



ELECTION MANIPULATION:

Is America's Voting System Secure?

John Allen





© 2020 ReferencePoint Press, Inc.
Printed in the United States

For more information, contact:

ReferencePoint Press, Inc.
PO Box 27779
San Diego, CA 92198
www.ReferencePointPress.com

ALL RIGHTS RESERVED.

No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, web distribution, or information storage retrieval systems—without the written permission of the publisher.

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA

Name: Allen, John, 1957– author.
Title: Election Manipulation: Is America's Voting System Secure?/John Allen.
Description: San Diego, CA: ReferencePoint Press, 2020. |
Includes bibliographical references and index.
Identifiers: LCCN 2019042848 | ISBN
9781682828076 (library binding) | ISBN 9781682828083 (ebook)
Subjects: Juvenile literature.

Introduction	4
A Stern Warning	
Chapter One	8
Hacking into Campaign Networks	
Chapter Two	20
Spreading Fake News on Social Media	
Chapter Three	32
Tampering with Voter Databases	
Chapter Four	44
Interfering with the Voting Process	
Chapter Five	56
The Future of Election Security	
Source Notes	67
For Further Research	72
Index	74
Picture Credits	79
About the Author	80

A Stern Warning

On July 24, 2019, special prosecutor Robert Mueller made a highly anticipated appearance on Capitol Hill. Before two committees in Congress, Mueller answered questions about his team's recent probe into Russian interference in the 2016 presidential election. The nearly two-year investigation found numerous instances of Russian meddling in the election, many of which led to indictments. Russia had interfered in two ways—first, by carrying out a social media campaign that favored the Republican candidate, Donald Trump; second, by hacking into the computer networks of Hillary Clinton's campaign and the Democratic National Committee (DNC).

In the end, Mueller's team determined there was insufficient evidence that Trump or members of his campaign had conspired with Russians in these activities. The team reached no conclusion as to whether Trump had acted to obstruct the investigation. During hours of testimony, Mueller added little to the official report on the probe. However, when asked whether Russia might be planning attacks on future US elections, the former FBI director delivered a stern warning. "It wasn't a single attempt," he said. "They're doing it as we sit here."¹


Faith in the Integrity of Elections

The Mueller Report's revelations about Russian interference sent shock waves through the halls of Congress and the nation. One day after Mueller's testimony, there was more evidence of Rus-

sian mischief. The Senate Intelligence Committee released a report claiming that in 2016 Russia had targeted election systems in all fifty states. The report contends that federal officials underestimated Russia's drive to interfere in the election. As a result, state officials received inadequate warnings and did not react strongly enough.

In a democracy that prides itself on free and fair elections, it is vital that American citizens not lose faith in the integrity of the election process. With its attempts to meddle in US elections, Russia seeks to destroy that faith. Beyond supporting individual candidates, Russian hackers want to spread confusion and discord among Americans. In April 2019, soon after the release of the Mueller Report, FBI director Christopher Wray warned that Russia's attacks would not wait for 2020 but were ongoing. "What has pretty much continued unabated is the use of social media, fake news, propaganda, false personas, etc. to spin us up, pit us against each other, to sow divisiveness and discord, to undermine America's faith in democracy," Wray said. "That is not just an election-cycle threat. It is pretty much a 365-day-a-year threat."² In response, Wray announced that the FBI was enlisting agents and analysts to bolster America's defenses against election interference.

Wray's boss in the White House has not been so forthright in his rhetoric. Trump believes that the focus on Russia's meddling in the election is really an attempt to question the legitimacy of his victory. At joint press events with Russian president Vladimir Putin, Trump has accepted Putin's claims that there was no interference. However, eight federal and congressional intelligence and national security groups, from the CIA to the House and Senate Intelligence Committees, have concluded that Russia interfered in the 2016 election.



"It wasn't a single attempt. They're doing it as we sit here."¹

—Special prosecutor Robert Mueller on Russian interference in US elections



Special prosecutor Robert Mueller meets with the House Judiciary Committee in July of 2019. Mueller answered questions about his team's probe into Russian interference in the 2016 presidential election.

Warnings About Election Attacks in 2020

US law enforcement and intelligence agencies are already warning about likely attempts to interfere in the 2020 election as well. Officials see Russia, with its sophisticated tools for cyberattack and propaganda, as the most urgent ongoing threat. But they also believe other foreign countries and domestic groups may try to manipulate the election. In response, certain federal agencies, including the National Security Agency and the US Cyber Command, have expanded and formed a joint task force to combat Russian influence in the months leading up to the election.

Officials are focused on three main methods of attack. The first is hacking into computer networks run by political parties or campaigns. If hackers gain access to these systems, they can steal information about campaign strategies, polling, and opposition research. Armed with this information, hackers could spoil campaign plans by


publishing them online or reveal the methods used to gather dirt on political opponents. They can also arrange for stolen emails to be made public, as was done by Russian hackers in the run-up to the 2016 election. Emails hacked from the DNC led to embarrassing revelations about the inner workings of the campaign.

Another method is using social media to spread false or misleading information. Political ads on Facebook or Instagram can influence voters with inflammatory attacks on candidates or deceptive takes on social issues. Fake news stories from obscure websites can be posted on Twitter and then retweeted thousands of times. Sizable numbers of readers may accept them as true before they can be debunked by respectable news sources.

A third method is tampering with the voting process itself, including the vote count. Hackers can break into election board computers and tamper with voter registration data. Some fear that electronic voting machines could be manipulated by hackers or tampered with on-site. Hackers also could interfere with how votes are counted and how the totals are reported.

Approaching the Threat with Urgency

All of these methods—along with whatever new techniques might be in the works—are apt to erode Americans' confidence in their democracy. Experts say federal and state governments must approach the threat with more urgency. Better communication is needed to warn campaigns and election officials when hacking is detected. Social media companies must take steps to eliminate fake news and deceptive ads. More money must be spent to shore up the nation's voting system. "Election security is national security," says Elizabeth Howard, former deputy commissioner for the Virginia Department of Elections, "and we are only as strong as our weakest link."³



"Election security is national security, and we are only as strong as our weakest link."³

—Elizabeth Howard, former deputy commissioner for the Virginia Department of Elections

Hacking into Campaign Networks

Microsoft, one of the world's leading technology companies, knows a hacking scheme when it sees one. The company spends vast sums to protect its software from malicious hackers. And long before American voters go to the polls in November 2020, cybersecurity experts at Microsoft are already warning of foreign attempts to hack into the computer systems of campaigns and related political groups.

In July 2019 Microsoft announced that its threat intelligence team had detected Russian hackers at work against United States think tanks, academic groups, and nongovernmental organizations. These are groups that help political campaigns prepare strategy and address current issues. The hackers include Russian cybercriminals known as Fancy Bear. Prior to the 2016 presidential election, they managed to break into the computer networks of Hillary Clinton's campaign and the DNC. Experts at Microsoft are all but certain that Fancy Bear is preparing another round of attacks for the run-up to the 2020 election. Moreover, they fear that campaigns are still vulnerable. According to Tom Burt, Microsoft's vice president of customer security and trust, "Many organizations essential to democracy do not have the resources or expertise to defend themselves against cyberattacks."⁴

Probing for Weaknesses

Hackers seem to be probing for weaknesses in preparation for the 2020 presidential campaign. Burt says Microsoft's threat in-


telligence team has uncovered hacking attacks against various targets in the past two years. In 2018 Microsoft alerted more than ten thousand customers to attacks from Russia, North Korea, and Iran, most of them aimed at corporations or political groups. In the months before the 2018 midterm elections in the United States, Fancy Bear hackers set up fake Internet domains linked to two conservative

nonprofit groups. One was the Hudson Institute, a prominent think tank. The other was the International Republican Institute, whose board of directors includes six Republican senators. Microsoft acted quickly to notify the organizations about the threats.

According to analysts at the security firm FireEye, Fancy Bear has also targeted campaigns in the 2019 parliamentary elections in Europe. Campaign workers in several European Union countries received emails with fake links to government websites. The links could allow hackers to get access to the campaigns' computer systems. It is unclear whether sensitive data was leaked, but FireEye notes that this type of hacking is usually successful. "It's clear that democracies around the world are under attack," says Brad Smith, Microsoft's president and chief legal officer.

Foreign entities are launching cyber strikes to disrupt elections and sow discord. Unfortunately, the internet has become an avenue for some governments to steal and leak information, spread disinformation, and probe and potentially attempt to tamper with voting systems.⁵

In response, tech firms have launched projects aimed at protecting political campaigns in the United States and the West. In 2017 Facebook contributed \$500,000 to Harvard University's Kennedy School of Government to create an initiative called



"Many organizations essential to democracy do not have the resources or expertise to defend themselves against cyberattacks."⁴

—Tom Burt, Microsoft's vice president of customer security and trust



Microsoft's threat intelligence team has uncovered hacking attacks against various targets in the past two years. In 2018 Microsoft alerted more than ten thousand customers to attacks, mostly toward corporations and political groups.

Defending Digital Democracy. One of its main goals is to help politicians and campaign personnel protect their networks from cyberattacks. In April 2018 Microsoft announced its own Defending Democracy Program, which includes measures for campaign security as well as tools to prevent disinformation and other online mischief. Diana Kelley, Microsoft's chief technology officer for cybersecurity, wants to advise campaigns on the various methods hackers use to infiltrate email accounts. "The first [goal] is to prevent the hacking, and to look at how they're hacking, what they're trying to accomplish,"⁶ says Kelley. These tech-based programs are ramping up even more in anticipation of the 2020 campaign.

Russian Phishing Attacks

Experts warn that in 2020 hackers likely will try the approach that worked so well in the 2016 election: a basic cyberattack called phishing. In a phishing attack, a person receives an email containing a link or a password request. Clicking on the link or keying in

the password enables hackers to infiltrate the computer system. According to the Mueller Report, military agents with the GPU, Russia's secret service, began their hacking efforts in March 2016. They used a special variation of phishing called spear phishing, in which fake emails seem to be from trusted sources, such as the government, banks, or tech companies.

The Russian hackers sent spear-phishing emails to various staff members on Clinton's campaign, including John Podesta, the campaign chair. Podesta received an email supposedly from Google claiming that a third party was trying to break into his account and urging him to change his password at once. An aide with access to Podesta's account saw the message and forwarded it to a staff

Bipartisan Hacking Attempts

Hackers also targeted the Republican National Committee (RNC) in 2016. In a January 2017 appearance before the Senate Intelligence Committee, then-FBI director James Comey said hackers believed to be Russians stole RNC emails. Comey revealed that the hacked RNC email domain was older and out of use. "There was evidence that there was hacking directed at state-level organizations and the RNC, but old domains of the RNC, that is, email domains they were no longer using," Comey told the committee. "Information was harvested from there, but it was old stuff. None of that was released." Comey added that he did not know whether hackers attempted to breach newer RNC emails or the Trump campaign. The fact that RNC emails went unpublished was one reason that intelligence officials determined Russia was intent on helping Donald Trump win the election.

Some cyber experts have expressed doubts about whether Russians actually hacked the DNC emails. Bill Binney, a retired technical director at the National Security Agency, believes the emails were downloaded to a thumb drive on-site at the DNC, perhaps by a staffer upset at the party's treatment of Bernie Sanders. Julian Assange, the founder of WikiLeaks, the site that published the stolen emails, has claimed the files did not come from the Russians. Robert Mueller did not have the DNC servers examined during his investigation, relying instead on information provided by Crowdstrike, a tech firm hired by the DNC. Mueller's team also did not interview Assange.

Quoted in Andy Greenberg, "Russia Hacked 'Older' Republican Emails, FBI Director Says," *Wired*, January 10, 2017. www.wired.com.

technician to see whether it was genuine. The technician recognized it as a hack attempt but replied with a fatal typo. He declared that the email was *legitimate*—not *illegitimate* as he intended—and advised Podesta to change his password immediately. When Podesta typed in the old password to make the change, Russian hackers gained access to thousands of Podesta’s emails for the campaign.

Shortly thereafter, Russian GPU agents also used a spear-phishing ploy to hack into other networks, including those of the DNC and the Democratic Congressional Campaign Committee (DCCC). To divert investigators from their hacking scheme, the Russians masked themselves using an online persona, Guccifer 2.0. According to the Mueller Report, they passed thousands of stolen emails to WikiLeaks, an Internet site that specializes in publishing leaked or stolen materials. WikiLeaks released the emails and documents from Podesta and the DNC in stages prior to the November 2016 election. The release led to some embarrassing disclosures for Democrats and the Clinton campaign. For example, emails from the DNC showed that the committee had tried to undermine the campaign of Senator Bernie Sanders, Clinton’s chief rival for the Democratic Party nomination.

Political analysts believe that some Sanders supporters, angered by the WikiLeaks emails, may have sat out the general election in protest or even voted for Trump. A survey of the 2016 presidential election by the Cooperative Congressional Election Study found that more than one in ten people who voted for Sanders in the Democratic primary switched to Trump in the general election. Political analysts note that there were many factors that led to Trump’s surprising victory. But according to NPR political analyst Danielle Kurtzleben, “To answer the question that many Clinton supporters may be asking: . . . yes—there are enough of those Sanders-Trump voters [to] have potentially swung the election toward Clinton and away from Trump.”⁷

Mueller and his team brought indictments against twelve Russian intelligence agents for their hacking activities. The Mueller Re-




Russian hackers targeted Hillary Clinton (pictured) during her 2016 presidential campaign. The hackers were successful in gaining access to thousands of confidential campaign emails.

port details how the Russians and WikiLeaks timed the release of the DNC emails to create conflict between the Clinton and Sanders camps during the party's convention. But experts on election security say the most important outcome of the Mueller investigation might be a greater awareness of how Russia could attack US political campaigns in 2020. As California secretary of state Alex Padilla declares, "For elections officials across the country, the Mueller investigation and indictments have heightened our need for additional resources to defend against cyber attacks."⁸

Taking the Threat Seriously

A major step for political campaigns in 2020 is to take the threat of Russian hacking seriously—and that means spending money for cyberdefenses. Campaigns generally are reluctant to divert scarce dollars from day-to-day operations into security. Yet

experts warn that leaving computer files and email systems unprotected is an invitation to malicious cyber-criminals. Also, since campaigns operate on a short-term basis, they tend not to have well-developed protocols for cybersecurity among staffers. “The reason campaigns are so bad at cybersecurity is they are here one day and gone the next,” says Aaron Trujillo, former chief of staff of the DCCC. “There needs to be a person who has to wake up every single day with part of their mission being how they are going to address threats and mitigate damage if there is a breach.”⁹



“The reason campaigns are so bad at cybersecurity is they are here one day and gone the next.”⁹

—Aaron Trujillo, former chief of staff of the DCCC

Plenty of tech companies are anxious to advise campaigns on cybersecurity. Many are willing to provide their services for free or at lower rates. Yet campaign officials are leery of violating campaign finance laws by accepting services at a reduced rate, which might be considered an illegal contribution. In May 2019 the Federal Election Commission (FEC) took action to relieve this concern. FEC chair Ellen Weintraub issued a ruling that allowed Defending Digital Campaigns, a nonprofit group, to offer free and low-cost cybersecurity services to political campaigns without running afoul of campaign finance laws. The group is a spinoff of Harvard’s Defending Digital Democracy project. It was specifically created to help campaigns defend themselves against hacking attempts. Weintraub says the ruling was necessary to guard against foreign cyberattacks and that the federal government needs to do more to protect political parties and campaigns from foreign hackers.

Matt Rhoades, one of the board members for Defending Digital Campaigns, served as Mitt Romney’s campaign manager in Romney’s run for president in 2012. He knows how much cash-strapped campaigns will benefit from the ruling. “When you’re first setting up and you’re first raising those precious hard dol-

Introduction: A Stern Warning

1. Quoted in Julie Hirschfeld and Mark Mazzetti, “Highlights of Robert Mueller’s Testimony to Congress,” *New York Times*, July 24, 2019. www.nytimes.com.
2. Quoted in Julian E. Barnes and Adam Goldman, “F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counter-intelligence Operations,” *New York Times*, April 26, 2019. www.nytimes.com.
3. Quoted in Tim Lau, “U.S. Elections Are Still Vulnerable to Foreign Hacking,” Brennan Center for Justice, July 18, 2019. www.brennancenter.org.

Chapter One: Hacking into Campaign Networks

4. Quoted in Nat Levy, “Microsoft Warns of Increased Attacks Ahead of European Elections, Expands AccountGuard Cybersecurity Program,” *GeekWire*, February 19, 2019. www.geekwire.com.
5. Brad Smith, “We Are Taking New Steps Against Broadening Threats to Democracy,” *Microsoft on the Issues* (blog), August 20, 2018. <http://blogs.microsoft.com>.
6. Quoted in Dan Patterson, “How Microsoft’s Defending Democracy Program Amplifies Account Security,” *TechRepublic*, October 31, 2018. www.techrepublic.com.
7. Danielle Kurtzleben, “Here’s How Many Bernie Sanders Supporters Ultimately Voted for Trump,” *NPR*, August 24, 2017. www.npr.org.
8. Quoted in Eric Geller, “Collusion Aside, Mueller Found Abundant Evidence of Russian Election Plot,” *Politico*, April 18, 2019. www.politico.com.
9. Quoted in Dustin Volz and Tarini Parti, “2020 Campaigns Remain Vulnerable as Signs of Russian Hackers Re-emerge,” *Wall Street Journal*, June 13, 2019. www.wsj.com.

FOR FURTHER RESEARCH

Books

Jake Braun, *Democracy in Danger: How Hackers and Activists Exposed Fatal Flaws in the Election System*. Lanham, MD: Rowman & Littlefield, 2019.

Mitchell Brown, ed., *The Future of Election Administration: Elections, Voting, Technology*. New York: Palgrave Macmillan, 2019.

James W. Cortada and William Aspray, *Fake News Nation: The Long History of Lies and Misinterpretations in America*. Lanham, MD: Rowman & Littlefield, 2019.

Malcolm Nance, *The Plot to Hack America: How Putin's Cyber-spies and WikiLeaks Tried to Steal the 2016 Election*. New York: Skyhorse, 2017.

Clint Watts, *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News*. New York: Harper Paperbacks, 2019.

Internet Sources

Joe Andrews, "Fake News Is Real—A.I. Is Going to Make It Much Worse," CNBC, July 12, 2019. www.cnbc.com.

Lawrence Norden and Andrea Córdova McCadney, "Voting Machines at Risk: Where We Stand Today," Brennan Center for Justice, March 5, 2019. www.brennancenter.org.

Nicole Perlroth and Matthew Rosenberg, "Election Rules Are an Obstacle to Cybersecurity of Presidential Campaigns," *New York Times*, June 6, 2019. www.nytimes.com.

Dustin Volz and Tarini Parti, "2020 Campaigns Remain Vulnerable as Signs of Russian Hackers Re-emerge," *Wall Street Journal*, June 13, 2019. www.wsj.com.

Kim Zetter, "The Crisis of Election Security," *New York Times Magazine*, September 26, 2018. www.nytimes.com.

Websites

Brookings Institution — www.brookings.edu

The Brookings Institution is a nonprofit public policy organization based in Washington, DC. Its mission is to conduct and present in-depth research on ideas for solving societal problems on the local, national, and international level. Among the articles on the Brookings website is “Political Campaigns Are the First Line of Defense in Election Security.”

Defending Digital Democracy — www.belfercenter.org/project/defending-digital-democracy)

The Defending Digital Democracy Project at Harvard’s Kennedy School of Government aims to develop strategies, tools, and technology to protect democratic processes and systems from cyber and information attacks. The project’s bipartisan team of technology experts and leaders in cybersecurity are working to offer concrete solutions to the urgent problem of election hacking.

US Department of Justice — www.justice.gov/storage/report.pdf

Volumes I and II of the *Report on the Investigation into Russian Interference in the 2016 Presidential Election* by Special Counsel Robert S. Mueller III can be found here. The redacted report, released in March 2019 by the special counsel’s office, appears in full. Related court documents, including indictments and plea agreements stemming from the investigation, can be found at www.justice.gov/sco.

US Election Assistance Commission — www.eac.gov

Created under the 2002 Help America Vote Act (HAVA), the EAC serves as a vital resource for administering elections in the United States. The EAC distributes federal funds to states, helps local election boards meet HAVA requirements, and conducts tests on and certifies voting equipment.

Note: Boldface page numbers indicate illustrations.

Abbott, Mark, 62
 absentee ballots, 54
 AccountGuard, 18–19
 Anomali Labs, 36
 Appel, Andrew, 65
 Area 1 (cybersecurity company), 15
 artificial intelligence (AI), 27–28
 Assange, Julian, 11

Bandow, Doug, 25
 Barahona, Dan, 36
 Becker, David, 60
 Binney, Bill, 11
 Blaze, Matt, 39
 blockchain (encryption technology), 54
 Boix, Xavier, 28
 Brennan Center for Justice, 49, 64
 Brexit, 30
 Brookings Institution, 73
 Burt, Tom, 8–9, 47
 Bush, George W., 47

Center for Democracy & Technology, 16
 Chávez, Hugo, 63–64
 China
 as potential source of election interference, 31
 use of disinformation by, 25
 Cillizza, Chris, 57

Clinton, Hillary, 4, **13**, 22
 on dangers of fake news, 21–22
 Comey, James, 11
 Constone, Josh, 24
 Cooperative Congressional Election Study, 12
 Córdova McCadney, Andrea, 49–50, 64–65
 CrowdStrike, 11
 cyberattacks
 of political parties/campaigns, 6–7
 initiatives to prevent, 6–7, 9–10
 on vote-reporting networks, 52–55
 Cyber Command, US, 6
 cybersecurity
 FEC ruling on, 15
 reluctance of campaigns to spend money on, 13–14
Cybersecurity Services Catalog for Election Infrastructure (US Department of Homeland Security), 15–16

dark web, 36
 deepfake technology, 28–29
 Def Con Hacking Conference, 44, **46**, 48
 Defending Digital Campaigns, 14
 Defending Digital Democracy, 9–10, 73