# CONTEMPORARY PRACTICE OF THE UNITED STATES RELATING TO INTERNATIONAL LAW

EDITED BY KRISTEN E. EICHENSEHR*

***In this section:***



* Jack V. Hoover, Kevin Krotz, Pierce MacConaghy, Kyle McGoey, Margaret Shin, and Lucianna Stamper contributed to the preparation of this section.



https://doi.org/10.1017/ajil.2021.10 Published online by Cambridge University Press

GENERAL INTERNATIONAL AND U.S. FOREIGN RELATIONS LAW

*Government Agencies and Private Companies Undertake Actions to Limit the Impact of Foreign Influence and Interference in the 2020 U.S. Election*

doi:10.1017/ajil.2021.10

After Russia targeted the 2016 presidential election,[1] U.S. government authorities repeatedly warned about the prospects of foreign interference in and influence on the 2020 election. Throughout the fall of 2020, government officials and private companies took a number of actions to address threats to the election, including issuing public warnings, imposing sanctions, and taking down foreign government-linked accounts. In a declassified report released in March 2021, the intelligence community concluded that although Russia and Iran carried out influence operations to affect the election, there are "no indications that any foreign actor attempted to alter any technical aspect of the voting process in the 2020 US elections, including voter registration, casting ballots, vote tabulation, or reporting results."[2] In December 2020, however, U.S. cybersecurity firm FireEye disclosed that it suffered a breach by a nation-state sponsored actor, and numerous U.S. government agencies soon revealed that they too had been breached in intrusions widely attributed to Russia.

In 2016, Russia conducted sustained operations targeting the election, including hacking into the Democratic National Committee (DNC) computer networks, providing over 20,000 DNC emails to WikiLeaks for release, and leveraging social media for influence operations.[3] Although the DNC hack was revealed in June 2016, the U.S. government did not publicly attribute the malicious cyber activity to Russia until October.[4] Social media companies too were heavily criticized for failing to recognize and respond to Russian influence operations on their platforms.[5]

In 2020, the federal government assumed a more proactive stance, taking a number of public actions before the election both to inform the public and disrupt potential operations. In doing so, it focused on potential threats from several countries. On July 24, 2020, the Office

[1] Kristina Daugirdas & Julian Davis Mortenson, Contemporary Practice of the United States, 111 AJIL 476, 483 (2017).

[2] Nat'l Intel. Council, Foreign Threats to the 2020 US Federal Election, ICA 2020-00078D (Mar. 10, 2021), *available at* https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

[3] *Id.* at 483–85; Report of the Select Committee on Intelligence, U.S. Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election (SSCI Report) (Nov. 2020), *at* https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures; Robert S. Mueller III, Report on the Investigation into Russian Interference in the 2016 Presidential Election, at 38, 44–50 (Mar. 2019), *available at* https://apps.npr.org/documents/document.html?id=5955997-Muellerreport; Office of Director of Nat'l Intelligence, Assessing Russian Activities and Intentions in Recent US Elections, ICA 2017-01D (Jan. 6, 2017), *available at* https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[4] Abigail Abrams, *Here's What We Know So Far About Russia's 2016 Meddling*, TIME (Apr. 18, 2019), *at* https://time.com/5565991/russia-influence-2016-election.

[5] Hearing Before the Senate Committee on Intelligence, 116 Cong. 2 (2017) (Remarks by S. Comm. Chairman Richard Burr), *at* https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections# ("[Y]our three companies have developed platforms that have tremendous reach and, therefore, tremendous influence. . . . The American people now need to understand . . . what you're doing to protect them. Your actions need to catch up to your responsibilities.").

of the Director of National Intelligence (ODNI) issued a warning about potential election-related operations:

> At this time, we're primarily concerned with China, Russia and Iran—although other nation states and non-state actors could also do harm to our electoral process. Our insights and judgments will evolve as the election season progresses.
>
> China is expanding its influence efforts to shape the policy environment in the United States, pressure political figures it views as opposed to China's interests, and counter criticism of China. Beijing recognizes its efforts might affect the presidential race.
>
> Russia's persistent objective is to weaken the United States and diminish our global role. Using a range of efforts, including internet trolls and other proxies, Russia continues to spread disinformation in the U.S. that is designed to undermine confidence in our democratic process and denigrate what it sees as an anti-Russia "establishment" in America.
>
> Iran seeks to undermine U.S. democratic institutions and divide the country in advance of the elections. Iran's efforts center around online influence, such as spreading disinformation on social media and recirculating anti-U.S. content.[6]

Democratic congressional leaders, however, criticized the ODNI release on the grounds that it created "a false sense of equivalence to the actions of foreign adversaries by listing three countries of unequal intent, motivation and capability together" and "fails to fully delineate the goal, nature, scope and capacity to influence our election, information the American people must have as we go into November."[7]

In response, ODNI provided more detailed analysis of Chinese, Russian, and Iranian motivations on August 7, asserting "that China prefers that President Trump—whom Beijing sees as unpredictable—does not win reelection," "Russia is using a range of measures to primarily denigrate former Vice President Biden and what it sees as an anti-Russia 'establishment,'" and "Iran seeks to undermine U.S. democratic institutions" and President Trump and "to divide the country in advance of the 2020 elections."[8] A January 2021 report by the ODNI Analytical Ombudsman noted that some intelligence analysts considered the July and August statements and others "a 'gross misrepresentation' of established [Intelligence Community] views,"[9] in part because of the Trump administration's emphasis on Chinese influence operations and attempts to deemphasize the threat posed by Russia.[10]

[6] Office of Director of Nat'l Intelligence Press Release, Statement By NCSC Director William Evanina: 100 Days Until Election 2020 (July 24, 2020), *at* https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020.

[7] Speaker of the House Press Release, Pelosi, Schumer, Schiff, Warner Joint Statement Following ODNI Announcement Regarding Election Security and Foreign Threats (July 24, 2020), *at* https://www.speaker.gov/newsroom/72420-1 [https://perma.cc/9SNR-2UP6].

[8] Office of Director of Nat'l Intelligence Press Release, Statement by NCSC Director William Evanina: Election Threat Update for the American Public (Aug. 7, 2020), *at* https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

[9] Barry Zulauf, Independent IC Analytical Ombudsman's on Politicization of Intelligence, SSC 2020-3029, at 4 (Jan. 6, 2021), *available at* https://fas.org/irp/eprint/politicization.pdf.

[10] *Id.* at 6. In her confirmation hearing in January 2020, the Biden Administration's new Director of National Intelligence (DNI) Avril Haines stated, "To safeguard the integrity of our intelligence community, the DNI must insist that, when it comes to intelligence, there is simply no place for politics—ever," and vowed to restore ODNI's

https://doi.org/10.1017/ajil.2021.10 Published online by Cambridge University Press

Some public warnings did categorize Russia as the primary threat. In September, Federal Bureau of Investigation (FBI) Director Christopher Wray told the House Homeland Security Committee "[w]e certainly have seen very active—very active—efforts by the Russians to influence our election in 2020 . . . to both sow divisiveness and discord, and . . . primarily to denigrate Vice President Biden in what the Russians see as a kind of an anti-Russian establishment."[11] In October, the Cybersecurity and Infrastructure Agency (CISA) and the FBI issued a joint advisory warning about "Russian state-sponsored advanced persistent threat (APT) actor activity targeting various U.S. state, local, territorial, and tribal (SLTT) government networks, as well as aviation networks."[12] The warning noted that since the activity was "directed at SLTT government networks, there may be some risk to elections information housed on" such networks, but that "the FBI and CISA have no evidence to date that integrity of elections data has been compromised."[13]

In addition to public warnings, the United States issued sanctions against individuals and entities involved in election interference. On September 10, the U.S. Treasury Department sanctioned Andrii Derkach, "a Member of the Ukrainian parliament, [who] has been an active Russian agent for over a decade . . . [and who] waged a covert influence campaign centered on cultivating false and unsubstantiated narratives concerning U.S. officials in the upcoming 2020 Presidential Election."[14] On September 23, Treasury also sanctioned individuals and entities tied to Yevgeniy Prigozhin, the financier behind the Russian troll factory, Internet Research Agency,[15] which organized an influence campaign in 2016 to denigrate then-presidential candidate Hillary Clinton.[16] The Treasury Department explained that the sanctions "build[] on the U.S. government's efforts to promote accountability for the Russian government's intelligence organizations, including the Federal Security Service (FSB), for perpetrating an array of destabilizing activities such as conducting malicious cyber activities and interfering in elections, by further targeting networks supporting their activities."[17]

Moreover, on October 19, the U.S. Department of Justice unsealed indictments against six Russian military officials for hacking incidents including attacks against Ukraine's power grid, deployment of the NotPetya malware, and "hack-and-leak efforts" targeting the 2017 French

nonpartisan role. Martin Matishak, *"Simply No Place for Politics" in Intelligence Work, Biden's Spy Chief Nominee Will Say*, POLITICO (Jan. 19, 2021), *at* https://www.politico.com/news/2021/01/19/avril-haines-spy-chief-confirmation-hearing-460309.

[11] Zolan Kanno-Youngs, *F.B.I. Director Warns of Russian Interference and White Supremacist Violence*, N.Y. TIMES (Sept. 17, 2020), *at* https://www.nytimes.com/2020/09/17/us/politics/fbi-russia.html.

[12] Cybersecurity & Infrastructure Security Agency Alert, Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets, AA20-296A (Oct. 22, 2020), *at* https://us-cert.cisa.gov/ncas/alerts/aa20-296a.

[13] *Id.*

[14] U.S. Dep't of Treasury Press Release, Treasury Sanctions Russia-Linked Election Interference Actors (Sept. 10, 2020), *at* https://home.treasury.gov/news/press-releases/sm1118; *see also* Nat'l Intel. Council, *supra* note 2, at 2 ("[W]e assess that Putin had purview over the activities of Andriy Derkach, a Ukrainian legislator who played a prominent role in Russia's election influence activities."). Following the election, the Treasury Department levied sanctions on additional members of Derkach's inner circle. U.S. Dep't of Treasury Press Release, Treasury Takes Further Action Against Russian-Linked Actors (Jan. 11, 2021), *at* https://home.treasury.gov/news/press-releases/sm1232.

[15] U.S. Dep't of Treasury Press Release, Treasury Increases Pressure on Russian Financier (Sept. 23, 2020), *at* https://home.treasury.gov/news/press-releases/sm1133.

[16] Nat'l Intel. Council, *supra* note 2.

[17] U.S. Dep't of Treasury, *supra* note 14.

https://doi.org/10.1017/ajil.2021.10 Published online by Cambridge University Press

elections.[18] According to reports, officials indicated that the "indictment was not a specific warning to Moscow to avoid interfering in this year's election, [but] serve[d] as a 'general' warning that such activities are not deniable."[19]

The U.S. actions were not confined to Russia. In late October, voters in Alaska and Florida received threatening "emails claim[ing] to be from . . . the Proud Boys, but evidence . . . mounted that they in fact were the work of another, hidden actor."[20] In "the fastest-ever public disclosure of such intelligence by the United States,"[21] the United States accused Iran of responsibility for the emails on October 21.[22] The next day the Treasury Department sanctioned Iranian government-linked entities, including Iran's Islamic Revolutionary Guard Corps "for having directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in the 2020 U.S. presidential election."[23]

In addition to the public actions by civilian agencies, U.S. Cyber Command also conducted election-related cyber operations. In an interview, Lieutenant General Charles L. Moore Jr., the deputy commander of Cyber Command, explained that "[d]efending the election is now a persistent and ongoing campaign for Cyber Command."[24] In the two years preceding the election, Cyber Command sent teams overseas to "find[] foreign hacking groups before the election . . . [and] identify not only Russian tactics but also those of China and Iran."[25] Cyber Command reportedly took actions to "interfere with the operations of" a Russian hacking group and to "take down, at least temporarily, the Iranian hacking group tied to Tehran's Islamic Revolutionary Guards Corps."[26] In congressional testimony in March 2021, General Paul M. Nakasone, the commander of U.S. Cyber Command, confirmed that Cyber Command "conducted more than two dozen operations to get ahead of foreign threats before they interfered with or influenced our elections in 2020."[27]

[18] U.S. Dep't of Justice Press Release, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (Oct. 19, 2020), *at* https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[19] Ellen Nakashima & Devlin Barrett, *U.S. Charges Russian Intelligence Officers in Several High-Profile Cyberattacks*, WASH. POST (Oct. 19, 2020), *at* https://www.washingtonpost.com/national-security/russia-cyberattacks-election-interference/2020/10/19/51a84208-1208-11eb-bc10-40b25382f1be_story.html.

[20] Ellen Nakashima, Amy Gardner, Isaac Stanley-Becker & Craig Timberg, *U.S. Government Concludes Iran Was Behind Threatening Emails Sent to Democrats*, WASH. POST (Oct. 22, 2020), *at* https://www.washingtonpost.com/technology/2020/10/20/proud-boys-emails-florida.

[21] *Id.*

[22] *Id.*; *see also* Office of Director of Nat'l Intelligence Press Release, DNI John Ratcliffe's Remarks at Press Conference on Election Security (Oct. 22, 2020), *at* https://www.odni.gov/index.php/newsroom/press-releases/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security.

[23] U.S. Dep't of Treasury Press Release, Treasury Sanctions Iranian Entities for Attempted Election Interference (Oct. 22, 2020), *at* https://home.treasury.gov/news/press-releases/sm1158.

[24] Julian E. Barnes, *U.S. Cyber Command Expands Operations to Hunt Hackers From Russia, Iran and China*, N.Y. TIMES (Nov. 2, 2020), *at* https://www.nytimes.com/2020/11/02/us/politics/cyber-command-hackers-russia.html.

[25] *Id.*

[26] David E. Sanger & Julian E. Barnes, *U.S. Tried a More Aggressive Cyberstrategy, and the Feared Attacks Never Came*, N.Y. TIMES (Nov. 9, 2020), *at* https://www.nytimes.com/2020/11/09/us/politics/cyberattacks-2020-election.html.

[27] Posture Statement of Gen. Paul M. Nakasone, Cmdr., U.S. Cyber Command, Before the 117th Cong. S. Armed Services Comm., at 3 (Mar. 25, 2021), *available at* https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-25-21.pdf.

In addition to the U.S. governmental efforts, U.S. technology and social media companies also stepped up to respond to operations aimed at the election. In September, Microsoft reported on cyberattacks "targeting people and organizations involved in the upcoming presidential election, including unsuccessful attacks on people associated with both the Trump and Biden campaigns."[28] Microsoft noted that a Russian hacking group "responsible for the attacks on the Democratic presidential campaign in 2016" had "attacked more than 200 organizations including political campaigns, advocacy groups, parties and political consultants."[29] Microsoft further explained that an Iranian hacking group, whose infrastructure Microsoft had seized pursuant to court orders, "continued to attack the personal accounts of people associated with" the Trump campaign.[30] Finally, the company noted that Chinese actors "appear[] to have indirectly and unsuccessfully targeted the Joe Biden for President campaign through non-campaign email accounts belonging to people affiliated with the campaign" and "also targeted at least one prominent individual formerly associated with the Trump Administration."[31]

Throughout the fall, social media companies publicized their efforts to thwart foreign influence operations. In 2019, Facebook CEO Mark Zuckerberg acknowledged some of his company's earlier failures to curb the spread of disinformation and noted "[w]e've gone from being on our back foot to proactively identifying clusters of fake accounts and taking them down."[32] In September and October 2020, Facebook issued statements detailing numerous networks and associated accounts, pages, and groups that it removed from both Facebook and Instagram.[33] Twitter also undertook policy changes ahead of the election to curb foreign and domestic disinformation,[34] and it suspended and banned foreign accounts for "platform manipulation."[35]

Finally, in October, Cyber Command and Microsoft, working simultaneously, but not in collaboration, conducted operations to disrupt "the TrickBot botnet, an army of at least 1 million hijacked computers run by Russian-speaking criminals" amid concern that it could be used to deliver ransomware to election-related systems.[36] Cyber Command reportedly hacked TrickBot's command and control servers and temporarily cut off access to thousands

[28] Tom Burt, *New Cyberattacks Targeting U.S. Elections*, MICROSOFT (Sept. 10, 2020), *at* https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden.

[29] *Id.*; *see also* David E. Sanger & Nicole Perlroth, *Russian Intelligence Hackers Are Back, Microsoft Warns, Aiming at Officials of Both Parties*, N.Y. TIMES (Sept. 10, 2020), *at* https://www.nytimes.com/2020/09/10/us/politics/russian-hacking-microsoft-biden-trump.html.

[30] Burt, *supra* note 28.

[31] *Id.*

[32] Shannon Bond, *"We Have A Big Responsibility": Facebook Rolls Out New Election Security Measures*, NPR (Oct. 21, 2019), *at* https://www.npr.org/2019/10/21/772035601/we-have-a-big-responsibility-facebook-rolls-out-new-election-security-measures.

[33] Nathaniel Gleicher, *Removing Coordinated Inauthentic Behavior*, FACEBOOK (Oct. 8, 2020), *at* https://about.fb.com/news/2020/10/removing-coordinated-inauthentic-behavior-september-report; Nathaniel Gleicher, *Removing Coordinated Inauthentic Behavior*, FACEBOOK (Sept. 24, 2020), *at* https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-russia.

[34] Vijaya Gadde & Kayvon Beykpour, *Additional Steps We're Taking Ahead of the 2020 US Election*, TWITTER (Oct. 9, 2020), *at* https://blog.twitter.com/en_us/topics/company/2020/2020-election-changes.html.

[35] *See, e.g.*, Sheera Frenkel & Julian E. Barnes, *Russians Again Targeting Americans with Disinformation, Facebook and Twitter Say*, N.Y. TIMES (Sept. 1, 2020), *at* https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html.

[36] Ellen Nakashima, *Cyber Command Has Sought to Disrupt the World's Largest Botnet, Hoping to Reduce Its Potential Impact on the Election*, WASH. POST (Oct. 9, 2020), *at* https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html; *see also* David E. Sanger & Nicole Perlroth, *Microsoft Takes Down a Risk to the Election, and Finds the U.S. Doing*

https://doi.org/10.1017/ajil.2021.10 Published online by Cambridge University Press

of affected computers.[37] In parallel, Microsoft obtained an injunction from a federal court allowing it to seize Trickbot infrastructure and disable some of the botnet's operations.[38]

U.S. officials have consistently asserted that foreign government operations did not compromise the security of the 2020 election.[39] The intelligence community report released in March 2021 provides more details on the nature of foreign governments' actions. The report distinguishes between "election interference," defined as "activities targeted at the technical aspects of the election, including voter registration, casting and counting ballots, or reporting results," and a broader category of "election influence," which includes efforts by foreign governments or their proxies "intended to affect directly or indirectly a US election—including candidates, political parties, voters or their preferences, or political processes."[40] While the report concludes that the intelligence community has "no indications any foreign actor attempted" election interference, it details influence operations by Russia and Iran tied to both countries' leaders.[41] With respect to Russia, the report states:

> We assess that President Putin and the Russian state authorized and conducted influence operations against the 2020 US presidential election aimed at denigrating President Biden and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US. Unlike in 2016, we did not see persistent Russian cyber efforts to gain access to election infrastructure. . . .
>
> A key element of Moscow's strategy this election cycle was its use of people linked to Russian intelligence to launder influence narratives including misleading or unsubstantiated allegations against President Biden-through US media organizations, US officials,

*the Same*, N.Y. TIMES (Oct. 12, 2020), *at* https://www.nytimes.com/2020/10/12/us/politics/election-hacking-microsoft.html.

[37] Jay Greene & Ellen Nakashima, *Microsoft Seeks to Disrupt Russian Criminal Botnet It Fears Could Seek to Sow Confusion in the Presidential Election*, WASH. POST (Oct. 12, 2020), *at* https://www.washingtonpost.com/technology/2020/10/12/microsoft-trickbot-ransomware.

[38] *Id.*; *see also* Tom Burt, *New Action to Combat Ransomware Ahead of U.S. Elections*, MICROSOFT (Oct. 12, 2020), *at* https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections. For filings and orders in the case, see Trickbot, Microsoft Corp. v. John Does 1-2, No. 1:20-cv-01171 (E.D. Va. Oct. 12, 2020), *available at* https://noticeofpleadings.com/trickbot.

[39] Ellen Nakashima, *U.S. Undertook Cyber Operation Against Iran as Part of Effort to Secure the 2020 Election*, WASH. POST (Nov. 3, 2020), *at* https://www.washingtonpost.com/national-security/cybercom-targets-iran-election-interference/2020/11/03/aa0c9790-1e11-11eb-ba21-f2f001f0554b_story.html (reporting that NSA Director General Nakasone "was 'very confident in actions' taken against adversaries 'over the last several weeks and the past several months to make sure that they're not going to interfere in our elections'"); CISA Press Release, Statement from CISA Director Krebs Following Final Day of Voting (Nov. 4, 2020), *at* https://www.cisa.gov/news/2020/11/04/statement-cisa-director-krebs-following-final-day-voting (quoting CISA Director Christopher Krebs asserting that "we have no evidence any foreign adversary was capable of preventing Americans from voting or changing vote tallies"); CISA Press Release, Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees (Nov. 12, 2020), *at* https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election (quoting a statement from a group of local, state, and federal officials declaring that "[t]he November 3rd election was the most secure in American history").

[40] Nat'l Intel. Council, *supra* note 2.

[41] *Id.* at 1. *See also* Julian E. Barnes, *Russian Interference in 2020 Included Influencing Trump Associates, Report Says*, N.Y. TIMES (Mar. 16, 2021), *at* https://www.nytimes.com/2021/03/16/us/politics/election-interference-russia-2020-assessment.html.

https://doi.org/10.1017/ajil.2021.10 Published online by Cambridge University Press

and prominent US individuals, some of whom were close to former President Trump and his administration.[42]

The report notes that Iran's actions were "more aggressive than in past election cycles" and asserts that "Supreme Leader Ali Khamenei probably authorized Iran's influence campaign."[43] The report concludes with "high confidence that Iran carried out an influence campaign . . . intended to undercut the reelection prospects of former President Trump and to further its longstanding objectives of exacerbating divisions in the US, creating confusion, and undermining the legitimacy of US elections and institutions."[44]

Contrary to some government statements in the runup to the election, the report concludes that "China did not deploy interference efforts and considered but did not deploy influence efforts intended to change the outcome of the US presidential election," noting that "Beijing's risk calculus . . . was informed by China's preference for stability in the bilateral relationship, their probable judgment that attempting to influence the election could do lasting damage to US-China ties, and belief that the election of either candidate would present opportunities and challenges for China."[45]

An accompanying report by the Departments of Justice and Homeland Security similarly concluded that those agencies lack evidence that "any foreign government-affiliated actor prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspects of the voting process; or otherwise compromised the integrity of voter registration information of any ballots cast during 2020 federal elections."[46] The report rejects as "not credible" "multiple public claims that one or more foreign governments—including Venezuela, Cuba, or China—owned, directed, or controlled election infrastructure," or manipulated such infrastructure or vote counts.[47]

Although the United States avoided foreign interference in the 2020 election, media interviews with government officials since the election suggest that "the government's emphasis on election defense, while critical in 2020, may have diverted resources and attention from long-brewing problems like protecting the 'supply chain' of software."[48] On December 8, the cybersecurity firm FireEye announced that it had been compromised by a state-sponsored actor,[49] but it quickly became clear that the incident was far broader. Traced to malicious code inserted into network management software from a company

[42] Nat'l Intel. Council, *supra* note 2, at 2.

[43] *Id.* at 5–6.

[44] *Id.* at 5.

[45] *Id.* at 7. The report notes a minority view from the national intelligence officer for cyber, who "assesses that China took at least some steps to undermine former President Trump's reelection chances." *Id.* at 8.

[46] Key Findings and Recommendations from the Joint Report of the Department of Justice and the Department of Homeland Security on Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2020 US Federal Election (Mar. 2021), *at* https://www.justice.gov/opa/press-release/file/1376761/download.

[47] *Id.* at 2. *See also* Barnes, *supra* note 41.

[48] David E. Sanger, Nicole Perlroth & Julian E. Barnes, *As Understanding of Russian Hacking Grows, So Does Alarm*, N.Y. Times (Jan. 2, 2021), *at* https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

[49] FireEye Inc., Current Report (Form 8-k) (Dec. 8, 2020), *at* https://www.sec.gov/ix?doc=/Archives/edgar/data/1370880/000137088020000037/feye-20201208.htm; *see also Unauthorized Access of FireEye Red Team Tools*, FireEye (Dec. 8, 2020) *at* https://www.fireeye.com/blog/threat-research/2020/12/unauthorized-access-of-fireeye-red-team-tools.html.

https://doi.org/10.1017/ajil.2021.10 Published online by Cambridge University Press

called SolarWinds,[50] the breach also compromised numerous government agencies, including the Departments of Treasury, State, Commerce, Labor, Agriculture, Homeland Security, Justice, and Energy (specifically, the National Nuclear Security Administration, which is responsible for the U.S. nuclear weapons stockpile), parts of the Pentagon, the National Institute of Health, and the U.S. federal courts, as well as around one hundred companies.[51] The "scale of potential access far exceeded the number of known compromises," however, suggesting that more breaches could be uncovered.[52] In a joint statement on January 5, the FBI, CISA, ODNI, and National Security Agency (NSA) indicated the intrusion was "likely Russian in origin . . . [and] was, and continues to be, an intelligence gathering effort."[53]

President Biden has tasked the intelligence community with providing a "full assessment of the SolarWinds cyber breach," among other things.[54] Deputy National Security Adviser for Cyber and Emerging Technology Anne Neuberger is "overseeing the response" to the SolarWinds breach.[55] In a February press briefing, Neuberger explained that, while coordinating with the private sector, the government is "working to expel the adversary, . . . working to . . . improve the cybersecurity of federal networks, and . . . also carefully thinking through how we respond."[56] Neuberger noted, "This isn't the only case of malicious cyber activity of likely Russian origin, either for us or for our allies and partners. So as we contemplate future response options, we're considering holistically what those activities were."[57]

[50] *See, e.g.*, Sanger, Perlroth & Barnes, *supra* note 48.

[51] Eric Geller, *The Big Hack: What We Know, What We Don't*, POLITICO (Dec. 17, 2020), *at* https://www.politico.com/newsletters/politico-nightly/2020/12/17/the-big-hack-what-we-know-what-we-dont-491184 (addressing the breaches at Treasury, State, Commerce, Energy, Agriculture, Homeland Security, and the National Institute of Health); U.S. Dep't of Justice Press Release, Department of Justice Statement on Solarwinds Update (Jan. 6, 2021), *at* https://www.justice.gov/opa/pr/department-justice-statement-solarwinds-update (noting the breach at the Department of Justice); U.S. Courts Press Release, Judiciary Addresses Cybersecurity Breach: Extra Safeguards to Protect Sensitive Court Records (Jan. 6, 2021), *at* https://www.uscourts.gov/news/2021/01/06/judiciary-addresses-cybersecurity-breach-extra-safeguards-protect-sensitive-court; Maryclaire Dale, *Russian Hack Brings Changes, Uncertainty to US Court System*, AP NEWS (Jan. 31, 2021), *at* https://apnews.com/article/coronavirus-pandemic-courts-russia-375942a439bee4f4b25f393224d3d778 (addressing breach in the U.S. federal courts); Eric Morath & Sarah Chaney Cambon, *SolarWinds Hack Leaves Market-Sensitive Labor Data Intact, Scalia Says*, WALL ST. J. (Jan. 14, 2021), *at* https://www.wsj.com/articles/solarwinds-hack-leaves-market-sensitive-labor-data-intact-scalia-says-11610627053 (noting breach at Department of Labor); White House Press Release, Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger (Feb. 17, 2021) *at* https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021 [https://perma.cc/7SRQ-25RP] ("[A]bout 100 private sector companies were compromised.").

[52] White House Press Release, *supra* note 51.

[53] CISA Press Release, Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director Of National Intelligence (ODNI), and the National Security Agency (NSA) (Jan. 5, 2021), *at* https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure.

[54] White House Press Release, Briefing by Press Secretary Jen Psaki (Jan. 21, 2021), *at* https://www.whitehouse.gov/briefing-room/press-briefings/2021/01/21/press-briefing-by-press-secretary-jen-psaki-january-21-2021 [https://perma.cc/4GWX-8CFR].

[55] Julian E. Barnes & David E. Sanger, *White House Announces Senior Official Is Leading Inquiry into SolarWinds Hacking*, N.Y. TIMES (Feb. 10, 2021), *at* https://www.nytimes.com/2021/02/10/us/politics/biden-russia-solarwinds-hacking.html.

[56] White House Press Release, *supra* note 51.

[57] *Id.*

https://doi.org/10.1017/ajil.2021.10 Published online by Cambridge University Press