. This is why, in June 2018, we brought together leaders from politics, media, academia, and business from a cross section of parties and backgrounds on both sides of the Atlantic to create the Transatlantic Commission on Election Integrity. The aim is to bridge the gaps that have so far prevented a collective response to election meddling and to avoid relitigating past elections and instead focus on future ones.

Transatlantic cooperation will be central to this effort. At the June 2018 G-7 meeting in Quebec, leaders took an important first step in agreeing to better coordinate national efforts to fight election meddling. But the commitment to this fight remains limited, and the concern, too low on the priority list of transatlantic business. At a meeting cohosted by the Atlantic Council and the Transatlantic Commission in mid-July, we brought together a bipartisan group of U.S. senators from the Senate Intelligence Committee and a dozen European parliamentarians in an attempt to broaden the scope of cooperation. For the first time, U.S. and European lawmakers shared their assessments of the threat and agreed on a series of far-reaching recommendations, including more government contingency planning, new legislation with immediate sanctions for meddlers, and more state funding for countering interference. These recommendations would bring together diverse parties, including civil society and technology companies, to monitor and report on activities that spread disinformation and to promote the sharing of best practices among governments.

Too many governments are either still in denial or don't fully understand the extent of the threat posed by election meddling.

Too many governments are either still in denial or don't fully understand the extent of the threat posed by election meddling. Most have a surprisingly vague sense of the vulnerabilities of their own democratic infrastructure. National intelligence agencies may be better positioned than governments to assess and follow the threats, but their findings do not reach the rest of government or civil society and political parties. To help fill these gaps, the Transatlantic Commission will conduct national assessments of democracies with critical upcoming elections. These assessments will analyze different factors related to elections and democratic processes in each country, including legislation, the vulnerability of cyberspace and social media platforms, and the presence of anti-Western groups within the country that might be looking to influence or disrupt the election. The purpose of these assessments is not to embarrass governments or fuel opposition parties but to help prevent foreign powers from exploiting weaknesses.

Some countries in eastern Europe are particularly vulnerable to foreign meddling and require more active support, from both other governments and civil society. Take Ukraine. Its presidential and parliamentary elections scheduled for 2019 will be critical for a country that is in the midst of its biggest political transformation since it achieved independence in 1991. This point is surely not lost on Moscow, which is almost certain to take all possible measures to undermine the validity of the elections and skew their results. The Transatlantic Commission is thus working with a group of experts to monitor and actively report interference activities in the lead-up to Ukraine's election.

The commission is also seeking to bridge the gap between the public and private sectors. We have deployed technological tools to monitor real-time disinformation, tracking the number of bot accounts created on social media, the messages they are disseminating, and their country of origin. With these insights, political leaders and civil society can fight back against disinformation campaigns more effectively. One of the best ways to defend against meddling is for citizens to inoculate themselves against disinformation. To help with that effort, the Transatlantic Commission is partnering with companies such as ASI Data Science to develop an algorithm that can distinguish deepfakes from real videos, allowing citizens to identify machine-generated content.

All these efforts should help prevent adversaries from exploiting the cleavages that exist in democratic societies. But it is important to remember that although Kremlin-sponsored interference may help populist parties, it does not create them. Populism is typically a symptom of a failing political system, not its cause. The greatest challenge for mainstream politicians, then, is to tackle societal cleavages at their source by addressing the issues that drive antipathy toward mainstream parties.

Across Europe and North America, democracy is being hacked. Citizens and governments can either sit back and accept foreign meddling in elections as an uncomfortable side effect of the digital age or they can safeguard their electoral systems. If history has taught anything, it is that individual countries cannot face such challenges alone. The goal of election meddling is to sow confusion and fear, which, in turn, drive support for candidates and parties that break down the alliances and undermine the values that have kept the West free, prosperous, and relatively peaceful for 70 years. Unless the transatlantic community stands together, malign foreign powers will continue to pick off democracies one by one. This is not hyperbole; it is already the reality.