H-Diplo | ISSF

POLICY Series
America and the World—2017 and Beyond

Beyond Cyber-Threats: The Technopolitics of Vulnerability

Essay by **Rebecca Slayton**, Cornell University

Published on **4 April 2018** | issforum.org

Editor: Robert Jervis, Joshua Rovner, and Diane Labrosse
Web and Production Editor: George Fujii

Shortlink: http://tiny.cc/PR-1-5BC
Permalink: http://issforum.org/roundtables/policy/1-5BC-technopolitics
PDF URL: http://issforum.org/ISSF/PDF/Policy-Roundtable-1-5BC.pdf

Cyber-threats seem to be everywhere these days. In the past two weeks alone, we have learned that Russia has hacked into critical infrastructure sectors upon which citizens depend for daily survival, including nuclear, water, and aviation; that Iran has stolen massive amounts of data and intellectual property from professors around the world (such activities have previously been attributed primarily to China); and that the self-professed lone hacker who claimed to have provided stolen Democratic National Committee e-mails to Wikileaks, was actually working for the Russian military intelligence agency to meddle in electoral politics.[1] Finally, after months of concern about Russian disinformation and propaganda campaigns, new revelations about how big tech companies like Facebook furthered these efforts, have amplified profound questions about the future of representative governance, national sovereignty, and self-determination.

Facebook has already been under scrutiny for its role in selling advertising and otherwise enhancing the operations of Russian troll farms and bots, which aimed not only to undermine Hillary Clinton's presidential run, but more fundamentally to spread disinformation, polarize political discourse, and undermine confidence in U.S. institutions.[2] Now, documents provided by whistleblower Christopher Wylie show that

[1] On Russian penetration of critical infrastructure, see Brian Naylor, "Russia Hacked U.S. Power Grid—So What Will the Trump Administration Do About It?," *National Public Radio*, 23 March 2018, https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it. On Iran, see Tal Kopan, "US Disrupts 'Massive and Brazen' Iranian Hacking Scheme, Doj Says," *CNN*, 23 March 2018, https://www.cnn.com/2018/03/23/politics/iranian-hackers-indicted-universities-government/index.html. On the DNC hack, see Spencer Ackerman and Kevin Poulsen, "'Lone Dnc Hacker' Guccifer 2.0 Slipped up and Revealed He Was a Russian Intelligence Officer," *The Daily Beast*, 22 March 2018, https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer.

[2] Alicia Parlapiano and Jasmine C Lee, "The Propaganda Tools Used by Russians to Influence the 2016 Election," *New York Times*, 16 February 2018, https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-

Cambridge Analytica obtained data on 50 million Facebook users without their full consent.[3] Cambridge Analytica claims it "uses data to change audience behavior," and its chief executive has bragged that it did "all the research, all the data, all the analytics, all the targeting" to successfully elect Donald Trump as President of the United States.[4] Using social media to micro-target voters is not new; Barack Obama's presidential campaigns used similar methods.[5] But Cambridge Analytica has been accused of deception. Wylie states: "If you start to warp the perception of voters without their consent or knowledge, that is a fundamental denial of their agency and autonomy to make a free choice when they are voting."[6]

Understanding, preparing for, and responding to threats, whether they are private actors, corporations, or foreign governments, is a necessary part of any cybersecurity strategy. But as I will argue below, it has its limits. Meanwhile, there is a real risk of neglecting the vulnerabilities that make cyber operations so successful. Vulnerabilities are layered and embedded within complex technopolitical regimes—intertwined systems of artifacts, laws, organizations, people, and norms that tend to maintain particular power structures.[7] Sheer complexity makes some vulnerabilities impossible to predict. But other vulnerabilities are strategically ignored by those who benefit from leaving them in place. This essay is a brief attempt to excavate some of the vulnerabilities that are often ignored amid the focus on threat.

But first, consider efforts to deal directly with threats.

*Threats, everywhere***.**

---

propaganda-election-2016.html; Cecilia Kang, "Facebook Faces Growing Pressure over Data and Privacy Inquiries," *New York Times*, 20 March 2018, https://www.nytimes.com/2018/03/20/business/ftc-facebook-privacy-investigation.html.

[3] Carole Cadwalladr, "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower," *The Guardian*, 17 March 2018, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

[4] The company's logo can be found on its homepage: https://cambridgeanalytica.org/, accessed 28 March 2018. For CEO Alexander Nix's claims, see Michael Kranish, "Cambridge Analytica Ceo's Claim About Role in Trump's Campaign Raises Questions," *Washington Post*, 21 March 2018, https://www.washingtonpost.com/politics/cambridge-analytica-ceos-claim-about-ties-to-trumps-campaign-raises-questions/2018/03/21/81685c6a-2d1f-11e8-8688-e053ba58f1e4_story.html.

[5] Ed Pilkington and Amanda Michel, "Obama, Facebook and the Power of Friendship: The 2012 Data Election," *The Guardian*, 17 February 2012, https://www.theguardian.com/world/2012/feb/17/obama-digital-data-machine-facebook-election.

[6] BBC News, *'Cambridge Analytica Planted Fake News'*, podcast audio2018, 20 March 2018, http://www.bbc.com/news/av/world-43472347/cambridge-analytica-planted-fake-news.

[7] I borrow the concept of a technopolitical regime from Gabrielle Hecht, who defines it as ""linked sets of people, engineering and industrial practices, technological artifacts, political programs, and institutional ideologies, which act together to govern technological development and pursue technopolitics." Gabrielle Hecht, *The Radiance of France: Nuclear Power and National Identity after World War II* (Cambridge: MIT Press, 1998).

Facebook and Cambridge Analytica both blame Aleksandr Kogan, a Russian-born psychology professor at the University of Cambridge who helped design a personality quiz app in 2013. Roughly 300,000 Facebook users gave the app access to their data for academic research. But the app also took data from their Facebook friends' profiles—something that was then allowable under Facebook's privacy policy—so the data of over 50 million Facebook users, mostly on the voter rolls in the United States, was gathered. Moreover, Kogan allegedly sold that data to Cambridge Analytica, in violation of Facebook's policies and British data protection laws. Kogan has also been scrutinized because he is an associate professor at the University of St. Petersburg, where he has accepted Russian government grants on social media and delivered lectures on political communication.[8] Kogan laughs at the notion that he is a Russian operative, claims that the data he sold came from an app which allowed for commercial use, and that he is "being basically used as a scapegoat."[9]

Facebook and Cambridge Analytica claim they did not know that Kogan had violated policies, and took appropriate actions once he did. But neither is off the hook. Facebook changed its privacy policy in 2015, making it impossible to access friends' data without those friends' explicit consent.[10] Nonetheless, the Federal Trade Commission is investigating whether Facebook violated a 2011 agreement requiring Facebook to get explicit consent from users before gathering information that went beyond the privacy limits they have established.[11]

Meanwhile, Cambridge Analytica is under investigation in multiple countries for potentially illegal interference in their political processes.[12] In the United States, the company continues to draw scrutiny for

[8] Carole Cadwalladr and Emma Graham-Harrison, "Cambridge Analytica: Links to Moscow Oil Firm and St Petersburg University," *The Guardian*, 17 March 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-academic-trawling-facebook-had-links-to-russian-university.

[9] Elizabeth Dwoskin, Drew Harwell, and Craig Timberg, "Facebook Had a Closer Relationship Than It Disclosed with the Academic It Called a Liar," *Washington Post*, 22 March 2018, https://www.washingtonpost.com/business/economy/facebook-had-a-closer-relationship-than-it-disclosed-with-the-academic-it-called-a-liar/2018/03/22/ca0570cc-2df9-11e8-8688-e053ba58f1e4_story.html; Matthew Weaver, "Facebook Scandal: I Am Being Used as Scapegoat – Academic Who Mined Data," *The Guardian*, 21 March 2018, https://www.theguardian.com/uk-news/2018/mar/21/facebook-row-i-am-being-used-as-scapegoat-says-academic-aleksandr-kogan-cambridge-analytica.

[10] Elizabeth Dwoskin and Tony Romm, "Facebook's Rules for Accessing User Data Lured More Than Just Cambridge Analytica," *Washington Post*, 19 March 2018, https://www.washingtonpost.com/business/economy/facebooks-rules-for-accessing-user-data-lured-more-than-just-cambridge-analytica/2018/03/19/31f6979c-658e-43d6-a71f-afdd8bf1308b_story.html.

[11] Kang, "Facebook Faces Growing Pressure over Data and Privacy Inquiries."

[12] On the investigation in Britain, see Richard Gonzales, "U.K. Investigators Raid Cambridge Analytica Offices in London," *National Public Radio*, 23 March 2018, https://www.npr.org/sections/thetwo-way/2018/03/23/596558772/u-k-investigators-raid-cambridge-analytica-offices-in-london. Brazil has also opened an investigation: Ricardo Brito, "Brazil Prosecutors Open Investigation into Cambridge Analytica," *Reuters*, 21 March 2018, https://www.reuters.com/article/us-facebook-cambridge-analytica-brazil/brazil-prosecutors-open-investigation-into-cambridge-analytica-idUSKBN1GX35A. Within the United States, Common Cause has asked the Justice Department and Federal Election Commission to investigate the company: Lorraine Woellert, "Justice and Fec Asked to

ties to Russia. Like the conservative news outlet Breitbart, whose many anti-Clinton stories included falsehoods and were amplified by Russian bots during the 2016 election, Cambridge Analytica was bankrolled by the wealthy financier and computer scientist Robert Mercer, and run by the media mogul Steve Bannon. Whether Breitbart deliberately colluded with Russia has been a subject of investigation by the FBI.[13] We know that Cambridge Analytica pitched its services to a Russian oil firm, explaining how it could help suppress voter turnout in Nigeria.[14]

While some government agencies are working to hold these tech companies and private actors accountable, others have tried to hold Russia accountable more directly. Trump has been reluctant to acknowledge the conclusions of U.S. intelligence agencies: not only did Russia meddle in the U.S. election, but it also developed a preference for Trump and aided his campaign.[15] Nonetheless, on March 15 the Treasury Department imposed new sanctions on Russian individuals and organizations for state-sponsored election meddling and other cyberattacks.[16]

There is good reason to hold actors accountable for deceiving voters. In principle, imposing punishments for past misdeeds can deter future activities. But there are limits to deterrence by threat of punishment, particularly when the rewards for cyber operations appear to be so great. The most recent sanctions are unlikely to have much impact on Russia's economy or intelligence operations.[17] Admiral Michael R. Rogers, Director of NSA, noted that sanctions have not "changed the calculus or the behavior" of Russia. He further states that "we're probably not doing enough," to impose a cost on Russia.[18] But if, as Russia experts have

---

Investigate Cambridge Analytica," *Politico*, 26 March 2018, https://www.politico.com/story/2018/03/26/cambridge-analytica-investigation-request-484866.

[13] Justin Hendrix, "Did Cambridge Analytica Leverage Russian Disinformation for Trump?," *Slate*, 21 March 2018, https://slate.com/technology/2018/03/did-cambridge-analytica-leverage-russian-disinformation-for-trump.html.

[14] Graham-Harrison, "Cambridge Analytica: Links to Moscow Oil Firm and St Petersburg University."

[15] Office of the Director of National Intelligence, National Intelligence Council, "Assessing Russian Activities and Intentions in Recent US Elections," ICA 2017-01D, 6 January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[16] "Trump Administration Hits Russian Spies, Trolls with Sanctions over U.S. Election Interference, Cyberattacks," *Washington Post*, 15 March 2018, https://www.washingtonpost.com/world/national-security/trump-administration-sanctions-russian-spies-trolls-over-us-election-interference-cyber-attacks/2018/03/15/3eaae186-284c-11e8-b79d-f3d931db7f68_story.html.

[17] Since six of the individuals and four of the organizations were already subject to sanctions, they are seen as relatively weak. Indeed, two of the sanctioned organizations—the FSB (successor to KGB), sanctioned for targeting high level government officials, and GRU, a military spy organization sanctioned for election meddling and the NotPetya attacks on Ukraine—have limited dependence on the United States.

[18] Aaron Blake and Ellen Nakashima, "Cyber Chief Says Trump Has Given Him No New Authority to Strike at Russian Interference Threat," *Washington Post*, 27 February 2018, https://www.washingtonpost.com/world/national-security/cyber-chief-says-trump-has-given-him-no-new-authority-to-strike-at-russian-interference-threat/2018/02/27/41185978-1c24-11e8-ae5a-16e60e4605f3_story.html.

argued, the Kremlin viewed a Hillary Clinton presidency as an existential threat, the only penalty that would make it regret election interference would need to be exceedingly severe—perhaps as severe as war.[19]

Penalties for the tech sector are also unlikely to be sufficiently stiff. While Facebook may temporarily suffer from fines and plunging stock values, history suggests that tech giants have generally weathered such privacy scandals fairly well, rebounding and then continuing to profit from the sale of users' data.

In short, there are limits to the ability to deter future misbehavior by punishing past misdeeds. Additionally, there will always be new threats to counter. Indeed, many have argued that Russian disinformation is a relatively small problem; domestic disinformation campaigns are not illegal and yet can be just as problematic.[20] Clint Watts, a former FBI agent, testified that Russian disinformation was effective because it was amplified by Trump himself.[21]

There is a real need to go beyond the near-term focus on culpability and consider the deeper technopolitical vulnerabilities that make societies so easily hacked—vulnerabilities that lie in complex interactions between technology, flawed laws, corporate interests, individual and social biases, and structural inequalities.

Beyond Threats: Identifying Vulnerability

In the world of cybersecurity, "vulnerabilities" most often refer to weaknesses in computer code, such as software errors that allow hackers to access or control computer systems. Although contemporary computer systems are too complex to completely eliminate such technical vulnerabilities, more could be done.

Importantly, reducing vulnerabilities in computer code is a technopolitical problem, because code is produced by human organizations and actors with vested interests. Companies currently have substantial economic incentives to rush products to market before doing diligence on security.[22] Systems that are currently in place to rate product security, thereby informing buyers and giving companies an incentive to do better, are deeply flawed.[23] For years, people have argued that companies should be liable for producing insecure products, but

[19] Clinton Ehrlich, "The Kremlin Really Believes That Hillary Wants to Start a War with Russia," *Foreign Policy*, 7 September 2016, http://foreignpolicy.com/2016/09/07/the-kremlin-really-believes-that-hillary-clinton-will-start-a-war-with-russia-donald-trump-vladimir-putin/.

[20] Dipayan Ghosh and Ben Scott, "#DIGITALDECEIT: The Technologies Behind Precision Propaganda on the Internet," New America, 23 January 2018, https://www.newamerica.org/documents/2068/digital-deceit-final.pdf.

[21] Spencer Ackerman, "Russian Deception Influenced Election Due to Trump's Support, Senators Hear," *The Guardian*, 30 March 2017, https://www.theguardian.com/us-news/2017/mar/30/trump-russia-fake-news-senate-intelligence-committee.

[22] Ross Anderson, "The Economics of Information Security," *Science* 314:5799 (2006): 610-613, DOI: http://dx.doi.org/10.1126/science.1130992.

[23] The process of getting products certified within the "Common Criteria" system tends to be so slow that products are obsolete by the time they are rated; the system mostly evaluates documentation rather than the products themselves; the companies seeking evaluation pay an evaluator, and can hire another evaluator if they do not get the answer they want. General consensus is that a common criteria rating is no guarantee of security. Joab Jackson,

they are not.[24] Since most computer science programs do not require security training, common mistakes continue to be made.[25] Powerful interests—in making quick profits and avoiding government regulation—limit systemic change.

Vulnerabilities lie in more than just code, however. The easiest way into many systems is to manipulate people into responding to deceptive e-mails, visiting compromised websites, giving out confidential information, or otherwise compromising security. The Democratic National Committee was hacked not through a vulnerability in code, but by phishing.[26] Even if we completely eliminated the vulnerabilities in computer code, citizens would still be vulnerable to disinformation and propaganda campaigns. Such campaigns exploit not only confirmation bias—the universal human tendency to focus on information that confirms what one already believes—but also a complex technopolitical system that has worsened such biases, encouraging the construction of a (potentially deceptive) echo chamber.

A recent report on digital deception described the "interconnected tools," including behavioral tracking technologies, social media management software, and search engine optimization techniques, which function as a "brilliant technological machine that serves to align the economic interests of advertisers and the platform companies."[27] This machine has been optimized for delivering manipulative messages, and is easily used for politically-motivated disinformation campaigns.

Approaches to combatting disinformation have yet to really tackle the dangers inherent in this system. Instead they have tended to focus on either rating the veracity of online content, or educating individual internet users to distinguish between legitimate and deceitful content. While both approaches have merit, neither one deals adequately with systemic vulnerabilities.

The challenge of truth brokerage

Social media companies have been under some pressure to warn users of potentially deceptive content. Thus, for example, Facebook introduced a system wherein users could flag content as questionable, and professional fact-checkers would then evaluate it. However, fact checking remained limited, not only by the sheer volume of questionable posts, but by Facebook's unwillingness to provide information that might help the evaluators

"Symantec: Common Criteria Is Bad for You," *Government Computer News*, 4 May 2007, https://gcn.com/articles/2007/05/04/symantec-common-criteria-is-bad-for-you.aspx.

[24] Jon Evans, "Should Software Companies Be Legally Liable for Security Breaches?," *TechCrunch*, 6 August 2015, https://techcrunch.com/2015/08/06/should-software-companies-be-legally-liable-for-security-breaches/.

[25] Warwick Ashford, "Developers Lack Skills Needed for Secure Devops, Survey Shows," *Computer Weekly*, 17 August 2017, http://www.computerweekly.com/news/450424614/Developers-lack-skills-needed-for-secure-DevOps-survey-shows.

[26] Raphael Satter, "Inside Story: How Russians Hacked the Democrats' Emails," *Associated Press*, 4 November 2017, https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a.

[27] Ghosh and Scott, "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet," 3.

prioritize—such as which posts had already been fact-checked, how the amount of time required to check a story affected its spread, or how often copycat stories emerged to replace those that had been flagged.[28]

One year after rolling out the news screening program, Facebook cancelled it and stated that it would simply change its algorithm to prioritize news from trusted contacts.[29] While Facebook claims it wants to bring people together, this only enhances individuals' ability to become trapped within a false reality.

Other efforts to rate the veracity of web content are also flawed. Government attempts to act as the truth broker—for example Germany's and France's efforts to outlaw offensive content or fake news—raise concerns about suppressing free speech.[30] Efforts to automate truth brokers will embed value-laden assumptions into their algorithms, and thus will be controversial (and subject to automated countermeasures). The limits of automation have also been revealed in the case of the automated "fake news" detector that failed to flag an erroneous story about itself.[31]

Trying to vet the content of online content will ultimately have limited efficacy, in part because it is faster to spin out more fake news than it is to fact-check it. Additionally, readers may interpret fake news warnings as more evidence of the untrustworthy mainstream media. It is telling that stories flagged as suspect began receiving more, rather than fewer, views online.[32] Confidence in mainstream media was declining even before Trump began attacking it.[33]

This lack of confidence, along with the biases of contemporary media institutions, all contribute to technopolitical vulnerability. Media corporations have turned to inexpensive entertainment news (or "infotainment"), at the expense of international news that could improve global citizenship, as well as investigative reporting that could address problems affecting citizens. Although the limitations of traditional news institutions go well beyond the scope of this brief essay, they must be recognized a vulnerability that leads citizens to seek alternative, and sometimes deceptive, sources of information.

---

[28] Jason Schwartz, "Facebook Undermines Its Own Effort to Fight Fake News," *Politico*, 7 September 2017, https://www.politico.com/story/2017/09/07/facebook-fake-news-social-media-242407.

[29] Violet Blue, "Facebook's Fake War on Fake News," *Engadget*, 19 January 2018, https://www.engadget.com/2018/01/19/facebooks-fake-war-on-fake-news/.

[30] Yasmeen Serhan, "Italy Scrambles to Fight Misinformation Ahead of Its Elections," *The Atlantic*, 24 February 2018, https://www.theatlantic.com/international/archive/2018/02/europe-fake-news/551972/.

[31] Olivia Solon, "Fake News Detector for Facebook Leads to Fake News Story About Who Made It," *The Guardian*, 2 December 2016, https://www.theguardian.com/technology/2016/dec/02/facebook-fake-news-flag-techcrunch-bs-detector.

[32] Serhan, "Italy Scrambles to Fight Misinformation Ahead of Its Elections."

[33] Art Swift, "Americans' Trust in Mass Media Sinks to New Low," *Gallup*, 14 September 2016, http://news.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx.

Individual education and its limits

The other dominant approach to fighting disinformation has been to make internet users more savvy. In the United States, several states have introduced or passed legislation encouraging schools to teach critical media literacy.[34] A March 2018 European Commission report from an expert group on disinformation recommended education, along with better transparency online (more on that below).[35] Italy has been seen as a leader in such education.[36]

Individual education is useful, but it also faces practical limits. One is that the sheer complexity and opacity of the contemporary systems for surveillance and manipulation can elude even very informed internet users. The other is that disinformation is only one of several tactics for polarizing the electorate and undermining confidence political process. Russian operatives also used social media to organize rallies that debased political discourse through stunts such as hiring people to dress up as Hillary Clinton in a cage.[37] Perhaps most significantly, they amplified legitimate grievances among voters. These deeper and more systemic vulnerabilities—in the technopolitical regimes that leave internet users vulnerable to manipulation, and the unaddressed grievances that contribute to polarized political discourse—are all too often strategically ignored.

The "fantasy" of notice and consent privacy laws

The regime that enabled the rapid spread of disinformation and the Russian-led organization of divisive political rallies is working exactly as it was designed. Profit-seeking companies have developed technologies for ubiquitous surveillance and manipulation, tracking user behavior online, and delivering customized advertising. While internet users are somewhat aware of efforts at manipulation, most cannot be expected to really understand just how deep and pervasive it is.

One reason is that privacy laws are grounded in the disempowering and opaque regime of "notice and consent," wherein companies may track and sell user data, so long as the user has been notified, and has

[34] Ryan J. Foley, "Spread of Fake News Prompts Literacy Efforts in Schools," *PBS Newshour*, 31 December 2017, https://www.pbs.org/newshour/education/spread-of-fake-news-prompts-literacy-efforts-in-schools.

[35] European Commission, "Final Report of the High Level Expert Group on Fake News and Online Disinformation," 12 March 2018, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

[36] Serhan, "Italy Scrambles to Fight Misinformation Ahead of Its Elections."

[37] Parlapiano and Lee, "The Propaganda Tools Used by Russians to Influence the 2016 Election."

explicitly agreed to the terms.[38] Thus, Facebook has acknowledged that it "made mistakes" that compromised the privacy of over 50 million users, but also claims that "everyone involved gave their consent."[39]

In 2014 the President's Council of Advisors on Science and Technology (PCAST) noted: "Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[40] Researchers have estimated that if individuals read the privacy policies of each unique website they visited, they would be reading policies for between two and seven full-time work weeks each year.[41] Since the technical and legal implications of such policies can be difficult to understand, and since policies often refer to third parties, really doing diligence would take far longer. Notice and consent is a "take-it-or-leave-it" privacy regime; users have no ability to negotiate their privacy rights. No wonder, then, that most people simply click "agree."

PCAST recommended alternatives to the "notice and consent" regime, such as allowing users to associate themselves with a standard privacy policy developed by a trusted third party, such as the American Civil Liberties Union. Users could choose between multiple standard privacy policies, which might be developed with distinctive policy goals in mind (e.g. civil liberties or consumer protection). They also recommended technologies that can automatically constrain the ways in which data are used.[42]

While the flaws of notice-and-consent have been much-discussed, and alternatives have been proposed, we have seen little meaningful action. Companies profit enormously by selling users' data without their full understanding, so they resist change, strategically ignoring this systemic vulnerability. Now would be a good time for scholars, citizens, and policymakers to push for more realistic and consumer-oriented regime.

Structural inequalities

[38] Europe has recently proposed a shift towards "transparency and consent," but it may well suffer from the same problems as traditional notice and consent—putting too much of the burden for understanding complex technology and policies on the average internet user. Mark Young, Joseph Jones, and Ruth Scoles Mitchell, "EU Regulators Provide Guidance on Notice and Consent under GDPR," Covington & Burling LLP, Inside Privacy (blog), 14 December 2017, https://www.insideprivacy.com/international/european-union/eu-regulators-provide-guidance-on-notice-and-consent-under-gdpr/.

[39] On "mistakes" see Mark Zuckerberg, 21 March 2018, https://www.facebook.com/zuck/posts/10104712037900071. On consent, see Paul Grewal, Facebook Vice President & Deputy General Counsel, news update on 17 March 2018, https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

[40] President's Council of Advisors on Science and Technology, *Report to the President: Big Data and Privacy: A Technological Perspective* (2014), xi.

[41] Aleecia McDonald and Lorrie Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* 4:3 (2008).

[42] President's Council of Advisors on Science and Technology, "Report to the President: Big Data and Privacy: A Technological Perspective."

Susceptibility to manipulation is about more than a flawed privacy regime. Russia can exacerbate divisions within American society, but it cannot start them. There will always be disagreements within a free society, but Russian cyber operations targeted some of the most fundamental vulnerabilities within American society: a political system that is rigged in favor of wealthy donors and politicians; religious intolerance and xenophobia; and structural racism.[43]

The public release of e-mails from leaders in the Democratic National Committee would not have been divisive had they not revealed biases in favor of the establishment candidate, Hillary Clinton, and against the challenger, Bernie Sanders. It is telling that supporters of both Sanders on the left and Trump on the right agreed on one thing: the system is rigged. In the 2016 election cycle, about half of one percent of all Americans funded nearly 68% of all political campaigns.[44] In 2014, the top 1 percent of 1 percent of donors funded 29% of all political campaigns, with 60 people giving over one million dollars, and three giving more than 10 million dollars. These wealthy donors tend to be male, to work in finance, and to push for policies that represent these elite interests.[45] And of course, their funds allow their preferred politicians to pay social media and advertising companies to target, manipulate and even deceive the majority of voters, who might otherwise prefer quite different policies.

Another very real vulnerability that these campaigns target is ethnic, racial, and religious divisions. Russians could not mobilize anti-Muslim and anti-immigrant rallies if religious bigotry and xenophobia were not real problems. A major reason that Russian operatives can infiltrate and polarize online discourse about the Black Lives Matter movement is that people have legitimate grievances.

These grievances, like other vulnerabilities, are rooted in a technopolitical regime that disproportionately incarcerates black and Latino men, strategically ignores pollution and other technological risks that disproportionately affect African Americans, and limits access to health care and safe housing.[46] Racialized voter suppression efforts have been on the rise for more than a decade, including voter identification requirements that persons of color are less likely to be able to achieve; restricting opportunities for early voting; and purging voter rolls. Over 800 polling stations closed in 2016, mostly in areas that are

[43] Adam Entous, Craig Timberg, and Elizabeth Dwoskin, "Russian Operatives Used Facebook Ads to Exploit America's Racial and Religious Divisions," *Washington Post*, 25 September 2018, https://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa_story.html.

[44] "Donor Demographics," *OpenSecrets.org,* The Center for Responsive Politics, https://www.opensecrets.org/overview/donordemographics.php?cycle=2016&filter=A, accessed 29 March 2018.

[45] Peter Olsen-Phillips, Russ Choma, Sarah Bryner, and Doug Weber, "The Political One Percent of the One Percent in 2014: Mega Donors Fuel Rising Cost of Elections," *OpenSecrets.org,* The Center for Responsive Politics, 30 April 2015, https://www.opensecrets.org/news/2015/04/the-political-one-percent-of-the-one-percent-in-2014-mega-donors-fuel-rising-cost-of-elections/.

[46] Dayna Bowen Matthew, Edward Rodrigue, and Richard V. Reeves, "Time for Justice: Tackling Race Inequalities in Health and Housing," Brookings Institution, 19 October 2016, https://www.brookings.edu/research/time-for-justice-tackling-race-inequalities-in-health-and-housing/.

predominantly populated by minorities, making it impossible for people unable to afford cars to vote.[47] This worsens the well-documented fact that minorities wait nearly twice as long as white people to vote—and some must wait for hours.[48] A statistical analysis of state legislation between 2006 and 2011 shows that restrictive voting laws are consistent with "the targeted demobilization of minority voters and African Americans."[49] Such measures only increased since then, with twenty states passing voting restrictions since 2010, and laws in fourteen of those states went into effect in 2016.[50] Not coincidentally, these targeted voters were also far less likely to vote for Trump.

Importantly, structural racism is not a new vulnerability for the United States. Indeed, Russian propaganda has highlighted racial violence and injustice in the United States since at least the 1930s, and concerns about the damage done by such propaganda at least partly contributed to politicians eventually championing civil rights legislation.[51] If concerns about basic human rights do not motivate action on these issues, perhaps concerns about national security and sovereignty can.

Conclusion

Cyber-threats will continue to grow. Each day that I have spent writing this essay, new headlines have appeared: about attacks on Atlanta's city services; Spanish police have arrested a Russian and Ukrainian cyber-gang for stealing over one billion Euros from financial institutions; and National Security Advisor-designate John Bolton has suggested launching retaliatory cyber attacks on Russia.[52] These threats will continue in large part because the perceived payoff for cyber-intrusions is so high—in some cases so high that deterrence by

[47] Ari Berman, "There Are 868 Fewer Places to Vote in 2016 Because the Supreme Court Gutted the Voting Rights Act," *The Nation*, 4 November 2016, https://www.thenation.com/article/there-are-868-fewer-places-to-vote-in-2016-because-the-supreme-court-gutted-the-voting-rights-act/.

[48] David A. Graham, "Here's Why Black People Have to Wait Twice as Long to Vote as Whites," *The Atlantic*, 8 April 2013, https://www.theatlantic.com/politics/archive/2013/04/heres-why-black-people-have-to-wait-twice-as-long-to-vote-as-whites/274791/; Ibid.

[49] Keith G. Bentele and Erin E. O'Brien, "Jim Crow 2.0? Why States Consider and Adopt Restrictive Voter Access Policies," *Perspectives on Politics* 11:4 (2013): 1088.

[50] Brennan Center for Justice, "Election 2016: Restrictive Voting Laws by the Numbers," 28 September 2016, https://www.brennancenter.org/analysis/election-2016-restrictive-voting-laws-numbers.

[51] Julia Ioffe, "The History of Russian Involvement in America's Race Wars," *The Atlantic*, 21 October 2017, https://www.theatlantic.com/international/archive/2017/10/russia-facebook-race/542796/.

[52] On Atlanta, see Alan Blinder and Nicole Perlroth, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder," *New York Times*, 27 March 2018, https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html. On the arrests, see Barry Hatton and Raphael Satter, "Spain Breaks up Cybercrime Gang after $1.2 Billion Spree," *Associated Press*, 26 March 2018, https://www.apnews.com/amp/187814286d7147aebf3b670623aeea51. On Bolton, see Cory Bennnett, "John Bolton, Cyber Warrior," *Politico*, 1 April 2018, https://www.politico.com/story/2018/04/01/john-bolton-cyber-hawk-russia-451937.

threat of punishment becomes impractical. Efforts to pre-empt malicious cyber operations, as has been suggested recently, may be valuable in some cases. But it will be impossible to preempt all possible threats.

An alternative is to remediate the fundamental vulnerabilities that enable and encourage malicious cyber operations. These vulnerabilities are rooted in technopolitical regimes—that is, they are produced by interactions between complex technology, corporate interests, flawed laws, individual and social biases, and structural inequalities.

None of these vulnerabilities will be easily fixed, and any full discussion of their solutions would go far beyond the scope of this brief essay. Nonetheless, we do have promising proposals for improving the quality and relevance of mainstream news, for empowering consumers to protect their privacy, for reducing the power of big money in elections, and for fighting structural racism including empowering citizens whose participation as voters has been suppressed. Technopolitical vulnerabilities are often ignored by those who benefit from leaving the current regime in place—incumbent policymakers, wealthy donors, big data and media corporations. While government agencies pursue questions of blame and accountability, now would be a good time to push for changes that can remediate technopolitical vulnerabilities.

Rebecca Slayton is Associate Professor at Cornell University, jointly appointed in the Science & Technology Studies Department and the Judith Reppy Institute for Peace and Conflict Studies. Her first book, *Arguments that Count: Physics, Computing, and Missile Defense, 1949-2012* (MIT Press, 2013) shows how the rise of a new field of expertise in computing reshaped public policies and perceptions about the risks of missile defense in the United States. She is currently working on *Shadowing Cybersecurity*, a book which examines the history of cybersecurity expertise through the interplay of innovation and repair.